«CHALLENGES AND THREATS TO CRITICAL INFRASTRUCTURE»

Detroit (Michigan, USA) - 2023

Challenges and threats to critical infrastructure. Collective monograph - NGO Institute for Cyberspace Research (Detroit, Michigan, USA), 2023. - 325 p.

The collective monograph was prepared by ukranian scholars within the framework of studies of a wide range of security issues. The authors of the monograph look at the problems of security of the state`s security in a rich manner behind such basic warehouses as military security, information security, military-technical security, environmental and technogenic security

Reviewers:

Ponomarev S.P. - Doctor of Jurisprudence, head of the Department of Administration of the State Service of Special Communications and Information Protection of Ukraine

Hnatyuk S.O. - Ph.D. Chief Researcher of the State Scientific and Research Institute of Cybersecurity Technologies and Information Protection

Silvestrov A.M. - Ph.D. Prof. National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”

ISBN-10/979-8-218-22315-1

Authors

Chapter 1. Avramenko O.V., Polishchuk V.V., Sarapin Yu.O., Voinov I.A. 1, V.A. Malik, N.V. Zhenyuk, N.I. Voropai, O.G. Korol, A.Yu. Strelnikova, Yu.V. Kostenko, O.V. Peredrii, V.V. Gordiychuk, Grinenko O.I., Hrytsyuk V.V., Zubkov V.P., Ptashkin R.L., Palagin V.V., Savostyanenko M.V., Klymenko K.V., Klymenko K.V., Tyutyunyk V . ., Kapelushna T.V.

Chapter 2. Azarenko O., Honcharenko Yu., Divizinyuk M., Shevchenko R., Shevchenko O., V.M. Vashchenko, V.I. Skalozubov, I.B. Korduba, Shcherbak O., Khmyrova A., Khrystych V., Zhuk V. M., Pohosyan G. A., Yevlanov M. V., Cherepnyov I. A., Chumachenko S. M., Kolomiets D. P., Matsko P. I., Kaplia I. O., Romanyuk V. P., Medvedev M. G., Mulyava O. M., Peredrii O. V., Komisarov M. V., Proshchyn I. V., Sydorenko V .L., Eremenko S.A., Tyshchenko V.O., Vlasenko E.A., Pruskyi A.V., Demkiv A.M., Yudina D.O.

Chapter 3. V. N. Yelisieiev, E. V. Bykova, V. S. Tyshchenko, N. V. Zaika, V. A. Popel, S. S. Chumachenko, O. V. Ivchenko, V. V. Palagin, R. Kyrychok. V., Laptev O.A., Laptev S.O., Sobchuk A.V., Ponomarenko V.V., Barabash A.O., Murasov R.K., Chumachenko S.M., Sirik A.O. , Yevtushenko O.V., Sobchuk V.V., Pichkur V.V., Lapteva T.O., Kopytko S.B.

Chapter 4. Goncharenko I.O., Kuchma T.L., Prodanyuk D.M., Zaretskyi I.S., Karpenko M.I., Moshenskyi A.O., Derman V.A., Khoperskyi S. V., Chumachenko S.M., Ponomarenko S.O., Popel V.A, Maslennikova T.A.

Chapter 5. Vovchuk T., Shevchenko R., Shevchenko O., Guida O.G., Kiselyov V.B., Ometsynska N.V., Trysnyuk T.V., Konetska O.O., Nagornyi E. I., Marushchak V.M., Volynets T.V., Prystupa V.V., Trofimchuk O.M., Trysnyuk V.M., Shumeiko V.O., Chumachenko S.M., Lysenko O.I. , O. M. Tachynina, O. V. Furtat, S. O. Furtat, I. O. Sushin.

Chapter 6. Viola Vambol, Alina Kowalczyk-Juśko, Sergij Vambol, Nadeem Ahmad Khan, Aaron Dumont, Zaporozhchenko M.M., Legominova S.V., Muzhanova T.M., Ometsynska N.V., Kiselyov V. B., Huida O. G., Shchavinskyi Y.V., Palchynska V.B.

Chapter 7. Altaf Hussain Lahori, Barbara Savytska, Parisa Ziarati, Barbara Krokhmal-Marchak, Niloofar Mozaffari, Nastaran Mozaffari, Miasoyedova A., Divizinyuk M., Shevchenko R., Myroshnychenko A., Aldoshin O.O., Kalinovsky A.Ya., Vykhvatin M.V., Havrys A.P., R.S. Yakovchuk, O.O. Pekarska, M.V. Yevlanov, R.V. Antoshchenkov, I.A. Cherepnyov, I.I. Kravchenko, V. Loik. B., Synelnikov O.D., Goncharenko M.O., Nazarenko S.Yu., Mandrychenko D.S., Shapovalov M.M., Pichugin M.A., Vynogradov S.A., Samchenko T.V. , Nuyanzin O.V., Sverchkov O.V., Faure E.V., Skutskyi A.B., Lavdanskyi A.O., Grechanyk O.S., Shakhov S.M., Zinchenko O.O., Yatsenko V.O., Vambol S.O.

Chapter 8. Adamova G.V., Anila Kausar, Ambreen Afza, Altaf Hussain Lahori, Bobkov Y.V., Shevchuk A.A., Stamati V.G., Vynogradov S.A., Chumachenko S.M., Lysenko O.I., Novikov V.I., Furtat O.V., Furtat S.O., Sushin I.O., Pisnya L.A., Mishchenko I.V., Vambol S.O., Vambol Viola

Chapter 9. Yakovliev Ye.O., Rudko G.I., Yermakov V.M., Chumachenko S.M., Kodryk A.I., Dyatel O.O., Lubenska N.O.

CONTENT

РОЗДІЛ 1

СИСТЕМНИЙ ПІДХІД ДО ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

УДК 623.48 (477)

1. ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ОБ'ЄКТІВ ЗБЕРІГАННЯ БОЄПРИПАСІВ ВІД НАДЗВИЧАЙНИХ СИТУАЦІЙ ШЛЯХОМ ВПРОВАДЖЕННЯ ОБГРУНТОВАНОЇ ПЕРІОДИЧНОСТІ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ СИСТЕМ ПРОТИПОЖЕЖНОГО ЗАХИСТУ

Авраменко О.В., Поліщук В.В., Сарапін Ю.О.
Національний університет оборони України імені Івана Черняховського
E-mail: savram1977@gmail.com, polva@ukr.net, upb25@ukr.net

Increasing the efficiency of protection of ammunition storage facilities against emergency situations by implementing justified periodic maintenance of fire protection systems

Most man-made emergency situations at military facilities arose and proceeded with fires followed by the detonation of ammunition.

At the fire stage before the start of the ammunition detonation, one of the most effective ways to protect military facilities from emergency situations is the use of fire protection systems.

There is a significant number of failures in the operation of fire protection systems, which are accompanied by false fire signals.

It is assumed that the introduction of a scientifically based periodicity of technical maintenance of fire protection systems will ensure their required operational reliability.

На сьогодні завдання запобігання виникненню надзвичайних ситуацій техногенного характеру (далі – НС) на об'єктах критичної інфраструктури, зокрема на військових об'єктах зберігання боєприпасів Збройних Сил України (далі – військові об'єкти) набуло загальнодержавного характеру [1-3].

Місця зберігання боєприпасів, що знаходяться на території військових об'єктів, є потенційними джерелами техногенної надзвичайної ситуації [4-5]. Одним із уражальних небезпечних чинників джерел НС на військових об'єктах є пожежа [6].

За роки незалежності України НС на військових об'єктах виникали понад два десятки разів. Практично всі вони виникали та протікали із супроводженням пожеж та подальшою детонацією боєприпасів.

Аналіз останніх досліджень і публікацій [7-10] показав, що актуальним завданням є пошук нових ефективних шляхів підвищення захисту військових об'єктів від виникнення НС унаслідок пожежі.

На етапі пожежі до початку детонації боєприпасів на об'єктах зберігання боєприпасів [11], одним із найбільш ефективних шляхів їх захисту від виникнення НС є використання систем протипожежного захисту [12], які призначені для виявлення, локалізації та ліквідування пожеж без втручання людини.

У Збройних Силах України на військових об'єктах (ВО) передбачено встановлення автоматичних систем пожежогасіння та систем пожежної сигналізації (далі – СПЗ ВО) [13].

Ще на етапі проектування СПЗ ВО особливу увагу приділяють характеристикам їх експлуатаційної надійності [14] та безвідмовності.

З досвіду використання СПЗ ВО відомо, що значна кількість відмов в їх роботі, тобто перехід зі стану справності в стан несправності, супроводжуються хибними сигналами системи (помилковими тривогами) про пожежу.

Для військових об'єктів, з урахуванням потенційної загрози, яку вони несуть, експлуатаційна надійність та забезпечення мінімальної частоти помилкових тривог СПЗ ВО є особливо актуальними.

Підтримання експлуатаційної придатності (технічне обслуговування) СПЗ ВО та спостерігання за ними відноситься до переліку послуг і робіт, що підлягають ліцензуванню [15]. Тобто виконання робіт з технічного обслуговування СПЗ ВО на військових об'єктах повинно здійснюватися виключно представниками спеціалізованих організацій (на договірній основі), які мають відповідну ліцензію.

У Міністерстві оборони України та Збройних Силах України встановлено, що СПЗ ВО повинні щороку перевірятися на їх відповідність технічним умовам виробників із залученням представників спеціалізованої організації (за згодою) [13]. Тобто фактично, технічне обслуговування СПЗ ВО планується та проводиться один раз на рік. Така періодичність проведення заходів з технічного обслуговування СПЗ ВО ніяк не обґрунтована.

Проведений аналіз кількості помилкових тривог СПЗ ВО свідчить, що чим більше часу проходить з моменту технічного обслуговування, тим більша кількість помилкових тривог в системах. Можна зробити припущення, що для СПЗ ВО існує необхідність у перегляді періодичності проведення технічних обслуговувань.

Оптимальна періодичність проведення технічного обслуговування СПЗ ВО повинна забезпечувати максимальне значення коефіцієнта технічного використання $K_{ТВ}$. При цьому повинні враховуватися показники безвідмовності конкретної СПЗ ВО, тривалості заходів по відновленню СПЗ ВО у разі її відмови, достовірності контролю визначальних параметрів технічного стану СПЗ ВО вбудованими та зовнішніми засобами контролю. Також необхідною умовою для визначення коефіцієнта технічного використання $K_{ТВ}$ є визначення моделі відмови СПЗ ВО.

Визначення оптимальної періодичності проведення технічних обслуговувань вплине на підвищення ефективності експлуатації СПЗ ВО. Ефективність експлуатації СПЗ ВО може бути визначена при наявності математичної моделі їх функціонування, яка повинна враховувати як планові, так і позапланові види відновлювальних (профілактичних) робіт.

Отже, науково обґрунтоване планування та регулярне виконання заходів з технічного обслуговування СПЗ ВО може безпосередньо вплинути на їх експлуатаційну надійність, а також у довгостроковій перспективі підвищити рівень захисту військових об'єктів від виникнення НС унаслідок пожежі.

Висновки

1. За результатами проведених досліджень визначено, що одним із чинників, які негативно впливають на експлуатаційну надійність систем протипожежного захисту, є необґрунтована періодичність проведення їх технічних обслуговувань.

2. В подальшому впровадження науково обґрунтованої періодичності технічних обслуговувань систем протипожежного захисту дозволить забезпечити потрібну їх експлуатаційну надійність та у довгостроковій перспективі запобігти виникненню надзвичайних ситуацій техногенного характеру унаслідок пожежі на військових об’єктах.

Література

1. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року “Про Стратегію національної безпеки України”: Указ Президента України від 14 вересня 2020 року № 392/2020 / Президент України. – Офіц. вид. – К.: Офіційний вісник Президента України, 2020, № 19, стор. 26, стаття 926.
2. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року ”Про Стратегічний оборонний бюлетень України”: Указ Президента України від 17 вересня 2021 року № 473/2021 / Президент України. – Офіц. вид. – К.: Офіційний вісник Президента України, 2021, № 24, стор. 27, стаття 1088.
3. Про додаткові заходи щодо покращення стану зберігання ракет, боєприпасів та продуктів їх утилізації на арсеналах, базах та складах Збройних Сил України: Указ Президента України від 4 листопада 2019 року № 799/2019 / Президент України. – Офіц. вид. – К.: Офіційний вісник Президента України, 2019, № 24, стор. 10, стаття 1003.
4. Безпека у надзвичайних ситуаціях. Техногенні надзвичайні ситуації. Терміни та визначення основних понять: ДСТУ 4933:2008. – [Чинний від 2008-07-01]. – К.: Держспоживстандарт України, 2008. – 17 с. – (Національний стандарт України).
5. Про об’єкти підвищеної небезпеки: Закон України від 18 січня 2001 року № 2245-III / Верховна Рада України. – Офіц. вид. – К.: Відомості Верховної Ради України, 2001, № 15, стаття 73.
6. Кодекс цивільного захисту України: Закон України від 2 жовтня 2012 року № 5403-VI / Верховна Рада України. – Офіц. вид. – К.: Відомості Верховної Ради України, 2013, № 34-35, стор. 1802, стаття 458.
7. Морщ С.В. Інформаційно-технічні методи попередження надзвичайних ситуацій техногенного характеру на об’єктах критичної інфраструктури в районах бойових дій: автореф. дис. на здобуття наук. ступеня д-ра техн. наук: спец. 21.02.03. “Цивільний захист” / С.В. Морщ. – Київ, 2021. – 35 с. (інв. № 17628 ДСК).
8. Тищенко О.М. Інформаційно-технічні методи попередження надзвичайних ситуацій техногенного та терористичного характеру на об’єктах критичної інфраструктури: автореф. дис. на здобуття наук. ступеня д-ра техн. наук: спец. 21.02.03. “Цивільний захист” / О.М. Тищенко. – Київ, 2021. – 32 с. (інв. № 17674 ДСК).
9. Касаткіна Н.В. Інформаційно-технічні методи запобігання надзвичайних ситуацій терористичного характеру з використанням баз даних відеосистем

зовнішнього спостереження на об’єктах критичної інфраструктури України: автореф. дис. на здобуття наук. ступеня д-ра техн. наук: спец. 21.02.03. “Цивільний захист” / Н.В. Касаткіна. – Київ, 2019. – 44 с. (інв. № 17105 ДСК).
10. Михайлова А.В. Система моніторингу та оповіщення про надзвичайні ситуації в зоні проведення операції Об’єднаних Сил: автореф. дис. на здобуття наук. ступеня канд. техн. наук: спец. 21.02.03. “Цивільний захист” / А.В. Михайлова – Київ, 2020. – 21 с. (інв. № 17359 ДСК).
11. Аветісян В.Г. Обґрунтування вихідних даних для розрахунку сил та засобів пожежогасіння на об’єктах з наявністю боєприпасів та вибухових речовин / В.Г. Аветісян, Ю.М. Сенчихін // Збірка наукових праць. Проблеми надзвичайних ситуацій. – 2018. – № 27. – С. 3–9.
12. Системи протипожежного захисту: ДБН В.2.5-56:2014. – [Чинні від 2015-07-01]. – К.: Мінрегіон України, 2015. – 127 с. – (Державні будівельні норми України).
13. Про затвердження Переліку об'єктів Міністерства оборони України та Збройних Сил України, які підлягають обладнанню системами протипожежного захисту: Наказ Міністерства оборони України від 21 грудня 2017 року № 690 / Міністерство оборони України.
14. Основні вимоги до будівель і споруд. Пожежна безпека. ДБН В.1.2-7:2021. – [Чинні від 2022-09-01]. – К.: Мінрегіон України, 2022. – 13 с. – (Державні будівельні норми України).
15. Деякі питання ліцензування господарської діяльності з надання послуг і виконання робіт протипожежного призначення: Постанова Кабінету Міністрів України від 23 листопада 2016 року № 852 / Кабінет Міністрів України. – Офіц. вид. – К.: Офіційний вісник України, 2016, № 94, стор. 115, стаття 3085.

УДК 351:62

2.СИСТЕМНИЙ ПІДХІД ДО ЗАХИСТУ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Воїнов І. А. [1], Малик В. А. [1]

1. Громадська організація «Асоціація Захисту Критичної Інфраструктури»

A systematic approach to the protection of critical infrastructure objects

The report provides a brief description of the current state of affairs regarding the protection of critical infrastructure objects in Ukraine. The article analyzes the current situation and threats affecting the functioning of critical infrastructure facilities, including threats related to military actions, highlights the problems that exist in the field of protection of critical infrastructure objects. Is also given an analysis of existing norms and legislation in the field of critical infrastructure, in particular the Law of Ukraine "About Critical Infrastructure". On the basis of the presented analysis, the issues that require a priority solution for the further development of the sphere of protection of critical infrastructure objects are shown.

Сьогоднішня ситуація в світі приносить з собою нові виклики безпеки, які пов’язані з техногенними катастрофами, що можуть бути спричинені загрозами через зміни клімату чи людський фактор, через здійснення терористичної діяльності, фізичними чи кібер- атаками. Це обумовлює постійну необхідність перегляду та оновлення політики, практики та технологій для забезпечення зростаючих потреб безпеки об’єктів критичної інфраструктури (ОКІ).

В Україні ситуація ще більш складна. У нас відбуваються воєнні дії і ми захищаємо свою незалежність та територіальну цілісність. Разом з проведенням суто бойових операції, ворог наносить численні удари по критичних об'єктах, маючи на меті унеможливити нормальне життя мирного населення, порушуючи Закони та звичаї війни і Міжнародне Гуманітарне Право.

Сьогодні життя нашого суспільства можна представити собі як організм людини, а елементи критичної інфраструктури на кшталт життєвих артерій. Ми залежимо від надійної роботи систем енергопостачання та водопостачання, інформаційних технологій, мобільного зв’язку, банківської системи тощо. Якщо значні обсяги цих систем чи інших важливих елементів інфраструктури виходять з ладу, хоча б на короткий термін, це може призвести до важких наслідків.

Українці, це відчули 28 листопада 2022 року коли ракетні обстріли російських окупантів по об’єктах критичної інфраструктури нашої країни призвели до руйнування багатьох складових енергосистеми в результаті чого відбулось критичне падіння частоти в електромережі, що завершилось зупинкою усіх атомних енергоблоків АЕС країни і, як наслідок, повний «Blackout». Більшість українців від 2 до 5 днів жили без електроенергії, води та мобільного зв’язку. Тому з впевненістю можна сказати, що критична інфраструктура починається з нас та наших осель, з того чим людина в сучасному світі звикла користуватися у повсякденні.

Говорячи про об’єкти критичної інфраструктури, треба враховувати всі загрози, що можуть впливати на їх нормальну роботу: пандемії, стихійні лиха, техногенні катастрофи, кібератаки та терористичні акти, які можуть призводити до значних наслідків. В Україні сьогодні додається ще один важливий чинник – це військові дії. Від терористичних актів вони відрізняються тим, що відбуваються не одноразово, а носять перманентний, планомірний характер, спрямований на знищення того, чи іншого об'єкту, або їх мережі.

Разом з цим існує ряд чинників, які ускладнюють захист ОКІ:

- Збройна агресія зі сторони російської федерації. Перед урядом стоять більш пріоритетні задачі щодо забезпечення функціонування держави. І ми вимушені реагувати на миттєві виклики.
- Велика кількість об’єктів, розміщених на великих відстанях один від одного.
- Важкі умови експлуатації.
- Широкий ряд засобів захисту та безпеки, які необхідні для комплексного захисту об’єктів.
- Відсутні рекомендовані стандарти, які забезпечують базові вимоги для захисту.

До законодавчої бази сьогодні можна віднести:

1. Закон України «Про критичну інфраструктуру» (1882-IX від 16.11.2021), який набрав чинності 15.12.2021, але почав діяти з 15.06.2022
2. Постанова КМУ від 09.10.2020 № 1109 «Деякі питання об'єктів критичної інфраструктури», зі змінами від 29.12.2021, яка набула чинності 31.12.2021

Сюди також можна віднести і Пояснювальну записку до проекту постанови Кабінету Міністрів України «Про затвердження Порядку віднесення об'єктів до об'єктів критичної інфраструктури», яка була підготовлена Державною службою спеціального зв'язку та захисту інформації України.

Отже, чітко прослідковуються проблеми, які існують в сфері захисту об'єктів критичної інфраструктури, а саме:

1. Відсутність єдиного реєстру ОКІ України (повинен формуватися і вестися уповноваженим органом).
2. Багато власників ОКІ не знають, чи відноситься їх об'єкт до критичної інфраструктури. Якщо відноситься то до якої категорії I, II, III або IV? (Секторальні органи мають визначати категорію ОКІ).
3. Відсутність детального плану побудови системи захисту ОКІ.
4. Відсутність єдиної злагодженої системи управління безпекою ОКІ.
5. Відсутність профільних фахівців з захисту ОКІ та навчальних закладів для їх підготовки.
6. Не розроблений та відсутній Паспорт Безпеки Об'єкта Критичної Інфраструктури (ПБО КІ).

Підсумовуючи все зазначене вище, можна сказати, що перші позитивні кроки в напрямку створення єдиної системи захисту об'єктів критичної інфраструктури вже відбуваються, але є питання які нам усім необхідно буде вирішити:

1. Створення та затвердження супровідних нормативних актів, які будуть регламентувати роботу операторів та суб'єктів захисту ОКІ (реєстр ОКІ, паспорт безпеки, координаційний центр, реєстр загроз, система оповіщення і порядок дій при виникненні відповідних загроз та багато іншого).
2. Проходження навчальних курсів закордоном із захисту ОКІ відповідними фахівцями та створення відповідних факультетів в цьому напрямку на базі існуючих вищих навчальних закладів.
3. Співпраця з європейськими колегами щодо побудови в Україні сучасної комплексної системи захисту ОКІ.
4. Плідна робота та взаємодія з представниками операторів критичної інфраструктури.
5. Започаткування нових проектів щодо відбудови зруйнованих ОКІ на території України.

Проте, ми впевнені, що об'єднання зусиль Уповноваженого органу, громадських організацій та операторів ринку захисту критичної інфраструктури, призведе до зміцнення даної галузі, залученню інвестицій та зміцненню авторитету держави Україна на міжнародній арені.

Література

1. Закон України «Про критичну інфраструктуру» 1882-IX від 16.11.2021
2. Постанова КМУ від 09.10.2020 № 1109 «Деякі питання об'єктів критичної інфраструктури», зі змінами від 29.12.2021
3. National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience.
4. ДИРЕКТИВА РАДИ 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту.
5. EN 62676-4 Video surveillance systems for use in security applications - Part 4: Application guidelines (IEC 62676-4:2014).

УДК 681.32:007.5

3.МОДЕЛЬ БЕЗПЕКИ СОЦІОКІБЕРФІЗИЧНОЇ СИСТЕМИ

Дженюк Н.В.[1], Воропай Н.І.[1], Король О.Г.[1], Стрельнікова А.Ю.[1]

1 Національний технічний університет «Харківський політехнічний інститут», Харків, Україна

E-mail: natalidzh16@gmail.com, voropay.n@gmail.com, vainanny96@gmail.com, korol.olha2016@gmail.com

Security model of sociocyberphysical system

The mathematical model that links the structure of the end devices of the CPSS wireless network - the system with the behavior strategy of the external environment was developed. The model proved the existence of the optimal behavior strategy of the external environment and the optimal primary structure of the system. Optimizing the structure of the system at the stage of its development made it possible to increase the resource of the external environment by more than one and a half times, which is sufficient to breach its security level.

В умовах формування високотехнологічного суспільства соціальні мережі на ґрунті Інтернет-сервісів перетворилися на найбільш популярні засоби масових комунікацій. Синтез соціальних Інтернет-сервісів з кіберфізичними системами дозволили сформувати соціокіберфізичну систему (cyberphysical social system, CPSS). При цьому слід зазначити, що кіберфізичні системи (Cyder-Physical System, CPS) є складними розподіленими системами, що керуються або контролюються комп'ютерними алгоритмами та здійснюють обчислювальні процедури у своєму розподіленому середовищі із зворотнім зв'язком [1]. Вони пов'язують фізичний світ з інформаційним та фокусуються на фундаментальній інтелектуальній проблемі об'єднання інженерних традицій кібер- та фізичних світів, створюючи гібридну систему. Це суттєво ускладнює можливість забезпечення необхідного рівня безпеки,

особливо з використанням безпровідних мобільних каналів передачі даних. Кібербезпека стає усе більш універсальною областю, де ціла низка аспектів, що включає переконання, соціальний вплив, емоції у прийнятті рішень та визначає пов'язану з цим людську вразливість. Ці механізми вразливості та методи атак використовують для обґрунтування успіху атак на CPSS системи [2]. При цьому зловмисник використовує людську вразливість та вразливість програмного забезпечення для порушення безпеки кіберпростору, що перетворює CPSS системи на постійну універсальну погрозу її безпеці.

Найбільш слабкою ланкою при реалізації відповідного рівня безпеки CPSS системи є гібридна безпровідна повітряна мобільна однорангова мережа FANET (Flying Ad Hoc Network) [3]. Вона являє собою сукупність БПЛА, на кожному з яких встановлено комутаційний модуль. Вони об'єднані один з одним каналами зв'язку, зовнішніми пунктами управління наземного базування та базовими станціями наземного мобільного зв'язку. Об'єднання окремих пристроїв до мережі FANET перетворює її на складну динамічну систему, що функціонує в умовах суттєвої апріорної невизначеності та випадковим чином організує взаємодію її різних складових. Особливістю її функціонування є автоматичне переміщення БПЛА у реальному часі по заздалегідь закладеній програмі. Причому, наявність комплексу засобів для керування БПЛА і потенційно вразливих місць у протоколах передачі даних, програмному забезпеченні систем управління, передачі даних та навігації створює загрозу безпеці CPSS – системі, зокрема як безпровідній системі зв'язку, так і кінцевим пристроям радіоелектронного обладнання, які забезпечують її працездатність

Для зменшення вразливості радіоелектронного та програмного забезпечення до дії завад розроблена загальна математична модель взаємодії зовнішнього середовища та самої системи. Розроблена мінімаксна модель кінцевого радіоелектрнного пристрою безпровідної мережі довела, що його структура залежить тільки від стратегії поведінки зовнішнього середовища та первинної структури кінцевого радіоелектрнного пристрою. Причому існує оптимальне співвідношення робочих та захисних елементів радіоелектрнного пристрою. Та коли кількість робочих елементів визначає необхідність виконання пристроєм свого призначення, то кількість захисних елементів пристрою обирають виходячи із знайденого співвідношення. Оптимізація структури системи на стадії її розробки дозволяє більше ніж у півтора рази збільшити ресурс зовнішнього середовища, який є достатнім для порушення рівня безпеки системи. Таким чином оптимальна первинна організація структури змушує зовнішнє середовище витратити максимум свого ресурсу, який є необхідним для порушення безпеки CPSS системи.

Висновки

Розроблена математична модель, яка пов'язує структуру кінцевих пристроїв безпровідної мережі CPSS – системи із стратегією поведінки зовнішнього середовища. Вона показала існування оптимальної стратегії поведінки зовнішнього середовища та оптимальної первинної структури системи. Оптимізація структури системи на стадії її розробки дозволяє більше ніж у півтора рази збільшити ресурс зовнішнього середовища, який є достатнім для порушення її рівня безпеки.

Література

1. Lee E. A. (2015). The past, present and future of cyber-physical systems: a focus on models. Sensors (Basel, Switzerland), 15(3), 4837–4869. https://doi.org/10.3390/s150304837
2. Serhii Yevseiev, Stanislav Milevskyi, Leonid Bortnik, Voropay Alexey, Kyrylo Bondarenko, Serhii Pohasii. Socio-Cyber-Physical Systems Security Concept. 4th International Congress on Human-Computer Interaction, Optimization and Robotic Applications. June 9-11, 2022, Ankara, Turkey
3. Ayass T, Coqueiro T, Carvalho T, Jailton J, Araújo J, Francês R. Unmanned aerial vehicle with handover management fuzzy system for 5G networks: challenges and perspectives. Intell Robot 2022;2(1):20-36. https://dx.doi.org/10.20517/ir.2021.07

УДК 338.2

4.ЗЕЛЕНИЙ ТАРИФ ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Костенко Ю. В.

ПВНЗ «Європейський університет»

Email: yukostenko@e-u.edu.ua

Green tariff as a tool for improving the security of critical infrastructure facilities

The paper outlines the theoretical perspectives on the use of small-scale renewable electricity generation facilities as a means of reducing the vulnerability of critical infrastructure facilities. The advantages of individual combinations of different types of generating capacity and opportunities to smooth out seasonal and daily fluctuations in power generation are considered. The features of using the green tariff as a tool to improve the security of critical infrastructure are described. The current state of the renewable energy market in Ukraine is discussed.

Починаючи з 70-х років минулого сторіччя у світі почалось запровадження стимуляції розвитку генерації електричної енергії з відновлюваних джерел. Метою цього процесу були протистояння енергетичній кризі та збереження чистоти довколишнього середовища. Одним із основних засобів забезпечення розвитку генерації з відновлюваних джерел став так званий зелений тариф.

Зелений тариф це економічний засіб винагородження виробників електроенергії з відновлюваних джерел. За допомогою цього засобу проводиться заохочення до використання для генерації електроенергії із застосуванням таких видів джерел як сонячна енергія, енергія вітру, гідроенергія, енергія, видобута із застосуванням біомаси та біогазу як палива, геотермальна енергія. Іншими словами зелений тариф це тариф, за яким держава оплачує електроенергію,

видобуту за допомогою вищеозначених джерел, і тим самими заохочує виробників підтримувати та нарощувати об'єми генерації [1]. Ставка тарифу повинна мати такий розмір, щоб учасники генерації мали економічну зацікавленість у процесі та були впевнені у тому, що після періоду компенсації собівартости вони будуть мати можливість отримувати прибуток протягом значного часу. Таким чином для нормальної роботи зеленого тарифу не достатньо лише забезпечити належний рівень оплати зеленого тарифу, але ще необхідно забезпечити роботу цієї схеми протягом довготривалого часу шляхом укладення довгострокових контрактів на закупівлю виробленої енергії. Завдяки цьому у потенційних учасників процесу генерації з'явиться впевненість в тому, що вони повернуть свої інвестиції та будуть мати прибуток у довготривалій перспективі.

Генерація електроенергії з відновлюваних джерел відбувається зазвичай на обладнанні, яке має досить велику територіальну розподіленість. Така розподіленість є значною перевагою в умовах надзвичайних ситуацій та у військових умовах, коли в будь-який момент система генерації з високим коефіцієнтом централізації може бути пошкоджена у наслідок стихійного лиха або шляхом завдання точкового удару. Також однією з переваг розподілених систем генерації є значне скорочення шляхів транспортування виробленої електричної енергії та радикальне зменшення потреби в магістральних лініях передачі, які, своєю чергою, теж є дуже вразливим об'єктом критичної інфраструктури. Їх пошкодження є майже еквівалентом виведення з ладу централізованої енергогенеруючої або розподільчої установки, а де яких випадках і не одної. В той час як у випадку генерації на більшій кількості установок значно зменшується вірогідність їх одночасного пошкодження, як і вірогідність пошкодження ліній передачі виробленої енергії.

В ідеальному випадку генерація в достатніх об'ємах може відбуватись безпосередньо на об'єкті, який споживає весь згенерований об'єм або близьке до нього значення. В такому випадку необхідність наявности підключення до мережі електропостачання диктується лише коливаннями об'ємів добової та сезонної генерації обладнання, яке використовується на об'єкті.

Швидкі коливання обсягів генерації протягом однієї або кількох діб можуть буди скомпенсовані використанням акумуляторних установок. Шляхом використання накопичувачів енергії генераторна установка має можливість накопичувати надлишок згенерованої енергії у батареях, коли це потрібно, і компенсувати нестачу генерації в моменти, коли зовнішні умови не сприяють видобутку великих об'ємів енергії. Також подібна компенсація може бути виконана за рахунок поєднання більш ніж одного виду генерації на одному об'єкті. Наприклад досить перспективно в цьому плані виглядає комбінація сонячних панелей та генератора, який використовує енергію вітру. Також не буде зайвим доповнення такої комбінації акумуляторною установкою [2].

Найменшу залежність від сезону та часу доби мають геотермальні, біогазові та біопаливні та гідрогенеруючі установки. В той самий час ті самі види генерації мають дещо меншу територіальну розподіленість ніж сонячні та вітрові установки генерації. Але в масштабах нашої країни ця різниця не виглядає критичною, хоча і приводить до деякого підвищення числа користувачів на одну установку у разі їх застосування.

Таким чином впровадження зеленого тарифу стимулює розвиток енергетики із застосуванням відновлюваних джерел енергії та одночасно підвищує захищеність об'єктів критичної інфраструктури, таких як енергогенерацій установки, шляхом їх розподілення на місцевості та унеможливлення виходу їх зі строю на значній території одночасно.

Однак для реалізації переваг розподіленої генерації електроенергії потрібно заохотити до цього значну кількість дрібних учасників. На сьогоднішній день, на жаль, наша держава не забезпечує достатнього рівня зацікавленості в учасників ринку генерації з відновлюваних джерел. Так, за результатами 2022 року заборгованість держави перед виробниками енергії становила трохи менше 50% [3]. Також несвоєчасно переглядається затверджений розмір виплат по зеленому тарифу відповідно до актуального курсу валюти. Зараз навіть ведуться розмови про скасування зеленого тарифу на час війни. Це може призвести до банкрутства існуючих електростанцій загальною потужністю близько 8 ГВт. На сьогоднішній час Україна вже почала експорт електричної енергії з Європи. Спотова ціна на електроенергію в ЄС минулого року іноді сягала позначки 600 євро/МВт-год. При цьому собівартість вітрової генерації в Україні знаходиться на рівні 88 євро/МВт-год, а сонячної близько 137 євро/МВт-год. Подібна нестабільність з боку органів влади приводить до значного зниження привабливості будівництва нових об'єктів малої потужності, достатньої для забезпечення електричною енергією окремих об'єктів, з боку потенційних інвесторів.

Висновки

Генерація енергії з відновлюваних джерел на установках малої потужності, достатньої для забезпечення окремих об'єктів інфраструктури, має значний потенціал для зниження уразливості об'єктив критичної інфраструктури шляхом децентралізації генеруючих потужностей. Головним економічним інструментом для стимуляції розвитку таких об'єктів генерації в нашій країні є зелений тариф. На сьогоднішній день, на жаль, повноцінне використання цього інструменту не ведеться і, як наслідок, перспективи такого розвитку не є дуже привабливими і продовжують знижуватись.

Література

1. Закон України про альтернативні джерела енергії. URL: https://zakon.rada.gov.ua/laws/show/555-15#Text

2. Промислова система накопичення енергії, створена в Україні. URL: https://kness.energy/news/energy-storage-system-by-kness-persha-promislova-sistema-nakopichennya-energii-stvorena-v-ukraini/

3. Актуальна інформація щодо розрахунків з виробниками електроенергії. URL: https://www.gpee.com.ua/news_item/342

УДК 004.056

5.ІНТЕГРАЦІЯ ІНОЗЕМНИХ ТА ВІТЧИЗНЯНИХ МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Передрій О.В.[1], Гордійчук В.В.[1], Гріненко О.І.[1], Грицюк В.В.[1], Зубков В.П.[1]

[1] Національний університет оборони України імені Івана Черняховського,

Київ, Україна

E-mail: skifwg@gmail.com

Integration of foreign and domestic mechanisms for ensuring cyber security of critical infrastructure objects

In the conditions of cyber war, launched by the Russian Federation along with military aggression, the issue of protecting information space, including cyberspace, from destructive actions that pose a real threat to national security is definitely relevant. In the course of the research, an analysis of foreign and domestic mechanisms for ensuring cyber security of critical infrastructure facilities was carried out. Prospective directions for the combination of the mentioned mechanisms to strengthen the cyber resilience of the national information infrastructure have been identified.

З початку 2022 року російська федерація розгорнула повномасштабну кібервійну проти України [1]. Це підтверджується зростанням кібератак на державні структури та об'єкти критичної інфраструктури, порушення функціонування яких є загрозою національним інтересам. Кібервійна стала реальною загрозою національній безпеці і передумовою порушення державного суверенітету та територіальної цілісності України країною-агресором 24 лютого 2022 року. Росія нарощувала свої хакерські зусилля проти союзників України, зокрема США. Компанія Microsoft стверджує, що виявила російських державних хакерів, які намагалися проникнути в 128 цілей у 42 країнах, які підтримували Україну [1]. 49% цілей були державними установами. Решта були поєднанням

аналітичних центрів, гуманітарних груп і приватних компаній, задіяних в оборонному чи економічному секторах України. У 2022 році Росія збільшила націлювання на користувачів в Україні на 250% порівняно з 2020 роком.

Україна ратифікувала «Конвенцію про кіберзлочинність», підписану від імені України 23 листопада 2001 року в Будапешті (Закон України про ратифікацію від 7 вересня 2005 року № 2824-IV). Але визнання кіберзахисту новою важливою складовою її захисту в Україні відбулося лише в березні 2016 року в Стратегії кібербезпеки України (далі – Стратегія).

Закон України "Про основи забезпечення кібербезпеки України" закріпив загальну архітектуру національної системи кібербезпеки та розподілив завдання та повноваження між основними суб'єктами забезпечення кібербезпеки, передбачає створення умов для залучення підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (управителями) об'єктів критичної інфраструктури, наукових установ, закладів освіти, організацій, громадських об'єднаннь та громадян.

Національна система кібербезпеки – це комплексна система взаємодії Державної служби спеціального зв'язку та захисту інформації України, Національної поліції України, Служби безпеки України, Міністерства оборони України та Генерального штабу Збройних Сил. України, розвідувальних органів, Національного банку України, діяльність яких спрямована на забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційного, правового, оперативно-розшукового, розвідувального, контррозвідувального, оборонного, інженерного характеру і технічні заходи, а також заходи криптографічного та технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури. Провідним суб'єктом національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, на яку припадає близько 80% навантаження.

Державний центр кіберзахисту та протидії кіберзагрозам Держспецзв'язку має структурний підрозділ – Група комп'ютерного реагування України (CERT-UA) – група реагування на комп'ютерні надзвичайні події України, основною метою якої є: забезпечувати захист інформаційних ресурсів та інформаційно-телекомунікаційних систем від несанкціонованого доступу, неправомірного використання, а також порушення їх конфіденційності, цілісності та доступності.

Основною системою, яка забезпечує кібербезпеку органів державної влади в Україні, є Система безпечного доступу (СБД) до мережі Інтернет для органів державної влади. Системою користуються близько 200 органів державної влади, у тому числі й сектору національної безпеки та оборони. Ця СБД зупиняє та блокує більшість кібератак, у тому числі в автоматичному та напівавтоматичному режимі.

Перед повномасштабним вторгненням. Визнаючи необхідність більшого та міцнішого міжнародного співробітництва та розбудови потенціалу для вирішення проблем кібербезпеки, потреби та загрози, які виникають, також висвітлюються в новій Стратегії кібербезпеки України. Україна співпрацює з низкою партнерів у кіберсфері. Україна була партнером у 12 спільних проектах Європейського Союзу та Ради Європи з управління кібербезпекою в Україні "Cybersecurity EAST"20, які мають регіональний вимір і включають усі країни Східного партнерства (тобто Вірменію, Азербайджан, Білорусь, Грузію, Республіка Молдова, Україна).

У сфері кіберзахисту Україна співпрацює з Трастовим фондом кіберзахисту НАТО для посилення технічних можливостей країни у протидії кіберзагрозам. Крім того, Україна стала головним бенефіціаром Програми співпраці «Наука заради миру та безпеки» (SPS – Science for Peace and Security).

Після початку повномасштабного вторгнення. Ранні рішення керівництва деяких найбільших світових технологічних і кібербезпекових компаній взяти на себе активну роль у захисті України були ключовими. Західні лідери були однозначні у судженнях що вони не будуть кидати військові сили воювати в Україні. Проте в цифровій сфері західні урядові, військові та комерційні актори безпосередньо протидіють російським зловмисникам та беруть на себе низку відповідальності за захист українських мереж і даних. Ця спеціальна коаліція протистояла інтенсивній кампанії російських кібератак.

Вторгнення створило невідкладність, яку неможливо було вирішити за допомогою програм, спрямованих на досягнення довгострокових цілей розвитку, а мобілізація державних і приватних ресурсів породила інноваційні партнерства. Наприклад, Управління закордонних справ, у справах Співдружності та розвитку Великої Британії (FCDO – UK Foreign, Commonwealth and Development Office (FCDO)) за допомогою технічних консультацій Національного центру кібербезпеки спонсорує програму, яка надає українським установам доступ до послуг комерційних компаній з кібербезпеки [2].

Іншою визначальною особливістю оборонних зусиль стала інтеграція великих американських постачальників технологій, зокрема Amazon, Cloudflare, Google і Microsoft. Здатність цих компаній переносити державні дані та сервіси України на розподілені хмарні сервери; забезпечувати автоматизований захист масивних мереж у поєднанні зі спеціальним захистом користувачів із високим ризиком; а також постійне оновлення розвідувальних даних про загрози, отриманих із глобальної телеметрії, додало глибини захисту та стійкості, що набагато перевищує ті, яких Україна могла б досягти самостійно.

Висновки

Можливо, війна в Україні не виявила готового плану колективної міжнародної оборони в кіберпросторі, але вона випробувала концепцію

співпраці багатьох зацікавлених сторін і в процесі продемонструвала п’ять ключових уроків.

1. Масштабний кіберзахист, у тому числі об’єктів критичної інфраструктури, спирається на залучення найбільших комерційних технологічних і кібербезпекових компаній.

2. Причини участі комерційних структур у захисті українського кіберпростору та об’єктів критичної інформаційної інфраструктури можуть носити характер комерційний (демонстрація можливостей і переваг), репутаційний та нормативний (захист цінностей і запобігання шкоді).

3. Компанії, що займаються технологіями та кібербезпекою, можуть бути мотивовані урядами щодо участі у міжнародному кіберзахисті.

4. Прикладом проблемного питання кіберзахисту об’єктів критичної інформаційної інфраструктури була зосереджена залежність уряду від потенційно вразливих локальних серверів. Залежність, яку потрібно було швидко виправити шляхом міграції до центрів обробки даних за межами зони бойових дій, якими зазвичай керують іноземні постачальники хмарних послуг.

Зазначений досвід вказує на те, що колективна оборона не лише демонструє свій оперативний потенціал в Україні, але й виявляє стратегічну напруженість, яку потрібно було б вирішити за допомогою будь-яких більш довготривалих домовленостей. В основі виклику для демократій лежить *інтеграція* комерційних акторів як агентів зовнішньої та оборонної політики. Таким чином, розробка *механізмів* співпраці оголить глибокі проблеми національного суверенітету, підзвітності та розподілу тягаря в кіберпросторі.

Література

1 Onishchenko S.V., Glushko A.D., Maslii O.A. (2022) Cyber resilience as the basis of Ukraine's national security. *Innovations and prospects of world science : Proceedings of XI International Scientific and Practical Conference (Vancouver, Canada, 22-24 June 2022)* – Vancouver : Perfect Publishing, 2022. – pp. 551-556. – URL: http://reposit.nupp.edu.ua/bitstream/PoltNTU/10642/1/INNOVATIONS-AND-PROSPECTS-OF-WORLD-SCIENCE-22-24.06.22-551-556.pdf

2 Microsoft warns of increased Russian hacking against allied governments. URL : https://siliconangle.com/2022/06/22/microsoft-warns-increased-russian-hacking-allied-governments/.

3 Evaluating the International Support to Ukrainian Cyber Defense. URL : https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322.

УДК 004.056.53

6.ДЕЯКІ ПРИНЦИПИ МІЖРІВНЕВОЇ СИСТЕМИ ЗАХИСТУ WEB-ДОДАТКУ

Пташкін Р.Л.[1], Палагін В.В.[2]
1 Черкаський науково-дослідний експертно-криміналістичний центр МВС України, Черкаси, Україна
2 Черкаський державний технологічний університет, Черкаси, Україна
e-mail: ndekc.ck@gmail.com, v.palahin@chdtu.edu.ua

Cross-layer web application security concept

This paper talk about some principles of protection web-applications. AS authors think, the most common problem of cybersecurity is encapsulation different layers of web-server. The system will be much more protected, when each layer has the ability to interact with each other. Server can be configurated for interaction of php with nginx or iptables. This approach will increase protection level and allow to realize security measures on each level of web-server.

Розглядаючи питання захисту web-ресурсу загалом, варто проаналізувати його складові елементи, визначити їх роль та функціональні можливості. Окрім того варто виділити найвразливіші елементи, що в подальшому дозволить ефективно побудувати систему захисту.

Фактично будь-який web-ресурс складається з web-серверу та web-додатку. Функціонально web-сервер є набором програмних засобів, що створюють середовище для виконання web-додатку. Безпосередньо web-додаток також можна розділити на дві умовні складові частини – «frontend» та «backend». Frontend – візуальна складова частина web-додатку, його інтерфейс. Backend – серверна частина web-додатку, котра реалізує його логіку та функціональність.

Звертаючись до даних «W3Techs - World Wide Web Technology Surveys» [1] можна констатувати, що найрозповсюдженішим програмним засобом, котрий застосовується для забезпечення функціонування web-серверів є «Nginx». Також розглядаючи вищенаведене джерело даних, можна констатувати, що найрозповсюдженішою мовою для створення web-додатків є PHP. В ході більш глобального аналізу також стає очевидним, що в переважній більшості випадків web-сервери в цілому функціонують під керуванням операційних систем сімейства Linux.

Якщо зіставити наведені відомості стосовно технологій, що застосовуються для створення web-серверів та функціонування web-додатків з відомостями стосовно шляхів проникнення при здійснені атак в кіберпросторі, можна побачити, що «точками входу» та подальшої компрометації системи є не що інше як вихідні коди web-додатків в деякій сукупності з некоректними налаштуваннями програмних засобів web-серверу [2,3,4]. Рівень вразливостей коливається від високого – отримання доступу до облікових даних окремих

користувачів, до критичного – можливості виконання стороннього коду на web-сервері з використанням вразливостей web-додатку.

Звернувшись до загальних принципів функціонування web-серверів типу «Nginx + PHP» не важко помітити, що фактично їхня структура складається з декількох рівнів (шарів) – запит користувача передається від одного програмного засобу до іншого доти, доки не буде сформовано відповідь. Тобто спочатку запит до серверу може оброблятися мережевим екраном чи proxy-менеджером (не завжди), потім надходить до програмного засобу nginx після чого, в залежності від запиту, передається в інтерпретатор PHP. Кожен з зазначених програмних рівнів є окремим шаром, що може сформувати відповідь на запит. Якщо властивості запиту суперечать правилам мережевого екрану, то запит буде скасовано. Аналогічно, якщо властивості запиту не відповідатимуть налаштуванням Nginx, то буде сформована та повернена відповідна відповідь й запит не буде переданий наступному рівню. Тут варто зазначити, що здійснення фільтрації ефективніше здійснювати на більш високому рівні. Тобто в разі виявлення неправомірного доступу до якоїсь з ланок web-ресурсу, найефективніше буде здійснювати безпекові заходи на рівні мережевого екрану чи web-серверу (Nginx), а не на рівні інтерпретатору.

Аналізуючи офіційну документацію що регламентує правила налаштування програмного забезпечення web-серверів, можна дійти до висновку, що зазвичай всі рівні обробки запитів є інкапсульованими один від одного та взаємодіють лише через чітко визначені інтерфейси. Такий підхід конфігурування є безсумнівно логічним, структурно вірним та захищеним. Але в разі виявлення спроби несанкціонованого доступу на рівні web-додатку, що працює в середовищі PHP, відсутній алгоритм взаємодії з вищими рівнями серверу з метою здійснення тих чи інших безпекових заходів.

Фактично завданням такої взаємодії є детальний аналіз вхідних даних не лише на різних інкапсульованих рівнях опрацювання запиту, а й на різних рівнях безпосередньо web-додатку, тобто на рівні інтерпретатору. PHP-додаток повинен на етапі фільтрації та типізації даних перевіряти їх цілісність, а разі виявлення певної нестандартної ситуації система має здійснити кваліфікацію рівня помилки – в разі підозри вторгнення здійснюються безпекові заходи. Оскільки на етапі первинної фільтрації фактично не можливо надійно та достовірно перевірити адекватність та прийнятність даних, їх додаткова фільтрація та перевірка здійснюється на кожному етапі опрацювання вхідних даних.

Завдання взаємодії між різними рівнями web-ресурсу можливо вирішити без інсталяції якогось додаткового програмного забезпечення використовуючи вже наявні функціональні можливості програмних засобів Nginx та PHP [5]. Відтак, PHP-додаток в разі виявлення підозри вторгнення та здійснення її належної кваліфікації, має створити файл-мітку, яка б чітко та однозначно ідентифікувала джерело запитів (користувача). В свою чергу програмний засіб Nginx при обробці кожного запиту перевірятиме наявність таких файлових міток з ідентифікатором користувача. В разі наявності співпадінь стосовно запиту

можливо здійснювати ті чи інші безпекові заходи, наприклад блокування IP-адреси чи перенаправлення запиту захищене середовище (так звану «пісочницю»). З огляду на досить широкі функціональні можливості Nginx, в якості ідентифікатора користувача може буде як IP-адреса, так й інші базові властивості запиту чи їх поєднання.

Окрім того, міжрівнева взаємодія не обмежується взаємодією лише програмним засобом Nginx. Функціональність мови PHP дозволяє генерувати системні логи з зазначенням будь-якої важливої інформації про запит [5,6]. такі записи в подальшому в режимі реального часу можуть аналізуватись будь-яким шаром захисту та в тих чи інших ситуаціях здійснювати безпекові заходи. Для прикладу – лог-файли можна аналізувати програмним засобом «fail2ban» й в разі виявлення відомостей про загрозу здійснювати блокування подальших запитів на рівні мережевого екрану (iptables).

Загалом запропоновані методи дозволяють реалізувати майже автономну систему захисту web-додатків, котра реагуватиме на заздалегідь визначені інциденти та автоматично здійснюватиме коригувальні чи обмежуючі безпекові заходи з метою унеможливлення ініціалізації обробки некоректних даних чи несанкціонованого доступу до окремих структурних елементів web-додатку.

Література

1. Web Technologies Statistics and Trends. W3Techs. https://w3techs.com /technologies (дата звернення: 08.03.2023);
2. Cyber Security Breaches Survey 2022 URL: https://www.gov.uk/government /statistics/cyber-security-breaches-survey-2022 (дата звернення: 08.03.2023);
3. OWASP Top Ten Web Application Security Risks. OWASP Foundation. https://owasp.org/www-project-top-ten/ (дата звернення: 08.03.2023);
4. CISA Insights. https://www.cisa.gov/insights (дата звернення: 08.03.2023);
5. D. DeJonghe, NGINX Cookbook: Advanced Recipes for High Performance Load Balancing. CA, USA: O'Reilly Media, 2019. ISBN: 978-1-491-96893-2;
6. M. Zandstra, PHP 8 Objects, Patterns, and Practice: Mastering OO Enhancements, Design Patterns, and Essential Development Tools. Brighton, UK: Apress, 2021. ISBN: 978-1-4842-6790-5

УДК 336.1 : 351.86

7.НОРМАТИВНІ АСПЕКТИ ІДЕНТИФІКАЦІЇ ТА КАТЕГОРИЗАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Савостьяненко М.В., Клименко К.В.
НДФІ ДННУ «Академія фінансового управління», м. Київ Україна
E-mail: savomax@ukr.net; klymenko_kateryna@ukr.net

Regulatory aspects of the identification and categorization of critical infrastructure facilities

The report reveals some regulatory aspects of the formation of a new system of operation and protection of critical infrastructure in Ukraine. The authors analyze the peculiarities of the legislative support for the identification and categorization of critical infrastructure objects. A new version of the Procedure for assigning objects to critical infrastructure is being studied. The new expanded list of critical infrastructure objects, approved by the Cabinet of Ministers of Ukraine, is analyzed.

Сьогодні в Україні стрімкими темпами відбувається формування нової системи функціонування і захисту критичної інфраструктури. Така система формується як на основі вивчення міжнародного досвіду, так і більшою мірою на основі реального практичного досвіду подолання вкрай тяжких пошкоджень, критичної інфраструктури від російської військової агресії. Позитивом в цьому контексті є те, що вибудована у повоєнному періоді нова система управління, функціонування, захисту критичної інфраструктури, має стати найбільш міцною, стійкою, еластичною і ефективною, враховуючи зазначений досвід.

Тим не менш, звичайно, на перших етапах побудови сучасної системи управління і захисту критичної інфраструктури відбувається формування нового законодавчого базису та відповідного нормативно-правового регулювання. Прийнятий Закон України про критичну інфраструктуру, важливі підзаконні акти, визначено державний орган, відповідальний за управління критичною інфраструктурою, проводиться класифікація секторів критичної інфраструктури тощо. В надзвичайно складних умовах діяльність органів влади, державного управління та місцевого самоврядування в цьому напрямку має на меті забезпечення максимального рівня національної безпеки і оборони.

У кожній країні наявні особливості у класифікації секторів критичної інфраструктури з урахуванням специфіки економічного та соціального їх розвитку. Перелік секторів, віднесених до критичних, затверджується нормативними документами країни, а їх складові визначаються підзаконними актами. Перелік ключових секторів критичної інфраструктури, застосовуваних у різних країнах є схожим і налічує в середньому 10-15 секторів. Але у той же час у кожної країни є певні особливості, зважаючи на географічне розташування, структуру економіки та її ключові сектори, ресурсний потенціал, спеціалізацію тощо.

Постановою Кабінету Міністрів України від 16.12.2022 р. № 1384 викладено в новій редакції Порядок віднесення об'єктів до критичної інфраструктури, затверджений постановою уряду від 09.10.2020 р. № 1109 [1]. В новій редакції викладено також Перелік секторів (підсекторів), основних послуг критичної інфраструктури держави, затверджений зазначеною постановою.

Відомості про об'єкти критичної інфраструктури, що містяться у зведеному переліку об'єктів критичної інфраструктури та секторальних переліках об'єктів критичної інфраструктури, є інформацією з обмеженим доступом, захист якої забезпечується відповідно до вимог законодавства.

Кабінет міністрів розширив перелік об'єктів критичної інфраструктури та оновив Порядок віднесення об'єктів до критичної інфраструктури. Так, відповідна урядова постанова передбачає, що до переліку додаються, зокрема, такі сектори: «Правосуддя» (перелік судів, які слід віднести до об'єктів критичної інфраструктури, уряд формуватиме на основі подання Держспецзв'язку); «Вибори та референдуми» (за перелік об'єктів у цій галузі відповідає Центральна виборча комісія); «Інформаційні послуги» (визначати ЗМІ, які зможуть стати об'єктами критичної інфраструктури, буде Міністерство культури та інформполітики); «Державна влада та місцеве самоврядування» (відповідальним органом щодо визначення таких об'єктів буде Держспецзв'язку); «Наукові дослідження та розробки» (визначати об'єкти дослідницької інфраструктури наукових установ та закладів вищої освіти, наукової діяльності, надання послуг з використання наукового обладнання буде Міносвіти); «Тримання під вартою» (критичні об'єкти у сфері тримання засуджених та осіб, взятих під варту, в установах виконання покарань та слідчих ізоляторах Державної кримінально-виконавчої служби визначить Мін'юст).

Що ж до зміни порядку віднесення до критичної інфраструктури, то оновлення передбачають, що ідентифікувати об'єкти критичної інфраструктури будуть секторальні органи (ЦВК, МКІП, МОН, Мін'юст, Держспецзв'язку тощо). Ці установи разом з оператором критичної інфраструктури здійснюють категоризацію об'єктів. Потім списки подаються до Держспецзв'язку, де перевірятиметься доцільність та коректність обрання конкретних об'єктів та формуватиметься зведений перелік об'єктів критичної інфраструктури. А вже цей документ передаватиметься на затвердження уряду [2].

Так, приміром нещодавно Наказом МОЗ України від 27.01.2023 р. № 163 утворено Робочу групу з категоризації об'єктів критичної інфраструктури, затверджено її склад та положення про неї [3]. Голові робочої групи доручено забезпечити: 1) координацію діяльності Робочої групи; 2) проведення засідання Робочої групи в разі необхідності; 3) підготовку пропозицій щодо категоризації об'єктів критичної інфраструктури у сфері охорони здоров'я; 4) інформування міністра охорони здоров'я України про результати діяльності Робочої групи; 5) дотримання вимог Примірного положення про утворення та діяльність консультативних, дорадчих та інших допоміжних органів при Міністерстві охорони здоров'я України, затвердженого наказом Міністерства охорони здоров'я України від 1 лютого 2022 р. № 202.

В умовах воєнного стану та блекаутів важливим для функціонування агропідприємств з певних напрямків виробництва є включення їх до переліку критичної інфраструктури. На сьогодні Міністерство аграрної політики та продовольства України визначено секторальним органом у сфері захисту критичної інфраструктури. Відповідно, в рамках відомства утворено робочу групу з ідентифікації та категоризації об'єктів критичної інфраструктури в секторі харчової промисловості та агропромислового комплексу, яка здійснює узагальнену нормовану оцінку рівня критичності та приймає рішення щодо кожного звернення, чи буде внесено виробника у перелік КІ [4].

З метою ідентифікації підприємства як об'єкта критичної інфраструктури, а також його категоризації, йому необхідно подати згідно з пунктом 8 розділу V Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15.01.2021 № 23 інформацію щодо:

- належності об'єкта критичної інфраструктури до певного сектору(ів) (підсектору(ів)) критичної інфраструктури;
- типу основної послуги (основних послуг), яку(і) об'єкт критичної інфраструктури надає;
- повної назви організації, форми власності, ЄДРПОУ власника (розпорядника) об'єкта критичної інфраструктури, місцезнаходження організації;
- керівника власника (розпорядника) об'єкта критичної інфраструктури (прізвище, ім'я, по батькові, номери контактних телефонів, email);
- найменування об'єкта критичної інфраструктури, фактичної адреси місцезнаходження об'єкта критичної інфраструктури;
- отримання об'єктом критичної інфраструктури основних послуг від інших об'єктів критичної інфраструктури, ненадання яких вплине на функціонування об'єкта критичної інфраструктури;
- надання об'єктом критичної інфраструктури основних послуг іншим об'єктам критичної інфраструктури, ненадання яких вплине на функціонування інших об'єктів критичної інфраструктури;
- рівнів негативного впливу, які особа, суспільство, навколишнє природне середовище, економіка, національна безпека та обороноздатність країни можуть зазнати внаслідок порушення або припинення функціонування об'єкта критичної інфраструктури відповідно до критеріїв, зазначених у дод. 1 і 2 до Методики [5].

Зареєстровано Проект Закону про внесення зміни до статті 8 Закону України "Про критичну інфраструктуру" (щодо врегулювання спорів, предметом яких є право власності держави на об'єкти критичної інфраструктури, що перебувають у державній власності) № 8316 від 28.12.2022 р. [6].

Література

1. Постанова КМУ від 16 грудня 2022 р. № 1384 Про внесення змін до постанови Кабінету Міністрів України від 9 жовтня 2020 р. № 1109. URL:

https://www.kmu.gov.ua/npas/pro-vnesennia-zmin-do-postanovy-kabinetu-ministriv-ukrainy-vid-9-zhovtnia-2020-r-1109-1384-161222
2. Уряд змінив Порядок віднесення до критичної інфраструктури / Кадровик-01. URL:https://prokadry.com.ua/news/60144-perelik-obektiv-kritichnoi-infrastrukturi-shcho-zminiv-kabmin»
3. Про Робочу групу по категоризації об'єктів критичної інфраструктури: Наказ МОЗ України від 27.01.2023 р. № 163. URL: https://moz.gov.ua/uploads/8/43370-dn_163_27012023.pdf
4. Оприлюднено деталі щодо включення до переліку критичної інфраструктури. URL: https://agronews.ua/news/oprylyudneno-detali-shhodo-vklyuchennya-do-pereliku-krytychnoyi-infrastruktury/
5. Мінагрополітики розпочало збір заявок з метою фіксації об'єктів критичної інфраструктури, важливих для продовольчої безпеки, - Денис Башлик. URL https://minagro.gov.ua/news/minagropolitiki-rozpochalo-zbir-zayavok-z-metoyu-fiksaciyi-obyektiv-kritichnoyi-infrastrukturi-vazhlivih-dlya-prodovolchoyi-bezpeki-denis-bashlik
6. Проект Закону про внесення зміни до статті 8 Закону України "Про критичну інфраструктуру" (щодо врегулювання спорів, предметом яких є право власності держави на об'єкти критичної інфраструктури, що перебувають у державній власності) № 8316 від 28.12.2022. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=75392

УДК 621.313

8.АВАРІЙНІ СИТУАЦІЇ ТУРБОГЕНЕРАТОРІВ ТЕС ТА ШЛЯХИ ЇХ ПОПЕРЕДЖЕННЯ

Тарнавський А.Б.
Львівський державний університет безпеки життєдіяльності
E-mail: andry090880@ukr.net

Emergency situations of turbogenerators of thermal electric plants and ways of preventing them

The main emergency situations that arise during the operation of turbogenerators of thermal power stations with a hydrogen cooling system are given. The cause of emergency situations is the violation of requirements for the operation of the turbogenerator and hydrogen leaks due to leaks in the pipeline system and sealing materials. The main ways to prevent emergency situations are compliance with the requirements of technological regulations and the correct sequence of releasing equipment from combustible substances.

Завдяки власній високій теплопровідності і теплоємності газоподібний водень широко застосовується в якості охолоджуючого середовища у турбогенераторах енергоблоків як теплових електричних станцій (ТЕС), так і на атомних електричних станціях. Охолодження турбогенераторів воднем є більш ефективним, порівняно з повітряним. Це зумовлено тим, що коефіцієнт теплопередачі водню, порівняно з повітрям, є у 1,5 рази більшим, а теплопровідність – у 7 разів вища. Крім того, використання водню у системі охолодження обмоток турбогенератора, порівняно з повітрям, не призводить до окислення ізоляції електричних проводів. Проте, основним недоліком водневого охолодження турбогенераторів вважається здатність водню утворювати з повітрям та парами масла вибухонебезпечні суміші.

При порушенні вимог технологічного регламенту і тривалому контакті поверхнево-активного водню з конструкційними матеріалами устаткування бабітові підшипники та деталі ротора можуть піддаватися водневій корозії [1] (вид деградації металевого матеріалу, що спричинена проникненням та нагромадженням у металі атомів водню).

Зміна з часом експлуатаційних властивостей конструкційних матеріалів, а також можливі витоки водню через ущільнення турбогенератора можуть призвести до перевищення гранично допустимої концентрації водню у повітрі машинного залу. При цьому підвищується ймовірність вибуху горючої воднево-повітряної суміші з утворенням потужної вибухової хвилі та можливістю виникнення катастрофічних наслідків.

Додаткова небезпека вибуху водню у суміші з повітрям, азотом або киснем виникає від електричних іскор або відкритого полум’я.

У машинних залах ТЕС різноманітні загоряння водню викликані, в основному, порушенням щільності технологічного устаткування та водневопідвідних і відвідних комунікацій (трубопроводів). Значну частину “хлопків” водню у газо-масляних системах турбогенераторів зазвичай не фіксують у звітних документах у випадку, якщо вони не призводять до виникнення вибухів, пожеж та травмувань обслуговуючого персоналу.

У суміші з повітрям водень може накопичуватися під обшивкою турбогенератора, в результаті чого можуть виникати локальні вибухи горючої воднево-повітряної суміші з наступним пошкодженням чи руйнуванням обшивки апарата [2].

Під час неповного витіснення водню вуглекислим газом з турбогенератора при проведенні планово-попереджувального ремонту і наступним заповненням корпусу апарата повітрям можливі “хлопки” воднево-повітряної суміші. Найбільш часто такі “хлопки” виникають під час проведення ремонтних зварювальних робіт на трубопроводах системи охолодження.

Водень, що подається на заповнення у турбогенератори, у суміші з повітрям (від 4,1 до 74 %, а в присутності парів масла – від 3,3 до 81,5 %), може утворювати вибухонебезпечні суміші. Тому у турбогенераторів з водневим охолодженням повинна бути забезпечена висока газощільність корпусу статора масляними ущільненнями валу, ущільнення струмопроводів до обмоток статора

і ротора, ущільнення кришок газоохолоджувачів, люків і знімних торцевих щитів. Найбільш складно виконати надійні масляні ущільнення валу генератора, що перешкоджають витоку газоподібного водню.

Серед причин виникнення аварійних ситуацій з витоком водню, що призводять до зупинки і виходу ладу технологічного устаткування газо-масляної системи турбогенератора, можна виділити такі основні:

– витікання водню через фланцеві з'єднання трубопроводів;

– витискання ущільнюючих матеріалів або гумових прокладочних матеріалів у місцях кришки люка, біля фланців корпуса турбогенератора з наступним можливим займанням водню;

– витікання водню через поплавковий гідрозатвор з наступним займанням або "хлопком" у зливних маслопроводах підшипників;

– витікання і наступне самозаймання водню при різкому відкриванні вентиля на газовому пості;

– витікання водню через гумові прокладочні матеріали системи газового охолодження;

– витікання або прорив водню через картери підшипників турбогенератора з наступним можливим спалахуванням або "хлопком" у картерах підшипника внаслідок дефектів вкладиша ущільнювача;

– витікання водню через зварні з'єднання трубопроводів і комунікацій;

– витікання водню через горизонтальні роз'єми торцевих щитів;

– витікання водню порушення роботи регуляторів перепаду тиску водню і масла, регуляторів надлишкового тиску масла.

Наявність у системах водневого охолодження турбогенератора горючого водню у суміші з маслом утворює проблему щодо забезпечення прийнятного рівня вибухо- і пожежобезпеки у машинному залі ТЕС. В основному вибухонебезпечне середовище з водню та парів масла може утворюватися в місцях ущільнення водню маслом, а також у прилеглих вузлах у випадку виникнення аварійних ситуацій із витоком водню.

Однією з основних причин аварійних зупинок та руйнувань вузлів турбогенераторів з водневим охолодженням також є інтенсивне забруднення холодоагента-водню вологою з домішками кисню, оксидів вуглецю або азоту, турбінного масла [3]. При підвищенні вказаних забруднюючих речовин у водні пожежовибухонебезпека займання і вибуху водню у генераторі суттєво зростає.

Основними забруднюючими домішками, що можуть потрапити під корпус турбогенератора, є вода (максимальна концентрація 25-30 г/м3), турбінне масло (5,0 г/м3), кисень (0,2 г/м3), воднево-масляний аерозоль (0,15 г/м3).

Під час експлуатації газо-масляної системи турбогенераторів необхідно запобігати утворенню вибухонебезпечної газової суміші не допускаючи:

– вмісту водню у струмопроводах турбогенератора більше, ніж 1 % об., а у картерах підшипників більше, ніж 2 % об.;

– вмісту кисню у водні у корпусі турбогенератора більше, ніж 1,2 % об., а у поплавковому затворі, бачку продування та водневовіддільному баці маслоочисного пристрою більше, ніж 2 % об.

В масляному баці турбогенератора не повинно бути водню.

Витискати з генератора водень або повітря необхідно інертним газом, мінімальна концентрація якого після закінчення витиснення визначається на виході із корпусу машини і повинна становити:

• вуглекислого газу – 85 % об. у разі витиснення повітря і 95 % об. у разі витиснення водню;

• азоту – 97 % об. у разі витиснення повітря і водню.

Для турбогенераторів з водневим охолодженням повинна передбачатися система автоматичного викиду водню з корпусу турбогенератора за межі машинного залу [4]. Пропускна здатність системи і необхідна її швидкодія повинна визначатися розрахунковим способом виходячи із необхідності зниження тиску водню до 1,0 атм. за час 20 с, що визначається допустимою тривалістю теплової дії горючого факела водню на несучі конструкції покриття машинного залу. Трубопровід для аварійного скидання водню з корпуса турбогенератора виводиться в атмосферу на 2,0 м вище за позначку покрівлі машинного залу [5].

Перед розкриванням корпусів турбогенераторів та апаратів газо-масляної системи водень повинен бути витиснений інертним газом, а інертний газ – повітрям. Відкривати торцеві щити, люки тощо дозволяється тільки після того, як аналіз підтвердить відсутність вуглекислого газу або (у разі витиснення азоту) достатній вміст кисню у повітрі (не менше, ніж 20 % об.).

У разі виведення в ремонт обладнання та трубопроводів газо-масляної системи необхідно від’єднати трубопроводи або встановити заглушки для виключення можливості проникнення водню або інертного газу на ділянки, що ремонтуються, через нещільність засувок.

Роботи з відкритим вогнем (електрозварювання, газове зварювання, різання тощо) на відстані менше 10 м від тих частин газо-масляної системи, що містять всередині водень, необхідно виконувати лише за нарядом. У цьому разі в рядку наряду “Окремі вказівки” потрібно записати додаткові заходи, що створюють безпечні умови виконання роботи (встановлення щитів-екранів, перевірка повітря у приміщенні на відсутність водню, наявність засобів пожежогасіння тощо).

Забороняється виконувати вогневі роботи безпосередньо на корпусі турбогенератора, трубопроводах та апаратах газо-масляної системи, що заповнені воднем.

Висновки

Основною причиною виникнення аварійних ситуацій і значних аварій при експлуатації турбогенераторів ТЕС є порушення регламентних норм експлуатації технологічного устаткування, зокрема вимог правил пожежної та техногенної безпеки, порушення цілісності воднево-вмісного обладнання.

Найбільш ймовірною причиною порушення герметичності турбогенераторної установки та комунікацій з наявністю водню є корозійне зношення основного металу та елементів устаткування.

Основними факторами пожежо- і вибухонебезпеки турбогенераторів є використання значної кількості горючих речовин і матеріалів, значний тиск турбінного масла у системах регулювання, значна довжина масляних і водневих комунікацій, складна система регулювання і захисту, підвищена температура паропроводів і корпусу турбіни, складність забезпечення газощільності турбогенератора.

Запобігання витокам і проривам водню з газо-масляної системи повинно забезпечуватися, в основному, високою якістю проведення ремонтних робіт на вузлі ущільнень та на системі постачання турбінного масла до турбогенераторної установки.

Література

1. Пособие для изучения Правил технической эксплуатации электрических станций и сетей (электрическое оборудование) / Под общ. ред. Ф.Л. Когана. – М.: Изд-во ЭНАС, 2002. – 356 с.
2. Жаров А.П., Беликова Н.З., Келлер В.Д., Ржезников Ю.В., Комаров В.А. Противопожарная система для турбоагрегатов энергоблоков ТЭС // Электрические станции. – М.: Энергопрогресс, 2001. – № 6. – С. 43-46.
3. Kempsell I.D., et al. Hydrogen Explosions – an Example of Hazard Avoidance and Control, IChemE, Symp. Series. № 148, 2001. – P. 523-539..
4. ВБН В.1.11-034-2003 “Протипожежні норми проектування атомних електростанцій з водо-водяними енергетичними реакторами” (НАПБ 03.005-2002, ГНД 34.03.307-2004, ВБН В.1.1-034-03.307).
5. Наказ Міністерства енергетики та вугільної промисловості України 26.09.2018 № 491 “Правила пожежної безпеки в компаніях, на підприємствах та в організаціях енергетичної галузі України”.

УДК 351.861

9.РОЗВИТОК СИСТЕМИ ПІДТРИМКИ АНКРИЗОВИХ РІШЕНЬ В УМОВАХ УВЕДЕННЯ ПРАВОВОГО РЕЖИМУ ВОЄННОГО ЧИ НАДЗВИЧАЙНОГО СТАНУ

Тютюник В. В.[1], Ященко О. А.[1], Тютюник О. О.[2]

1 Національний університет цивільного захситу України, Харків, Україна
2 Харківський національний економічний університет імені Семена Кузнеця, Харків, Україна
E-mail: tutunik.vadim.72@gmail.com, malahay@ukr.net, tutunik.o@ukr.net

Development of a system for supporting the adoption of anti-crisis decisions in the context of the introduction of the legal regime of military or state of emergency

In order to further develop the scientific and technical foundations for creating an information and analytical subsystem for managing the processes of preventing and eliminating emergencies in the Unified State Civil Protection System, the paper considers the features of the functioning of situational centers at various stages of the development of emergencies, as well as the features of substantiation by experts of anti-crisis decisions regarding the functioning public authorities, local governments, governments and civil protection forces to ensure an appropriate level of safety for the life of the population and the territory of the state.

Національна безпека України як інтегральне явище, охоплює політичну, економічну, державну, соціальну, інформаційну, економічну, гуманітарну, військову, цивільну, пожежну, екологічну та інші види безпеки [1].

Нормативно-правова основа функціонування системи національної безпеки України та її підсистем побудована на підставі Конституції України, законів України «Про основи національної безпеки України», «Про оборону України», «Про правовий режим воєнного стану», «Про правовий режим над звичайного стану», «Про демократичний і цивільний контроль над Воєнною організацією і правоохоронними органами держави», затверджена Указом Президента України відповідно до положень Закону України «Про основи національної безпеки України» Стратегія національної безпеки 2015 року, інших законів і нормативно-правових актів, а також на підставі визнаних Україною договорів та угод.

У разі виникнення в Україні чи на окремих її місцевостях надзвичайної ситуації (НС) техногенного або природного характеру не нижче загальнодержавного рівня, що призвели чи можуть призвести до людських і матеріальних втрат, а також створюють загрозу життю і здоров'ю громадян, або при спробі захоплення державної влади чи зміни конституційного ладу України шляхом насильства Указом Президента України (який підлягає затвердженню Верховною Радою України) може тимчасово вводитися правовий режим надзвичайного стану [2].

Надзвичайний стан в Україні або в окремих її місцевостях передбачає надання відповідним органам державної влади, військовому командуванню та органам місцевого самоврядування відповідно до цього Закону повноважень, необхідних для відвернення загрози та забезпечення безпеки і здоров'я громадян, нормального функціонування національної економіки, органів державної влади та органів місцевого самоврядування, захисту конституційного ладу, а також допускає тимчасове, обумовлене загрозою, обмеження у здійсненні конституційних прав і свобод людини і громадянина та прав і законних інтересів юридичних осіб із зазначенням строку дії цих обмежень.

В сучасній історії незалежної України прецедент виник 23 лютого 2022 року. Президент держави видає Указ № 63/2022 "Про введення надзвичайного стану в окремих регіонах України". Причиною стає визнання 21 лютого 2022 року керівництвом Російської Федерації незалежність

самопроголошених "ЛНР" і "ДНР" та прийняття рішення щодо введення на тимчасово окуповані території Донецької та Луганської областей підрозділів збройних сил Російської Федерації.

Такі дії є продовженням політики Російської Федерації щодо ескалації збройної агресії проти України, нав'язування сепаратизму, провокування міжнаціональних і міжконфесійних конфліктів, масових безпорядків, що загрожує безпеці, життю і здоров'ю громадян, державному суверенітету, конституційному ладу та територіальній цілісності України.

Підривна діяльність спеціальних служб Російської Федерації, підтримувана нею діяльність сепаратистських сил, кримінальних та незаконних військових угруповань на окупованих територіях Донецької та Луганської областей, здійснення ними терористичної діяльності набули характеру збройного протистояння і загрожують поширенню на інші регіони України.

У разі збройної агресії чи загрози нападу, небезпеки державній незалежності України та її територіальній цілісності Указом Президента України (який підлягає затвердженню Верховною Радою України) може тимчасово вводитися правовий режим воєнного стану [3].

Воєнний стан в Україні або в окремих її місцевостях передбачає надання відповідним органам державної влади, військовому командуванню, військовим адміністраціям та органам місцевого самоврядування повноважень, необхідних для відвернення загрози, відсічі збройної агресії та забезпечення національної безпеки, усунення загрози небезпеки державній незалежності України, її територіальній цілісності, а також тимчасове, зумовлене загрозою, обмеження конституційних прав і свобод людини і громадянина та прав і законних інтересів юридичних осіб із зазначенням строку дії цих обмежень.

Вперше рішення щодо запровадження воєнного стану у 10 областях України з 26 листопада 2018 року на 30 днів було прийнято 26 листопада 2018 року у зв'язку з актом збройної агресії Російської Федерації у районі Керченської протоки проти кораблів Військово-Морських Сил Збройних Сил України, наявною загрозою широкомасштабного вторгнення в Україну збройних сил Російської Федерації.

24 лютого 2022 року у зв'язку з військовою агресією Російської Федерації проти України Указом Президента України № 64/2022 введено воєнний стан із 05 години 30 хвилин 24 лютого 2022 року строком на 30 діб.

Згодом строк дії воєнного стану в Україні продовжено: з 05 години 30 хвилин 26 березня 2022 року строком на 30 діб згідно з Указом Президента № 133/2022 від 14.03.2022; з 05 години 30 хвилин 25 квітня 2022 року строком на 30 діб згідно з Указом Президента № 259/2022 від 18.04.2022; з 05 години 30 хвилин 25 травня 2022 року строком на 90 діб згідно з Указом Президента № 341/2022 від 17.05.2022; з 05 години 30 хвилин 23 серпня 2022 року строком на 90 діб згідно з Указом Президента № 573/2022 від 12.08.2022; з 05 години 30 хвилин 21 листопада 2022 року строком на 90 діб згідно з Указом Президента № 757/2022 від 07.11.2022; з 05 години 30 хвилин 19 лютого 2023 року строком на 90 діб згідно з Указом Президента № 58/2023 від 06.02.2023.

У зв'язку із введенням в Україні воєнного стану Державна служба України з надзвичайних ситуацій (ДСНС) невідкладно разом з обласними, Київською міською державними адміністраціями, іншими державними органами, установами, підприємствами, організаціями всіх форм власності привела єдину державну систему цивільного захисту (ЄДСЦЗ), її функціональні та територіальні підсистеми у готовність до виконання завдань за призначенням в особливий період.

Заходи з ліквідації наслідків НС, пожеж та небезпечних подій на території України здійснюються силами цивільного захисту, у тому числі підрозділами Оперативно-рятувальної служби цивільного захисту, із залученням органів Національної поліції України та підрозділів Національної гвардії України відповідно до покладених на них завдань.

Безпосередня організація та координація робіт з ліквідації наслідків надзвичайних ситуацій, пожеж та небезпечних подій здійснюються шляхом: обмін інформацією про загрозу або виникнення надзвичайних ситуацій, пожеж та небезпечних подій у різних регіонах країни; проведення спільних оперативних нарад Голови ДСНС або його заступників з Головою (заступниками) Національної поліції України та Командувачем (заступниками) Національної гвардії України, керівників територіальних органів ДСНС з керівниками територіальних (у тому числі міжрегіональних) органів Національної поліції України та оперативно-територіальних об’єднань Національної гвардії України; здійснення спільних заходів за планами взаємодії органів управління та сил цивільного захисту в разі виникнення надзвичайної ситуації, що розробляються на регіональних і місцевих рівнях; проведення спільних навчань та тренувань; здійснення інших заходів.

Одним з перспективних напрямків розвитку інформаційно-аналітичного забезпечення прийняття управлінських рішень, взаємодії, координації і контролю за діяльністю органів виконавчої влади, правоохоронних органів та військових формувань у сферах національної безпеки і оборони у мирний час, а також в особливий період, у тому числі в умовах воєнного стану, в умовах надзвичайного стану та під час виникнення кризових ситуацій, що загрожують національній безпеці України, є створення та розширення єдиної мережі ситуаційних центрів, до складу якої мають входити Головний ситуаційний центр України, Урядовий ситуаційний центр, ситуаційні центри органів сектору безпеки і оборони, ситуаційні центри центральних органів виконавчої влади, Ради міністрів Автономної Республіки Крим, обласних, Київської та Севастопольської міських державних адміністрацій, а також резервні та рухомі ситуаційні центри [4].

Спираючись на цю перспективу, авторами у роботах [5, 6] запропоновано створення ефективної інформаційно-аналітичної підсистеми управління процесами попередження й локалізації наслідків НС шляхом комплексного включення в діючу систему ЄДСЦЗ по вертикалі від об’єктового до державного рівнів різних функціональних елементів територіальної системи моніторингу НС та складових системи ситуаційних центрів, які жорстко пов’язані між собою на

інформаційному та виконавчому рівнях для прийняття відповідних антикризових рішень для розв’язання різних функціональних задач моніторингу, попередження та ліквідації НС природного, техногенного, соціального та воєнного характеру.

Показано, що основною функцією системи ситуаційних центрів на всіх рівнях управління ЄДСЦЗ є збір й обробка фактичної інформації, прогнозування ризику виникнення різного роду НС та розробка ефективних антикризових рішень. Процедура прийняття управлінських рішень ускладнюється тим, що необхідними умовами ефективності рішень є їх своєчасність, повнота й оптимальність. Тому, підвищення ефективності прийнятих рішень пов'язане з необхідністю рішення задачі багатокритеріальної оптимізації в умовах невизначеності, що потребує розробки формальних, нормативних методів і моделей комплексного рішення проблеми прийняття рішень в умовах багатокритеріальності й невизначеності при управлінні процесами попередження й локалізації наслідків НС для забезпечення ефективного функціонування ЄДСЦЗ.

Література

1. Постанова Верховної Ради України від 16 січня 1997 р. № 569-р «Про Концепцію (основи державної політики) національної безпеки України».
2. Закон України «Про правовий режим надзвичайного стану» від 16 березня 2000 року № 1550-III.
3. Закон України «Про правовий режим воєнного стану» від 12 травня 2015 року № 389-VIII.
4. Рішення Ради національної безпеки і оборони України від 4 червня 2021 року «Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони», Введено в дію Указом Президента України від 18 червня 2021 року № 260/2021.
5. Рубан І.В., Тютюник В.В., Тютюник О.О. Особливості створення системи підтримки прийняття антикризових рішень в умовах невизначеності вхідної інформації при надзвичайних ситуаціях. Науковий журнал "Сучасні інформаційні технології у сфері безпеки та оборони". Київ: Національний університет оборони України імені Івана Черняховського. 2021. №1(40). С. 75–84.
6. Тютюник В.В., Ященко О.А., Рубан І.В., Тютюник О.О. Особливості функціонування системи ситуаційних центрів на різних стадіях розвитку надзвичайних ситуацій. Науковий журнал "Сучасні інформаційні технології у сфері безпеки та оборони". Київ: Національний університет оборони України імені Івана Черняховського. 2022. Вип. 1(43). С. 41–52.

УДК 004.056

10.ПІДХОДИ ДО ПОБУДОВИ ЗАВАДОСТІЙКОГО ПЕРЕСТАНОВОЧНОГО КОДУ ДЛЯ НЕРОЗДІЛЬНОГО ФАКТОРІАЛЬНОГО КОДУВАННЯ ДАНИХ

Фауре Е.В.[1], Махинько М.В.[2]
1 Черкаський державний технологічний університет, Черкаси, Україна
ГО «Інститут дослідження кіберпростору»
2 GoodLabs Studio Inc., Toronto, ON M5H 3E5, Canada
E-mail: e.faure@chdtu.edu.ua

Approaches to construct error-correcting permutation code for non-separable factorial data coding

The report highlights approaches to construct error-correcting permutation code in the context of its use in integrated data protection systems against channel errors and unauthorized access based on non-separable factorial coding. The use of affine and projective general linear groups to form an ensemble of permutations, in addition to providing a given code distance for permutation dictionaries (arrays), allows generating network and session keys during secure data exchange. The statistical approach to construct permutation code is based on enumerating permutations and selecting those permutations, which distance does not exceed a given value to all previously selected codewords.

Передавання коротких пакетів є ключовою особливістю сучасних бездротових систем, наднадійних і сенсорних мереж, масових комунікацій машинного типу (МТС), IoT застосувань. Поширеність таких систем і мереж у сучасному світі вимагає створення нових і адаптацію існуючих підходів до забезпечення цілісності та конфіденційності переданої інформації. Зокрема, потужність необхідних ресурсів для канального кодування та криптографічного захисту, а також їх швидкодія відіграють подекуди визначальну роль.

Ця робота розглядає підходи до побудови завадостійких перестановочних кодів [1, 2] у контексті використання їх у системах інтегрованого захисту інформації від помилок каналу зв'язку та несанкціонованого доступу на основі нероздільного факторіального кодування даних [3, 4]. Такі перестановочні коди можуть бути використані, зокрема, з метою формування ансамблю кодових символів факторіального коду для інформаційної взаємодії об'єктів МТС з динамічно змінюваною структурою, а також забезпечення надійного передавання перестановок у складних завадових умовах, утому числі, для трьохетапного криптографічного протоколу на основі перестановок [5].

Множину перестановок на Z_M будемо називати масивом перестановок [6] і позначати через S_M. Відстань між перестановками $\pi_i, \pi_j \in S_M$ будемо позначати

через D_{ij}. Тоді завадостійким перестановочним кодом є (M, D_{min}) є код, утворений підмножиною перестановок масиву S_M, де попарна відстань між перестановками π_i, π_j цієї підмножини задовольняє нерівності $D_{ij} \geq D_{min}$. Потужність коду (M, D_{min}) позначимо через $N(M, D_{min})$.

Спершу розглянемо алгоритми формування кодів $(M, M-1)$ і $(M+1, M-1)$ з простим M для досягнення $N(M, M-1) = M(M-1)$ і $N(M+1, M-1) = (M+1)M(M-1)$.

Код $(M, M-1)$ утворюється афінною загальною лінійною групою $AGL(1, M) = \{ax + b | a, b, x \in GF(M), a \neq 0\}$ [6] і з простим M породжується будь-яким елементом (перестановкою) цього коду, тобто якщо $S_M = \{ax + b, a, b \in Z_M, a \neq 0\}$ і $\sigma \in S_M$, то $\{a\sigma_x + b, a, b \in Z_M, a \neq 0\} = S_M$.

Код $(M+1, M-1)$ утворюється проективною загальною лінійною групою $PGL(2, M) = \left\{ f(x) = \frac{ax+b}{cx+d} \middle| a, b, c, d \in GF(M), x \in GF(M) \bigcup \infty, ad \neq bc \right\}$ [6] і з простим M породжується будь-яким елементом (перестановкою) цього коду, тобто якщо $S_{M+1} = \left\{ f(x) = \frac{ax+b}{cx+d} \middle| a, b, c, d \in Z_M, x \in Z_M \bigcup \infty, ad \neq bc \right\}$ і $\sigma \in S_{M+1}$, то $\left\{ f(x) = \frac{a\sigma_x + b}{c\sigma_x + d} \middle| a, b, c, d \in Z_M, ad \neq bc \right\} = S_{M+1}$.

Застосування афінної та проективної загальної лінійної груп для формування алфавіту повідомлень (перестановок), окрім забезпечення кодової відстані $M-1$ для словників (масивів) перестановок S_M і S_{M+1}, дозволяє формувати мережні та сеансові ключі під час захищеного обміну даними.

Статистичний підхід [7] до формування (M, D_{min})-коду та оцінювання його потужності $N(M, D_{min})$ базується на переборі множини перестановок $\{\pi\}$ довжини M і відбору тих перестановок, відстань від яких не перевищує значення D_{min} до всіх відібраних до цього кодових слів.

Для забезпечення можливості побудови коду (M, D_{min}) за значень M, для яких реалізувати практично формування $M!$ перестановок неможливо, початкова множина перестановок представляє собою деяку власну підмножину потужності N_{lim} повної множини з $M!$ перестановок.

Експериментально визначені залежності середнього та максимального значень потужності $N(M, D_{min}, N_{lim})$ коду (M, D_{min}), утвореного за підмножиною

з N_{lim} перестановок, від значення N_{lim}, а також методика побудови апроксимаційних квадратичних поліномів для визначених залежностей можуть бути використані для екстраполяції цих залежностей і прогнозування їх поведінки.

Література

1. Blake I. Permutation codes for discrete channels / I. Blake // IEEE Trans. Inf. Theory. – 1974. – Issue 20, No. 1. – P. 138–140.
2. Smith D. H. A new table of permutation codes / D. H. Smith, R. Montemanni // Des. Codes Cryptogr. – 2012. – Issue 63, No 2. – P. 241–253.
3. Faure E. V. Factorial coding with data recovery / E. V. Faure // Visnyk Cherkaskogo Derzhavnogo Tehnol. Univ. – 2016. – No. 2. – P. 33–39.
4. Faure E. V. Factorial coding with error correction / E. V. Faure // Radio Electron. Comput. Sci. Control. – 2017. – Issue 3. – P. 130–138.
5. Shcherba A. Three-Pass Cryptographic Protocol Based on Permutations / A. Shcherba, E. Faure, O. Lavdanska // 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT). – Kyiv, Ukraine : IEEE, 2020.
6. Mojica de la Vega L. G. Permutation Arrays with Large Hamming Distance / L. G. Mojica de la Vega. – The University of Texas at Dallas, 2017. – 106 p.
7. Faure E. Permutation-Based Block Code for Short Packet Communication Systems / E. Faure, A. Shcherba, M. Makhynko, B. Stupka, J. Nikodem, R. Shevchuk // Sensors. – 2022. – Issue. 22, No. 14, 5391.

УДК 336.74

11.АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ ІНФОРМАЦІЇ В СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ І МЕРЕЖАХ

Хохлачова Ю. Є.[1], Гаврилова А. А.[2]

1 Національний авіаційний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна

2 Національний технічний університет «Харківський політехнічний інститут», Харків, Україна

E-mail: yuliiahohlachova@gmail.com, sharaya1972@gmail.com

Analysis of information security threats in modern information and communication systems and networks

Threats to information security and the consequences of their implementation in the form of cyberattacks were analyzed, and attractive directions for cybercriminals by sphere of activity were clarified. The dynamics of changes in the activity of cybercriminals are considered. As a result, it

was found that it is related to the intensification of shelling of strategic civilian objects. Based on the results of the analysis by types of attacks, a rating of cyberattacks on state bodies was created..

Найбільша частка злочинів, які вчиняються за допомогою Інтернет-мереж приходиться на державний і фінансовий сектор. До передових інформаційних технологій сьогодення проявляється інтерес не тільки із наукової зацікавленості чи у пошуках вирішення найважливіших задач людства, а й через пошук шляхів швидкого збагачення за рахунок фізичних осіб, різного рівня бізнес-структур, для проведення дистанційного шпіонажу та для нанесення збитків через несанкціоноване отримання доступу до критично важливої інфраструктури, даних, а також спотворення та крадіжки інформації.

Якщо досліджувати виток банківського сектору, то можна відмітити, що в останнє десятиріччя було значно розширено спектр послуг завдяки використанню обчислювальних ресурсів Інтернет-технологій та технологій X“G“–LTE (Long-Term Evolution). Дані зміни визначили введення поняття цифрової економіки та подальший розвиток електронного банкінгу [1, 2].

До 24 лютого 2022 р. більшість кібератак була спрямована на державний сектор. На сьогодні загальна їхня кількість зросла в десятки разів. За даними Держспецзв’язку [3] основні кібератаки з початком бойових дій припали на стратегічні та критичні сфери. Наслідки кібератак за привабливими для злочинців за стратегічними сферами діяльності наведені на рис. 1.

Рис. 1. Схема взаємозв’язку наслідків кібератак за стратегічними сферами діяльності

З наведеної схеми видно як впливають кібератаки на критичні та стратегічні сфери життя українського суспільства.

Так, при дезінформуванні та сіянні паніки, люди втрачають змогу отримувати перевірену офіційну інформацію як від органів державного управляння, так і від органів безпеки і оборони.

Викрадання грошей у фінансовій сфері призводить до припинення фінансування, а саме впливає на податки, пенсії , заробітну плату та субвенції.

Що стосується енергетичного сектору, логістичних вузлів та транспорту, то це як дестабілізація роботи самих систем, так й неможливість надавати та отримувати послуг та сервіси для користувачів.

Якщо до повномасштабного вторгнення кіберзлочинці зосереджувались на атаках центральної влади, медіа і військових, то після вторгнення – це також й цивільні об’єкти, до яких має відношення й критична інфраструктура. (енергетики, транспорту, зв’язку), без якої люди не можуть нормально жити [3].

За статистикою на державний сектор з початку військової агресії значно збільшилася кількість кібератак (рис. 2).

Згідно із наведеною діаграмою найбільша кількість кібератак припала на травень та липень 2022р., що пов'язано із загостренням бойових дій.

Станом на 3 квартал 2022 р. розподіл кібератак на держоргани за категоріями наведено на рис. 3.

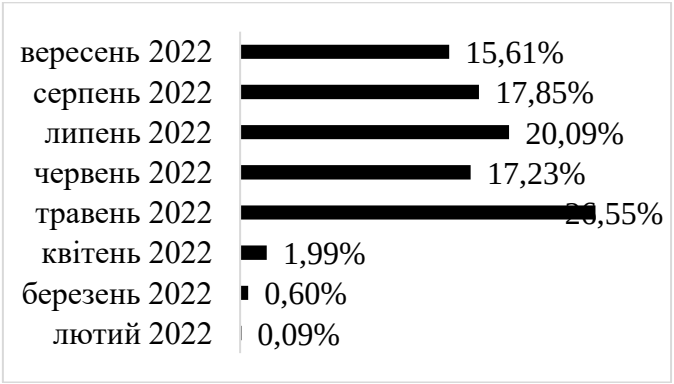


Рис. 2. Динаміка кількості атак на державний сектор України (частка атак від загальної кількості за лютий – вересень 2022 р.)

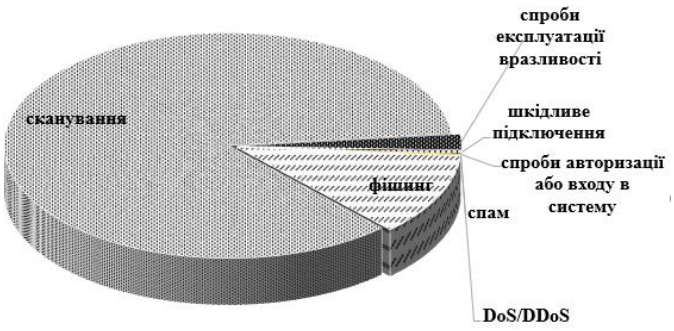


Рис. 3. Розподіл кібератак на держоргани за категоріями (за лютий – вересень 2022 р.)

За наведеною діаграмою видно, що найбільшу частину складають найпоширеніший тип кібератак – сканування [4 – 6], тобто збір інформації про систему і мережі шкідливим програмним забезпеченням. Це зчитування паролів, листування, встановлених додатків із доступами, активності в мережі і відвідування сайтів: усього, що мало би бути як приватною справою користувача, так і комерційною таємницею підприємства чи установи.

На другому місці – фішинг-атаки [4 – 6] на державний сектор, який представляє собою розсилку електронних листів чи повідомлень зі шкідливою програмою, відкриття яких або перехід за долученим посиланням загрожує втратою даних, зараженням вірусами, передачею персональних даних (паролі, дані банківських карток), втратою доступу до мережі.

На третьому місці – спроби експлуатації вразливості [4 – 6], які представляють собою спроби вторгнення з використанням вразливості у системі, компоненти чи мережі.

На четвертому місці – шкідливе підключення [4 – 6], тобто спроби з’єднання від або до IP/URL-адреси, пов'язаної з відомим шкідливим програмним забезпеченням. До таких підключень має місце C2C або приєднання до ресурсу розповсюдження компонентів, пов’язаних із активністю певної бот-мережі.

На п’ятому місці – спроби авторизації або входу в систему [4 – 6], яка полягає у спробі входу до служб або механізмів доступу, невдала спроба підбору автентифікаційних даних чи використання раніше скомпрометованих вже не актуальних даних.

На шостому місці – атаки на відмови в обслуговуванні DoS/DDoS [4 – 6], сенс яких у впливі на нормальну роботу системи чи сервісу, що досягається скеруванням з одного чи багатьох джерел до цільового ресурсу запитів для перенасичення пропускної здатності чи системних ресурсів.

На сьомому місці – спам [4 – 6], що стосується надсилання небажаних повідомлень або великої кількості повідомлень.

З врахуванням обставин, що склалися, безпека об'єктів критичної інфраструктури виходить на перше місце. Тому необхідно не тільки захищати їх з фізичної точки зору, але й розглядати можливості підвищення безпеки передачі інформації незахищеними каналами за допомогою криптографічного захисту.

Висновки

1. Було проаналізовано загрози безпеці інформації та наслідки їх здійснення у вигляді кібератак та з'ясовано привабливі напрямки для кіберзлочинців за сферами діяльності.

2. Розглянуто динаміку змін активності кіберзлочинців. В результаті з'ясовано, що вона пов'язана з активізацією обстрілів стратегічних цивільних обєктів.

3. В результаті проведеного аналізу за видами атак, що були скоєні за люти – вересень 2022 р., створено рейтинг кібератак на держоргани.

Література
1. Алла Гаврилова, Юлія Хохлачова, Володимир Погорелов, Аналіз застосування гібридних крипто-кодових конструкцій для підвищення рівня стійкості геш-кодів до зламу, «Безпека інформації», Том 28, № 2, 2022, URL: https://jrnl.nau.edu.ua/index.php/Infosecurit,doi: 10.18372/2225-5036.28.16953.
2. Gavrilova A., Volkov I., Kozhedub Yu., Korolev R., Lezik O., Medvediev V., Milov O., Tomashevsky B., Trystan A., Chekunova O. Development of a modified UMAC Algorithm based on crypto-code constructions // Eastern-European Journal of Enterprise Technologies. – 2020. – № 4/9 (106). – С. 45 –63.
3. Війна в Україні. Пульс кіберзахисту // Державна служба спецзв'язку та захисту інформації, серпень 2022р. https://www.ppl.org.ua/wp-content/uploads/2022/09/1662392024242416.pdf
4. Захист систем електронних комунікацій: навч. посіб. / В. О. Хорошко, О. В. Криворучко, М. М. Браіловський та ін. – Київ : Київ. нац. торг.-екон. ун-т, 2019. – 164 с. DOI: http: //doi.org/10.31617/np.knute.2019-649
5. Пирцхалава Л. Г., Хорошко В. А., Хохлачева Ю. Е., Шелест М. Е. Информационно-аналитическое обеспечение безопасности: монография. – Киев: ФЛП Ямчинский А. В., 2021. – 470 с.
6. Браіловський М. М., Зибяін С. В., Кобозєва А. А., Хорошко В. О., Хохлачова Ю. Є. Аналіз кіберзахищеності інформаційних систем: монографія. – К.: ФОП Ямчинський О. В., 2021. – 360 с.

УДК 004.056.5, УДК 004.491/.492, УДК 341.232

12.ВИКОРИСТАННЯ МЕТОДИЧНИХ ПІДХОДІВ СИСТЕМНОГО АНАЛІЗУ ДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Якименко Ю.М., Рабчун Д.І., Капелюшна Т.В.
Державний університет телекомунікацій, Київ, Україна
E-mail: yakum14@ukr.net, rabchundima92@gmail.com, e-skr@ukr.net.

U**se of methodological approaches of system analysis to ensure information security of critical infrastructure objects**

The report examines the actual importance of applying methodical approaches of system analysis to ensure information security of critical infrastructure objects in modern conditions of Ukraine. In relation to information, an information protection strategy should be developed in the form of a comprehensive information protection system. In order to best solve the issue of increasing the efficiency of the information security system of critical infrastructure objects, it is proposed to design, implement and improve the information security management system as a complex system with the presence of other subsystems: risk management and security incident management.

Сьогодні для України критична інфраструктура відіграє важливу роль, а забезпечення її безпеки впливає на загальний стан всіх процесів в нашій державі. За останні шість років у світі в 57 разів збільшилася кількість кібератак, у 2020 році в Україні було зафіксовано близько 1 мільйона випадків кіберзагроз, в тому числі на об'єктах критичної інфраструктури [1]. Тому країни змушені посилювати захист стратегічно важливих підприємств та об'єктів критичної інфраструктури. Наразі найрозвиненіші держави світу витрачають на кібербезпеку у 5 разів більше, ніж на інші напрямки ІТ-галузі. За оцінками фахівців вже у 2025 році ці витрати можуть сягнути 10, 5 трильйонів доларів [2]. В цьому контексті Україні необхідно якнайшвидше нарощувати захист об'єктів критичної інфраструктури.

Інформаційна безпека визначається сукупністю технічних і організаційних заходів, основною метою яких є захист та збереження всієї інформації, якою володіє організація. Разом з тим, інформаційна безпека (ІБ) включає в себе не лише захист інформації та даних, а й захист систем, мереж та інше. Заходи ІБ повинні бути також зосереджені на мережевих системах та комп'ютерній інфраструктурі організації, яка найчастіше всього може стати об'єктом кібератак та інших зловмисних дій, направлених на знищення, крадіжку або пошкодження інформації.

Забезпечення безпеки України – це завдання державних інституцій та її власників і операторів. Забезпечення ІБ слід розглядати як невід'ємний елемент процесу управління будь-якою організацією (підприємством, фірмою, компанією). До організацій можно віднести і об'єкти критичної інфраструктури (ОКІ), забезпечення ІБ яких мають свої особливості. Функціонування таких об'єктів напряму залежить від ефективної діяльності суб'єктів їхнього захисту, взаємної узгодженості та своєчасної координації їхніх дій, які повинні забезпечувати цей захист. Автор Сурмін Ю.П. пропонує представляти ОКІ в дослідженні як деяку систему з характеристиками: елементним складом; структурою як формою взаємного зв'язку елементів; функціями елементів і цілого; єдністю внутрішнього і зовнішнього середовища системи; законами розвитку системи та її складників [3].

Відповідно до «Концепції створення державної системи захисту критичної інфраструктури», затвердженої постановою Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р [4]. вибудовується логічна модель інтегрованих між собою систем і підсистем, головним компонентом яких виступають суб'єкти діяльності. Автор Теленик С.С. пропонує в [5] до суб'єктів безпосереднього забезпечення захисту ОКІ, як складної розгалуженої системи, відносити такі основні підсистеми, як: управлінсько-координаційна, техніко-функціональна, моніторингово-аналітична, охоронно-превентивна, кризово-ситуативна підсистема. Для більш ефективної реалізації державної політики у сфері захисту ОКІ можлива зміна перелічених або доповнення підсистем- в залежності від

сучасних реалій розвитку держави в епоху постійної ескалації і появі нових видів загроз.

В аналітичній записці [6] показано необхідність захисту ОКІ від усіх видів фізичних та кіберзагроз, що вимагає якісно нового рівня координації дій, взаємодії та обміну інформацією між численними суб'єктами діяльності. Задовільнити усі вимоги у сфері безпеки ОКІ можливо лише тільки на системній основі.

Застосування методичних підходів системного аналізу для забезпечення ІБ організацій багато в чому визначається сучасними можливостями інформаційних технологій при вирішенні завдань і проведенні досліджень складних систем, де широко використовується комп'ютерне обладнання. ОКІ розглядаються як досить складні організаційно-технічні системи.

Саме фахівці з системного аналізу проектують, створюють й експлуатують комп'ютерні системи управління та проектування динамічних процесів в технічних і технологічних об'єктах. Системний аналіз — це певний підхід до вирішення проблем, методологія дослідження та проектування складних систем, пошуку, планування та реалізації заходів, спрямованих на вирішення проблемних ситуацій. Системний аналіз в англомовній літературі використовують частіше як синонім системного підходу. Тому системний підхід дозволяє визначити забезпечення ІБ як складний, комплексний вид діяльності, що висуває особливі вимоги до його структурної характеристики [7]. Головною метою будь-якої системи забезпечення ІБ є створення умов успішного функціонування організації, запобігання всіх видів загроз її безпеці, захист від втрат, витоку, спотворення та знищення конфіденційної інформації. Забезпечення ІБ повинно бути представлене як безперервний і динамічний процес, основний зміст якого становить управління безпекою в загальній системі управління, а управління інформаційною безпекою в іншій системі розглядається також як процеси, але по відношенню управління: персоналом, засобами захисту інформації, ризиками і інцидентами ІБ, безперервністю бізнесу і ресурсами з метою забезпечення інформаційної безпеки [8, 9].

Для цього необхідно створювати ефективну систему управління інформаційною безпекою (СУІБ), використовуючі вже напрацьовані практики (стандарти, методології) побудови подібних системи управління.

Для успішного функціонування і виконання завдань СУІБ повинна відповідати вимогам нормативно-методичних документів і, перш за все, стандарту ISO / IEC 27001 (ДСТУ ISO / IEC 27001) .

По відношенню до інформації повинна бути розроблена стратегія захисту інформації у вигляді комплексної системи захисту інформації (КСЗІ) , як загальна спрямованість діяльності організації з урахуванням її об'єктивних

потреб, можливих умов здійснення і можливостей. Цільова комплексність в КСЗІ означає, що вона в організації має будуватися в напрямах:

захисту інформаційних ресурсів та систем, особистості, суспільства та держави від зовнішніх та внутрішніх загроз;

захисту особистості, суспільства та держави від негативного інформаційного впливу [9,10].

Безпеку інформації вже неможливо забезпечити лише одним набором технічних засобів і підтримувати тільки силами підрозділів безпеки. Особливо це треба робити при проектуванні, впровадженні та поліпшенні СУІБ [101.

Але відповідно до вимог стандарту ISO/IEC 27001 [12] функціонування СУІБ тісно пов'язане з управлінням ризиками та інцидентами ІБ. Тому СУІБ пропонується розглядати ще, як комплексну систему з наявністю в неї у вигляді цілком самостійних інших підсистем: управління ризиками ІБ (СУРІБ) та управління інцидентами ІБ (СУІІБ). Кожна підсистема управління відповідно до своїх цілей, завдань і ресурсів, запланованих для їх виконання, створює механізми, що забезпечують об'єднання зусиль і ресурсів, які вона має (розподіл ресурсів, постановка завдань виконавцям та введення процедур для їх досягнення).

Усі процеси управління цих систем збагачують виконання процесів функціонування СУІБ. Логічно цю комплексність в СУІБ можно зафіксувати у новому понятті – КСУІБ (як комплексна СУІБ). Для вирішення слабо структурованих проблем у дослідженні з побудовою КСУІБ вже на практиці використовується методологія системного аналізу [13,14].

Єдиної методики системного аналізу у наукових дослідженнях з побудовою СУІБ поки що немає. Завдання системного аналізу визначаються його етапами. Тому часто завдання та етапи його проведення розглядаються як тотожні- як завдання аналізу, декомпозиції і сінтезу.

В основу дослідження з побудовою КСУІБ як складової частини системи управління організації можна запропонувати такі основні методологічні підходи, які частіше икористовуються в проведенні досліджень складних об’єктів і процесів:

• Системний підхід, що означає дослідження конкретного об'єкта як системи, вимагає багаторівневого вивчення системи управління. Аналіз і синтез в своєму єднанні складають основу системного підходу до вивчення діяльності організації, як науково-методологічну основу, яка сприяє знаходженню найбільш вигідних шляхів вирішення виникаючих проблем.

• Процесний підхід - підхід до дослідження систем управління як до безперервного виконання сукупності взаємопов'язаних між собою робіт і загальних функцій управління. Вся діяльність організації розглядається як набір процесів. Для структурування всіх процесів в СУІБ управління і для забезпечення обліку всіх значимих елементів процесного підходу застосовується

циклічна класична модель або цикл PDCA (від англ. Plan-Do-Check-Act - плануй - виконуй - перевіряй - дій »).

Для найкращого вирішення питання підвищення ефективності ІБ об'єктів критичної інфраструктури пропонується використовувати їх системно: при створенні (або вдосконаленні) СУІБ в організації треба завжди акцентувати значну увагу на окремі її підсистеми з організаційними і технічними особливостями: СУРІБ і СУІІБ.

Висновки

1. Розглянуто актуальне значення застосування методичних підходів з системного аналізу до забезпечення інформаційної безпеки об'єктів критичної інфраструктури в сучасних умовах України. Системний аналіз дозволяє визначити забезпечення інформаційної безпеки як складний, комплексний вид діяльності, спрямованного на створення умов успішного функціонування об'єктів критичної інфраструктури (організацій), запобігання всіх видів загроз їх безпеці, захист від втрат, витоку, спотворення та знищення конфіденційної інформації. Проаналізовано необхідність створення ефективної системи управління інформаційною безпекою, яка повинна відповідати вимогам нормативно-методичних документів. По відношенню до інформації повинна бути розроблена стратегія захисту інформації у вигляді комплексної системи захисту інформації з урахуванням необхідних об'єктивних потреб, можливих умов здійснення і можливостей.

2. Запропоновано розглядати (проектувати, впроваджувати та поліпшувати) систему управління інформаційною безпекою, як комплексну систему з наявністю в неї у вигляді цілком самостійних інших підсистем: управління ризиками та управління інцидентами інформаційної безпеки. Усі процеси управління цих систем збагачують успішне функціонування інших організаційних і технічних систем та своєчасне виконання задач по забезпеченню високого рівня інформаційної безпеки. В основу дослідження з побудовою комплексної системи управління інформаційною безпекою як складової частини загальної системи управління організації можна запропонувати основні методологічні підходи, які вже частіше икористовуються в проведенні досліджень складних об'єктів і процесів: системний і процесний. Але для найкращого вирішення питання підвищення ефективності системи інформаційної безпеки об'єктів критичної інфраструктури пропонується використовувати її підсистеми окремо - організаційно і технічно.

Література

1. Співробітники Укргідроенерго обговорили актуальні питання з кібербезпеки в рамках «CISCO DIALOG DAY». URL:

https://uhe.gov.ua/media_tsentr/novyny/spivrobitniki-ukrgidroenergo-obgovorili-aktualni-pitannya-z-kiberbezpeki-v
2. Як захистити об’єкти критичної інфраструктури від кібератак? енергетики обмінялись досвідом щодо охорони стратегічних об'єктів. URL: https://uhe.gov.ua/media_tsentr/novyny/yak-zakhistiti-obekti-kritichnoi-infrastrukturi-vid-kiberatak-energetiki
3. Сурмин Ю.П. Теория систем и системный анализ. Київ : МАУП, 2003. 368 с
4. Концепція створення державної системи захисту критичної інфраструктури: затверджено розпорядженням Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р. Урядовий кур’єр від 10.01.2018. № 5.
5. Теленик С.С. Система суб’єктів захисту об’єктів критичної інфраструктури Прикарпатський юридичний вісник с.36-44 Випуск 4(29) Том 2, 2019. URL: http://pjv.nuoua.od.ua/v4-2_2019/9.pdf
6. Проблеми забезпечення взаємодії при реагуванні на інциденти та кризи комплексного характеру на об’єктах критичної інфраструктури: Аналіт. записка НІСД від 07.09.2018. URL: https://niss.gov.ua/doslidzhennya/ nacionalna-bezpeka/problemi-zabezpechennya-vzaemodiipri-reaguvanni-na-incidenti-ta.
7. Якименко Ю.М., Савченко В.А., Легомінова С.В. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. Київ: Державний університет телекомунікацій, 2022. 308 с. URL: https://dut.edu.ua/uploads/l_2230_88161692.pdf.
8. Знакомство с методикой создания СМИБ”. URL: https://intercert.com.ua/articles/posts/282-it-grundshutz-metodikasmib.
9. Организационные основы защиты информации на предприятии URL: http://bezopasnik.org/article/19.htm.
10. Анисифоров А. Б. Методики оценки эффективности информационных систем и информационных технологий в бизнесе. //А.Б.Анисифоров, Л.О Анисифорова/.- Санкт-Петербург: 2014- 97с. URL: https://docplayer.com/31056290-Metodiki-ocenki-effektivnosti-informacionnyh-sistem-i-informacionnyh-tehnologiy-v-biznese.html.
11. То Кен Сик. Системный подход и системный анализ для исследования социально-экономических объектов и принятия управленческих решений : уч. пособие / То Кен Сик,– Южно-Сахалинск : СахГУ, 2014. – 168 с.
12. ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements. URL: https://www.iso.org/standard/82875.html
13. Носаков В.Создание комплексной системы управления информационной безопасностью.- Jet Info №7, 2008. URL: http://www.jetinfo.ru/stati/sozdanie-kompleksnoj-sistemy-upravleniya-informatsionnoj-bezopasnostyu
14. Организационные основы защиты информации на предприятии URL: http://bezopasnik.org/article/19.htm.

РОЗДІЛ 2

ТЕОРЕТИЧНІ І МЕТОДОЛОГІЧНІ ОСНОВИ ОЦІНЮВАННЯ КІБЕРЗАГРОЗ, ТЕХНОГЕННИХ ТА ЕКОЛОГІЧНИХ ЗАГРОЗ І РИЗИКІВ ДЛЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

UDC 351.861

13.GENERALIZATION OF THE CHARACTERISTICS OF CRITICAL STATE INFRASTRUCTURE OBJECTS

Azarenko O.[1], Honcharenko Yu.[2], Divizinyuk M.[3], Shevchenko R.[4], Shevchenko O.[4]

1 Scientific-research laboratory-experimental center "BRAND TRADE", Kharkiv, Ukraine;

2 European University, Kyiv, Ukraine;

3 Institute of Geochemistry and Environment of the National Academy of Sciences of Ukraine, Kyiv, Ukraine;

4National University of Civil Defense of Ukraine, Kharkiv, Ukraine

E-mail:shevchenko605@i.ua

Узагальнення характеристик об’єктів інфраструктури критичного стану

У роботі визначено об’єкти критичної інфраструктури держави, їх взаємозв’язок зі стратегічними та іншими небезпечними об’єктами та виробництвами.

It should be noted that today Ukraine, as a state that defends its independence in the war, faces many different tasks, one of which is the protection of critical infrastructure objects from military-terrorist influence, the solution of which not only saves the lives of civilians, but also ensures the defense of sovereignty, territorial integrity and independent existence of the state. The solution of this task is carried out both in wartime and in peacetime. The problem is to determine the objects of the state's critical infrastructure, in their correlation with strategic and other dangerous objects and productions, which in practice allows determining the priority of their protection in terms of the involvement of technical and material means.

Based on the above, the purpose of this article is to determine the relationship between the terms critical infrastructure object, potentially dangerous object, dangerous production object and strategic object, from the standpoint of ensuring their security and countering terrorist threats.

The concept of state infrastructure and the process of formation of the term critical infrastructure of the state are considered. The characteristics of the objects of strategic purpose are given. The meaning of the concepts of potentially dangerous, dangerous industrial and critically important objects is analyzed.

It is proved that based on the assessment of the constituent parts of the state's critical infrastructure, the concepts of a potentially dangerous object, an object of hazardous production, a critically important object and a strategic object can be considered identical in relation to nuclear objects.

Prolonging the reasoning in this way, it is possible to confirm the validity of this identity in relation to other objects of critical infrastructure, for example, hydro and thermal power, petrochemicals and others.

УДК 614.8 (076)

14.NUCLEAR AND ENVIRONMENTAL DANGER OF THE ZAPORIZH NPP IN THE EXTREME CONDITIONS OF THE WAR IN UKRAINE

V.M. Vashchenko [1], V.I. Skalozubov [2], I.B. Korduba[3]

[1] *Interdepartmental Scientific Center for Fundamental Research on Energy and Ecology, Odessa*

[2] *Department of Nuclear Power Plants of Odessa National Polytechnic University, Odesa.*

[3]*Department of technology of environmental protection and labor protection, Kyiv National University of Construction and Architecture, Kyiv, Ukraine.*

E-mail: nucleoroid@gmail.com

An urgent issue of the safety of Ukraine's nuclear power industry in extreme conditions is the situation at the Zaporizhia Nuclear Power Plant (ZNPP), the largest in Europe, due to the location of the plant in a war zone and difficulties in management and operation, as well as regulating the safety of the plant in the occupied territory. Therefore, an objective assessment of the level of nuclear and radiation safety of the ZNPP in the extreme conditions of wartime, as well as the justification of practical recommendations for the prevention of environmental disasters, is an urgent issue.

Traditionally, the assessment of the state of nuclear and radiation safety of NPPs is based on probabilistic and deterministic safety indicators [2-13].

The following are the main probabilistic indicators of safety in global nuclear energy:

- the probability of a nuclear (severe) accident with damage to nuclear fuel (ЧПАЗ (– the frequency of damage to the active zone of the reactor):

$$\text{ЧПАЗ} \sim IP_s \qquad (1)$$

- the probability of occurrence of a maximum permissible radioactive release:

$$\text{ЧПАВ} \sim \text{ЧПАЗ} \cdot P_b \qquad (2)$$

De *I* - is the probability of the original emergency event (VAP); Ps - the possibility of failure of critical changes in the safety systems of nuclear power plants; Pb- is the probability of failure of protective safety barriers that prevent conditions of radioactive emissions.

Events/incidents/violations of normal operating conditions leading to an emergency shutdown of the reactor are regulated as VAP:
leaks/ruptures of pipelines and steam pipelines of systems important for the safety of nuclear power plants (NPP nuclear power plants); de-energization of power units; failure of normal operation of the SVB; extreme natural phenomena (earthquakes, floods, tornadoes, hurricanes, etc.); the fall of large objects on the power unit, etc.

Probable nuclear safety criteria:

$$ЧПАЗ = \begin{cases} 10^{-4}/\text{(reactor • hour)} - \text{for active NEU} \\ 10^{-5}/\text{(reactor • hour)} - \text{for new NEU} \end{cases} \quad (3)$$

Probable nuclear safety criteria:

$$ЧПАЗ = \begin{cases} 10^{-6}/\text{(reactor • hour)} - \text{for active NEU} \\ 10^{-7}/\text{(reactor • hour)} - \text{for new NEU} \end{cases} \quad (4)$$

Thus, the application of probabilistic approaches and methods of assessing the state of nuclear, radiation and environmental safety of the ZNPP in extreme wartime conditions is insufficiently substantiated for the following reasons:

imperfection of probabilistic methods of assessing the level of safety of nuclear power plants; military operations are unpredictable and subject to stochastic patterns.

Deterministic methods and approaches based on deterministic modeling of accident sequences of VAP are more reasonable for objective assessment of safety.

Deterministic criteria of nuclear and radiation safety are usually defined as: maximum permissible temperatures of nuclear fuel and fuel cell shells; maximum allowable pressures in the reactor and hermetic volume (containment); maximum permissible concentration of hydrogen; maximum permissible doses of radioactive exposure to personnel, the population and the environment.

In the extreme wartime conditions of ZNPP operation, the initial events of nuclear and radiation accidents can be: destruction of NPP safety barriers as a result of intentional or accidental hitting of warheads; destruction or failure of critical infrastructure facilities that provide external or emergency power consumption of power units of the ZNPP; flooding of the industrial site of the ZNPP as a result of the destruction of the dam of the Kakhovsky Reservoir; the impact of powerful warheads in the cooling pond and others.

The first group of VAP in the extreme conditions of wartime operation of the ZNPP include: damage or destruction of the protective safety barriers of the nuclear power plant (protective envelope of the hermetic volume - ZO GO, reactor body, heat-emitting assemblies - TVZ, shells and fuel matrix, fuel cell) due to external influence combat charges.

Numerous simulation results of the VVER 1000 MPA with deterministic codes have established that, under the conditions of maintaining the operability of critical (to

ensure safety) safety system configurations, the conditions for the start of a nuclear accident (upon reaching the maximum allowable temperature of the Twel shells for the beginning of the intensification of the vapor zirconium reaction - 1473 oK) do not occur at the MPA. Thus, on the basis of the analysis presented above, it was established that the power of the external warhead necessary for the occurrence of a nuclear and radiation accident must be able to destroy all protective barriers of NPP safety and safety systems that provide management of emergency processes. This power can be atomic or hydrogen bombs.

Damage or destruction by external warheads of critical infrastructure objects that provide external and emergency power supply of the nuclear power plant are included in the second group of VAP in the extreme conditions of wartime operation of the nuclear power plant.

Only during the last period of hostilities in Ukraine, there were several dozen damages to critical infrastructure objects of the external and emergency power supply of the ZNPP (transformer equipment, power supply systems to the consumer, diesel generator rooms, and others) and corresponding emergency shutdowns of the ZNPP power units due to power loss of the plant. At the same time, it should be noted: the process of emergency shutdown of the nuclear power unit reduces the overall level of nuclear and radiation safety according to the design permissible cycles of thermal and dynamic loads on systems important for the safety of nuclear power plants with nuclear power plants; emergency shutdowns of nuclear power plants significantly affect the reliability and efficiency of the entire energy system of Ukraine.

The next dominant group of WAP for safety in the extreme conditions of wartime operation of the ZNPP is the flooding of the station's industrial site as a result of warheads hitting the dam and the volume of the Kakhovsky Reservoir (the height of the dam is more than 50 meters above the level of the reservoir), in the volume of the cooling pond of the ZNPP Cascade of Reservoirs (over 2 million tons of water)

Consequences of the flooding of the industrial site of the ZNPP may be: WAP of complete de-energization of power units (similar to WAP of the Fukushima accident); violation of heat exchange conditions in dry storage facilities for spent nuclear fuel (SNF).

Thus, the most relevant for the nuclear and radiation safety of the WAP in the extreme conditions of wartime operation of the ZNPP is a complete long-term blackout (PTZ) due to the destruction/damage of critical power supply infrastructure facilities and/or flooding of the industrial site.

Currently, in Ukraine, as in the world's nuclear energy, which is widespread during modernization, nuclear power plants have acquired the principle of "admissibility of reduced safety level (DZRB)" [1]. According to this principle, lowering the level of safety of nuclear power plants is permissible under the condition

$$\frac{\Delta ЧПАЗ}{ЧПАЗ_0} << 1 \qquad (5)$$

where ЧПА3*0* is the basic probabilistic estimate of the frequency of damage to the active zone (ЧПА3);

ΔЧПА3 – intentional or unintentional increase of ЧПА3.

In extreme operating conditions of the ZNPP, ΔЧПА3 may be associated with an increase in the probability of VAP, and if the events/incidents/violations of normal operation that occur satisfy condition (5), then the probability of violation of condition (5) remains. In addition, as noted above, the lessons of known nuclear accidents set the level of safety and permissible further operation of power units at the current moment in time. This approach to assessing the level of safety of nuclear power plant operation in extreme conditions of war is insufficiently substantiated for the following reasons: in the pre-Fukushima period, in the operational reports on probabilistic safety analysis (IAB) of Ukrainian nuclear power plants with VVER-1000, a severe nuclear accident was supposed to be an unambiguous consequence of the WAP PTZ.

Flooding of the ZNPP production site can have critical consequences: complete and long-term blackout of the power unit; violation of the conditions of heat exchange in the SHVYAP. It should be taken into account that there are dry spent nuclear fuel storage facilities (SFU) located on the ZNPP site, in which nuclear fuel is cooled by natural air circulation. In case of flooding together with garbage, the conditions for the necessary cooling of the SHVYAP, which corresponds to additional exit emergency events (VAP), may be violated. To prevent the possible flooding of the industrial site of the ZNPP, the construction of dams on the coast of the cooling pond can be effective

Conclusions

Therefore, the current issue of the security of Ukraine's nuclear power industry in the extreme conditions of war is the situation at the Zaporizhzhia NPP, the largest in Europe, due to the station's location in the war zone and difficulties in management and operation, as well as the safety regulation of the station in the occupied territory. Probabilistic approaches to assessing the objective state of safety of the Zaporizhzhia NPP in extreme conditions are insufficiently substantiated, taking into account the lessons of the largest nuclear and radiation accidents. Flooding of the industrial site of the ZNPP can be the cause of the occurrence of two primary emergency events: complete and long-term blackout of power units and violation of heat exchange conditions in dry storage facilities for spent nuclear fuel. Prevention of flooding of the industrial site of the Zaporizhzhya NPP can be based on the construction of protective barriers against flooding on the coast of the cooling pond.

Bibliography (transliterated)

1. Zabuloniv Yu.L., Lysychenko H.V., Kovalevskyi V.V. Teroryzm KhKhIstolittia – realna zahroza tekhnohenno-ekolohichnii bezpetsi. – Zbirnyk tez dopovidei – Mizhnarodna naukovo-praktychna konferentsiia “Pershyi Vseukrainskyi zizd ekolohiv” - Internet-spilnota «Promyslova ekolohiia», - http://eco.com.ua/

2.Kompleks metodiv pereotsinky bezpeky atomnoi enerhetyky Ukrainy z urakhuvanniam urokiv ekolohichny khkatastrof u Chornobyli ta Fukusimi / Zared. V. I. Skalozubova. Odesa: Astroprynt, 2013. 242 s.

3. Korolev A.V., Derevianko O.V. Emergensy composition of steam generators in shutdown conditions Nuclear and radiation safety/ - Riev? 2014. - T. 2 (62). – P. 10-12.

4. Hromov H. V., Dybach A. M., Zelenyi O. V., Iniushev V. V. Ta in. Rezultaty ekspertnoi otsinky stres-testiv diiuchykh enerhoblokiv AES Ukrainy z urakhuvanniam urokiv avariina AES «Fukusima-1» Yaponii. Yaderna ta radiatsiina bezpeka. 2012. № 1 (53). Z. 3 – 9.

5. Ostreikovskyi V. A., ShvyriaievYu. V. Bezpeka atomnykh stantsii. Imovirnisnyi analiz bezpeky. M.: FIZMATLIT, 2008. 352 s.

6. IAEA International Fact Finding Expert Mission of FukushimaDai-Ichi NPP Accident Following the Great East Japan Earthquake and Tsunami: IAEA MissionReport. IAEA, 2011. 160 hrn.

7.Hryshchenko B. Yu., Polianskyi M. A., Sevbo O. Ye., Semeniuk I. A. Zastosuvanni aymovirnisnykh metodiv analizu bezpeky AES pry doslidzhenni porushen krykhkoi mitsnosti korpusu reaktora. Yadernataradiatsiinabezpeka. 2013. № 1 (57). S. 22 - 25.

8.Shchodo Planu dii z vykonannia tsilovoipozacherhovoi perevirky ta podalshoho pidvyshchennia bezpeky AES Ukrainy z urakhuvanniam podii na Fukusima-1. Kolehiia Derzhatomrehuliuvannia, №2 vid 19.05.11 r.

9.Borysenko V. I. Pro deiaki zakonomirnosti naslidkiv avariina AES. Problemy bezpeky AES ta Chornobylia. 2012. Vypusk 18. S. 6 - 15.

10.Rezultaty provedennia stres-testiv Natsionalnyizv it Ukrainy. HIIaRU, 2011. 137 s.

11.Pravyla ekspluatatsii vodoskhovyshch Dniprovskoho kaskadu HES. Ukrhidroproekt, 1981.

12.00.HT.Rh.04 A.Posibnyky z upravlinnia zaproektnymy avariiamy enerhoblokiv ZAES. 1998.

13.Accident Management Programsin Nuclear Power Plants: a Guidebook. Technical Report SeriesNo 368. Vienna: IAEA, 1994. 127 p.

14.OECD Work shop na Implementation of Severe Accident Management Measures (Villigen-PSI, Switzerland, September 10 – 13, 2001). (Pre-Printof the Proceedings).

UDC 351.861

15.METHODS OF DETECTING KEY SIGNS OF AN EMERGENCY SITUATION AT CRITICAL INFRASTRUCTURE OBJECTS

Shcherbak O., Khmyrova A., Khrystych V., Shevchenko R.
National University of Civil Defense of Ukraine
E-mail:shevchenko605@i.ua

As a result of burning, which occurs as a result of an emergency situation related to a fire, materials, structures, equipment and individual objects that are in the zone of action of high temperature undergo various destructions, deformations or are completely destroyed - they burn. As a rule, the destruction occurs unevenly and this circumstance is often used when establishing the focus of an emergency situation related to a fire.

The location of the cell is often associated with the place of greatest burnout and destruction. In such a case, they proceed from the assumption that the greatest destruction is due to longer burning, longer effect of high temperature, i.e. the time factor, and, as a result, they come to the conclusion that the fire could have originated in this area. The problem of obtaining objective data, necessary to establish the center of the fire and the ways of the spread of combustion, remains extremely relevant, especially in cases where it is impossible to examine the objects of the physical environment due to their destruction and removal from the fire site. Soot deposits on structures and objects are present in almost any fire - both in the burning zone and in the smoke zone.

This circumstance allows us to consider soot as a promising object of expert research. At present, the claw is used to a very limited extent as an object of research and, accordingly, as a source of forensically significant information about the fire. Specialists made only attempts to determine the nature of burned materials by the structure and composition of soot, as well as to establish the fact of the presence of leaded fuels in the combustion zone by the presence of lead oxide and non-leaded petroleum products in the soot by detecting their microquantities sorbed by soot particles.

The tasks of determining the burning conditions in different fire zones and identifying the focal signs of the fire were not considered and solved. The analysis of the electrical resistance of the soot layer makes it possible to study smog directly at the site of the fire and, thus, to identify the paths of propagation of the main convective flows and the focal zone.

Further research will be directed to the development of appropriate mathematical models and conducting field experiments, performed using a specially designed laboratory facility to determine the reliability of the latter, comparing theoretical and practical results.

УДК 504.058

16.ДЕЯКІ ПИТАННЯ УПРАВЛІННЯ РИЗИКАМИ ЗАТОПЛЕННЯ ВНАСЛІДОК ПАВОДКІВ І ПОВЕНЕЙ

Жук В. М., Погосян Г. А.
Міністерство захисту довкілля та природних ресурсів України
E-mail: zhukvetal@gmail.com, hamletpogosian@gmail.com

Some issues of flooding risk management

Floods are one of the most common natural phenomena in the world, the damages from which are increasing every year. In order to prevent hydrodynamic hazards, the construction of anti-flood hydrotechnical structures is carried out. International experience shows that the most effective approach to flood protection is to develop flood risk management programs that include elements such as: prevention, protection, emergency preparedness and recovery.

Паводки і повені є одними з найпоширеніших природних явищ у світі, збитки від яких щороку складають близько 40 млрд. доларів США . В Україні негативні наслідки від паводків можливі на 27 % її території, де проживає майже третина населення країни. Найбільшого негативного впливу від них зазнають гірські та передгірські райони Карпат, які займають територію Закарпатської, Львівської, Івано-Франківської та Чернівецької областей. Однак негативного впливу систематично зазнають й інші регіони України. Зливові паводки стають однією з найбільш розповсюджених причин виникнення надзвичайних ситуацій, що призводять до виникнення загрози життю або здоров'ю населення, великої кількості загиблих і постраждалих, а також до завдання значних матеріальних збитків. Наукові дослідження свідчать, що під впливом кліматичних змін гідрологічний цикл буде змінюватись, збільшуючи інтенсивність та частоту таких катастрофічних паводків у всьому світі [1].

У 2020 році в Україні зафіксовано збільшення масштабності надзвичайних ситуацій та зростання більш ніж у 6 разів суми завданих ними збитків, зокрема внаслідок катастрофічного розвитку зливових паводків у західних регіонах України. Негативні наслідки паводків 2020 року на території Івано-франківської, Чернівецької, Закарпатської, Львівської та Тернопільської областей стали найбільш масштабними в історії України. Різкий підйом рівню води у басейнах річок призвів до підтоплення 349 населених пунктів, 14.3 тис. будинків, 22.4 тис. присадибних ділянок, пошкодженню 3.5 тис. господарських споруд, руйнуванню та пошкодженню понад 940 км автодоріг, понад 140 км берегоукріплень, понад 20 км дамб та понад 300 мостів. Тоді у найбільш постраждалій Івано-Франківській області загинуло 5 осіб, у тому числі 1 дитина [2].

Отже, катастрофічні наслідки паводків вкотре продемонстрували необхідність та важливість координації зусиль з управління ризиками таких стихійних лих гідрометеорологічного характеру, як зумовлені паводками затоплення. Скорочення ризиків зумовлених паводками затоплень – це комплекс

заходів, які мають бути спрямовані на контроль чинників розвитку паводків, зниження ймовірності їх виникнення та пом'якшення потенційних негативних наслідків, зменшення вразливості населення/майна, а також підвищення рівня готовності до несприятливих подій і відновленню після них.

З метою запобігання гідродинамічній небезпеці здійснюється будівництво протипаводкових гідротехнічних споруд, що знаходяться на балансі підприємств, установ та організацій сфери управління міністерств та відомств різних галузей економіки України або перебувають в оренді чи приватній власності громадян, та виконують функцію запобігання виникненню негативних наслідків, пов'язаних із захистом від шкідливої дії вод, пов'язаної з паводками та повенями, а також прийняттям управлінських рішень щодо охорони та раціонального використання водних ресурсів, а також виконання робіт із природоохоронних заходів [3].

Міжнародний досвід показує, що найефективніший підхід з протипаводкового захисту полягає у розробці програм управління ризиками затоплення, що включають такі елементи як: запобігання, захист, готовність до надзвичайного реагування та відновлення [4].

В рамках імплементації Паводкової Директиви 2007/60/ЄС [5] в Україні розроблені Плани управління ризиками затоплення у межах районів басейнів річок Вісли, Дніпра, Дністра, Дону, Дунаю, Криму, Приазов'я, Причорномор'я, Південного Бугу тощо. Ці Плани управління ризиками затоплення затверджені розпорядженням Кабінету Міністрів України від 8 жовтня 2022 року № 895-р. [6] та містять заходи, спрямовані на досягнення цілей управління ризиками затоплення на окремих територіях у межах усіх районів річкових басейнів на 2023-2030 роки, що включають будівництво та реконструкцію захисних дамб, розчищення русел річок, заліснення і залуження водозбірних площ, удосконалення захисної протипаводкової інфраструктури тощо.

Наразі триває робота з розроблення карт загроз і ризиків затоплення для окремих територій у межах районів річкових басейнів, які мають високий ризик затоплення. Також потребує проведення інвентаризації протипаводкової захисної інфраструктури, включаючи геодезичні вимірювання абсолютних відміток висот елементів захисних гідротехнічних споруд.

Протипаводковий захист населених пунктів та прилеглих до річок земель повинен забезпечуватись системою запобігання, реагування та ліквідацією наслідків виникнення надзвичайних природного та техногенного характеру. Дотепер недостатньо уваги приділялось всім трьом елементам системи управління ризиками стихійних лих, в тому числі затопленням, що зумовлені паводками. Нестача необхідних заходів у сфері запобігання, пом'якшення негативних наслідків та підготовці до ліквідації наслідків стихійних лих, пов'язаних зі змінами клімату, призводить до стрімкого збільшення сум завданих ними збитків та кількості постраждалих. Нестача заходів протипаводкового захисту, як важливої складової системи управління ризиками, рівної до інших за значущістю, підвищує ризики підтоплення міських, сільських населених пунктів

та сільськогосподарських угідь, внаслідок чого населення та економіка держави зазнає багатомільйонних збитків.

З метою забезпечення захисту об'єктів критичної інфраструктури 16 грудня 2022 року внесені зміни до постанови Кабінету Міністрів України від 9 жовтня 2020 року № 1109 «Деякі питання об'єктів критичної інфраструктури» [7] в частині визначення переліку секторів критичної інфраструктури, а саме включено сектор з охорони навколишнього природного середовища, в якому передбачено напрямок щодо захисту від підтоплення захисних масивів, протипаводковий і протиповеневий захист. Протипаводкові гідротехнічні споруди, що відносяться до даного напрямку, обслуговуються водогосподарськими організаціями, що належать до сфери управління Державного агентства водних ресурсів України. Секторальним органом даного напрямку являється Міністерство захисту довкілля та природних ресурсів України.

Відповідно до методики категоризації об'єктів критичної інфраструктури проведено ідентифікацію об'єктів критичної інфраструктури підсектору «Управління, використання та відтворення поверхневих водних ресурсів, розвиток водного господарства», та віднесено їх до II, III і IV категорій критичності. В подальшому заплановано визначення рівня негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури.

Висновки

З метою забезпечення надійного управління об'єктами протипаводкової критичної інфраструктури доцільно:

1. Запровадження підходу до управління ризиками затоплення, який включає всі три елементи системи управління ризиками (запобігання, захист, підготовка до реагування та відновлення);
2. Підвищення ефективності реалізації, як конструкційних (інженерних), наприклад, утримання, відновлення або будівництво захисних гідротехнічних споруд, так й неконструкційних заходів протипаводкового захисту, наприклад, шляхом запровадження програм переселення населення із зон ризику, розчищення та регулювання русел річок, вдосконалення системи гідрометеорологічних спостережень та системи раннього виявлення загрози і оповіщення населення в цілому;
3. Усунення недоліків у системі фінансування конструкційних (інженерних) та неконструкційних заходів протипаводкового захисту.

Література

1. Програма розвитку ООН в Україні. Протипаводковий захист територій як складова системи управління ризиками затоплення. URL: https://www.undp.org/sites/g/files/zskgke326/files/migration/ua/8304e4a911344bc93cb7e44c544b3c94bce10c87fdad64f804cb78e2c44528c2.pdf.
2. Панасюк І.В., Томільцева А.І. Гідродинамічна небезпека – шляхи з її упередження. Комунальне господарство міст, 2015, випуск 120 (1). С. 130-136.

3. Безпека водних ресурсів України у глобальному вимірі: монографія (за заг. ред. М.А. Хвесика). К.: Державна установа «Інститут економіки природокористування та сталого розвитку Національної академії наук України», 2013. 500 с.
4. Левківський С.С., Падун М.М. Раціональне використання і охорона водних ресурсів. К.: Либідь, 2006. 280 с.
5. Директива № 2007/60/ЄС Європейського парламенту та Ради ЄС щодо оцінки та управління ризиками, пов'язаними з повенями. URL: https://zakononline.com.ua/documents/show/293758___293823;
6. Розпорядження Кабінету Міністрів України від 8 жовтня 2022 р. № 895-р. «Про затвердження планів управління ризиками затоплення на окремих територіях у межах районів басейнів річок». URL: https://zakon.rada.gov.ua/laws/show/895-2022-%D1%80#Text;
7. Постанова /Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 «Деякі питання об'єктів критичної інфраструктури». URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text.

УДК 664. 8/9

17.ДЕЯКІ АСПЕКТИ ЗБІЛЬШЕННЯ ТЕРМІНІВ ЗБЕРІГАННЯ ТА ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ ХАРЧОВИХ КОНЦЕНТРАТІВ В ЕКСТРЕМАЛЬНИХ УМОВАХ

Євланов М. В.[1], Черепньов І.А.[2], Чумаченко С.М.[3], Коломієць Д.П.[3]
1 Харківський національний університет радіоелектроніки
2 Державний біотехнологічний університет
3 Національний університет харчових технологій
E-mail: voenpred314@ukr.net, s_chum@ukr.net, kdp1210@i.ua

Some aspects of increasing the shelf life and efficiency of using food concentrates in extreme conditions

The thesis substantiates the relevance of research in the field of production and use of food concentrates in extreme conditions. Unsuitability for the concentrates production of agricultural products, which containing antibiotics and harmful food additives, has been determined. It is proposed to investigate the possibility of increasing the efficiency and shelf life of concentrates as a result of replacing antibiotics with plant-based extracts.

За останні тридцять років у світі спостерігається збільшення кількості людей, загиблих у катастрофах природного походження. На рис. 1 представлені дані ООН по глобальній смертності, пов'язаної з природними катаклізмами [1].

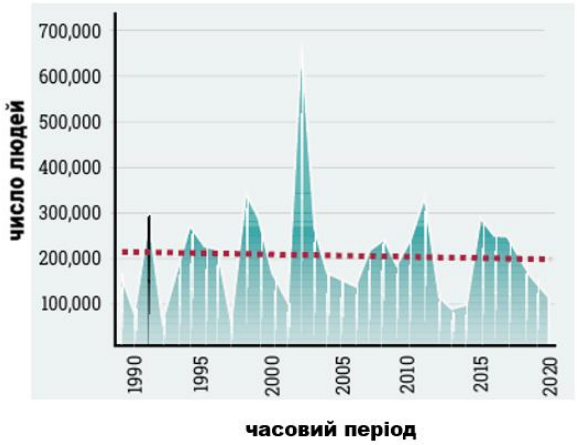


Рисунок 1 – Глобальна смертність, яка пов'язана зі стихійними лихами, 1989-2020 роки

Як зазначено у [1]: «… тенденції смертності сильно різняться з року в рік… Спостерігається помітне зниження з більш ніж 104 000 смертей на рік у 2000-х роках до в середньому 81 000 на рік у 2010-х роках. Тим не менш, зберігаються значні проблеми у зниженні глобальної смертності від стихійних лих до 2030 року». Значно більша кількість людей отримують поранення і (або) знаходяться в умовах, коли порушені умови нормальної життєдіяльності. Досить часто значно більша частина людей гине не від безпосередньої дії вражаючих чинників надзвичайної ситуації (НС), а в результаті голоду або епідемій, які виникають на постраждалих територіях. Класичним прикладом цього є катастрофа 8 серпня 1975 року греблі Баньцяо (КНР) як частини комплексу з 62 дамб. Ці дамби було прорвано повінню, викликаною тайфуном «Ніна». За офіційними даними 26 тисяч осіб загинуло безпосередньо в результаті повені, а через голод і епідемії як наслідки цієї повені загинуло в цілому 145 тисяч осіб.

Світовий досвід порятунку людей та ліквідації наслідків НС свідчить про складність своєчасного забезпечення постраждалих продуктами харчування та питною водою і, як наслідок, про численні випадки смерті від виснаження [2]. З огляду на сказане вище, продукти харчування, які необхідно використовувати для створення запасів продовольства, повинні відповідати наступним вимогам: мати мінімальну вагу і обсяг, а також найбільші енергетичні показники і зберігати свою якість при максимально можливому тривалому зберіганні. Група британських фахівців з виживання і ліквідації наслідків НС підготувала огляд, в якому розглянуто концептуальний підхід до розподілу продовольства, починаючи від потреб в харчуванні і закінчуючи політичними пріоритетами. За цим підходом, зокрема, раціони плануються таким чином, щоб відповідати вимогам до харчування і критеріям культурної прийнятності, засвоюваності і витрати енергії. Рекомендації щодо вмісту білка варіюються від 8 до 12,5% від загальної енергії. Більшість фахівців рекомендує, щоб жир забезпечував не менше 10% загальної енергії, а ряд представників Всесвітньої організації охорони здоров'я вважають за необхідне збільшити цей показник до 20% [3].

Характер змін в поживних речовинах при зберіганні харчових продуктів представлений в [4]. Можна відзначити, що вуглеводи є більш стійкими до зберігання в порівнянні з чутливими поживними речовинами, такими як вітаміни. У заморожених, консервованих або сушених продуктах немає істотної втрати поживної цінності вуглеводів. Як зазначено в [5], одними з найважливіших факторів, що скорочують термін придатності багатьох харчових продуктів, є кисень, світло, бактерії, що викликають псування, а також недостатнє охолодження. Враховуючи той факт, що в зоні НС цілком можливі перебої або повна відсутність електроенергії, холодильні установки або апаратура озонування повітря сховищ, швидше за все, не будуть функціонувати. Тому при формуванні продуктового запасу не слід орієнтуватися на свіжі овочі і фрукти, заморожені м'ясо або рибу. Необхідно орієнтуватися на харчові консерви і концентрати, тим більше, що накопичено значний (більш, ніж двохсотлітній) позитивний досвід використання їх в раціоні військовослужбовців [6].

У другій половині XX століття почалися широкі дослідження, які потім трансформувалися в практику використання антибіотиків при переробці та консервуванні харчових продуктів. Досить тривалий час вважалося, що ця практика абсолютно нешкідлива. Більш того, навіть в наукових публікаціях звучали з цього приводу абсолютно безапеляційні заяви, на кшалт наступної: «…Багаторічне промислове згодовування хлортетрацикліну і деяких інших антибіотиків домашній худобі і птиці свідчить про істотну нешкідливість декількох проміле. Тетрацикліни досить нестабільні і псуються в їжі і під час приготування. У деяких випадках щось інше може залишитися, але це будуть незначні сліди» [7]. На щастя, з часом була доведена згубність цієї небезпечної помилки. Щоб стимулювати ріст і збільшення ваги, цілі стада сільськогосподарських тварин зазвичай годують низькими дозами антибіотиків у їжі або воді. Ця практика застосовується для запобігання захворюванням у тварин, які живуть у часто переповнених та антисанітарних приміщеннях. Наслідком цієї практики є масове накопичення антибіотиків у навколишньому середовищі та набуття стійкості до антибіотиків у мікроорганізмів, що контактують з ними.

Споживання антибіотиків у секторі тваринництва є найвищим у Китаї (23%), США (13%), Бразилії (9%) та Індії (3%), на які припадає більшість світових продажів антибіотиків [8]. Крім антибіотиків також застосується широкий спектр хімічних добавок, які продовжують термін зберігання харчових продуктів, але одночасно завдають значної шкоди здоров'ю споживачів. Використовувати дані продукти для виготовлення консервів і харчових концентратів, які призначені, в тому числі, для харчування людей в екстремальних умовах, неприпустимо. На жаль, результати вивчення різних харчових продуктів, яке проводиться на території України, досить часто виявляють наявність антибіотиків. Так, на рис. 2 наведена діаграма досліджень курячих яєць на предмет виявлення різних антибіотиків [9].

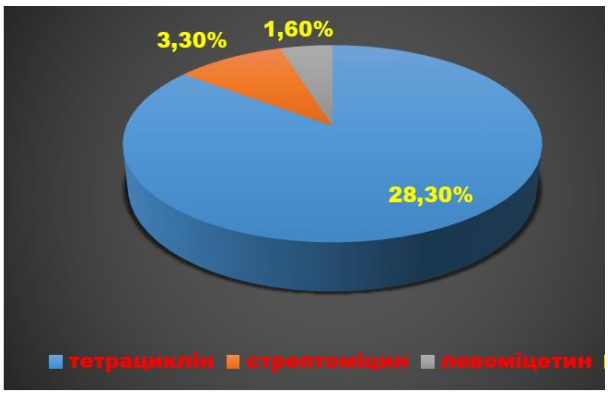


Рисунок 2 – Результати дослідження курячих яєць на наявність антибіотиків

Переважання частоти наявності тетрацикліну, ймовірно, обумовлена тим, що його продовжують давати птиці для стимуляції росту, незважаючи на заборону цієї дії відповідними документами. У ряді публікацій пропонується замінити антибіотики природними протимікробними препаратами для підвищення терміну зберігання продуктів харчування і в тому числі харчових концентратів. Зокрема, в [10] запропоновано використовувати екстракти на рослинній основі, які здатні не тільки збільшити термін зберігання, але і надавати лікувальну або стимулюючу дію на організм людини. В [11] авторами запропонована методика вибору оптимального виду адаптогену, що забезпечує підвищену працездатність людини за умови впливу на нього несприятливих зовнішніх факторів. Але для коректної і об'єктивної оцінки можливостей природних антибактеріальних засобів підвищити ефективність і термін зберігання харчових концентратів, на наш погляд, необхідно провести відповідні експерименти та ретельно проаналізувати їх результати. При цьому необхідно мати чітку впевненість в тому, що для виготовлення концентратів використовувалися рослинні продукти апріорі без добавок антибіотиків або інших хімічних консервантів

Література

1. Our World At Risk: Transforming Governance for a Resilient Future. United Nations Office for Disaster Risk Reduction: веб-сайт. URL: https://www.undrr.org/gar2022-our-world-risk (дата звернення 04.02. 2023).

2. Использование электромагнитных технологий для формирования продовольственного резерва / И.А. Черепнев та ін. Колективна монографія Харківського університету Повітряних Сил. 2015, Вип. 2(43). С. 154-158.

3. S, Young H. General food distribution in emergencies:from nutritional needs to political priorities. Good practice review 3. London: Relief and Rehabilitation Network, Overseas Development Institute, 1995.

4. Dandago, M.A. Changes in nutrients during storage and processing of foods - a review. Techno Science Africana Journal, Volume 3 Number 1, June 2009. Pp.24-27.

5. Eie, Thomas; Larsen, Hanne; Sørheim, Oddvin; Pettersen, Marit Kvalvåg; Hansen, Anlaug Ådland; Wold, Jens Petter; Naterstad, Kristine; Mielnik, Maria Bogumila. New technologies for extending shelf life. Italian journal of food sciences, vol. 19, 2007. Pp.127-154.
6. Багатокритеріальна (векторна) оптимізація раціону військовослужбовців, розташованих в стаціонарних і польових умовах / І.А. Черепньов та ін. Системи озброєння і військова техніка. 2019. № 2(58). С.152-167.
7. Deatherage FE. Use of Antibiotics in the Preservation of Meats and Other Food Products. Amer J Public Health 1957; 47:594.
8. Antibiotics in Food Chain: The Consequences for Antibiotic Resistance. Shashi B. Kumar, Shanvanth R. Arnipalli and Ouliana Ziouzenkova Antibiotics 2020, 9(10), 688; 26p doi.org/10.3390/antibiotics9100688
9. Кічук О.Д. Виявлення залишкових кількостей антибіотиків у продуктах тваринництва. Гуманітарні та природничі науки: актуальні питання: зб. матеріалів II Наук-практ. конф. 23-24 жовтня 2020 р. Дніпро: Молодий вчений, 2020. С. 45-49.
10. Natural Ingredients That Can Extend The Shelf-life Of Food Products. Asia Pacific food industry: сайт. URL:https://www.apfoodonline.com/industry/natural-ingredients -can- extend-shelf-life-food-products/ (дата звернення: 03.02. 2023).
11. Статистический анализ действия адаптогенов на работоспособность экипажей бронетанковой техники при выполнении боевой задачи / И.А. Черепнев та ін. Системи озброєння і військової техніки. 2017. № 3(51). С. 95-113.

УДК 355.58

18.ТЕОРЕТИЧНІ І МЕТОДОЛОГІЧНІ ОСНОВИ ОЦІНЮВАННЯ ТЕХНОГЕННИХ ЗАГРОЗ І РИЗИКІВ ДЛЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ В УМОВАХ ПОВНОМАСШТАБНОГО ВТОРГНЕННЯ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

Мацько П. І., Капля І. О., Романюк В.П.

Національний університет оборони України імені Івана Черняховського, Київ, Україна

Theoretical and methodological basis for assessing man-made threats and risks to the critical infrastructure of Ukraine under the conditions of a full-scale invasion of the russian federation

Ukraine is a country waging a full-scale war with the Russian Federation. One of the most vulnerable objects in such conditions is the state's critical infrastructure. This means that places where there are power plants (nuclear power plants, hydroelectric power plants, thermal power plants), water pipelines, gas pipelines, communication networks, transport hubs and other objects that support the life of the population and the economy are exposed to man-made threats and risks during operation hostilities.

Україна є країною, яка веде повномасштабну війну з російською федерацією. Один з найбільш вразливих об'єктів в таких умовах - критична інфраструктура держави. Це означає, що місця, де знаходяться електростанції (атомні електростанції, гідроелектростанції, теплоелектростанції), водопроводи, газопроводи, мережі зв'язку, транспортні вузли та інші об'єкти, які забезпечують життєдіяльність населення та економіку, піддаються техногенним загрозам та ризикам під час ведення бойових дій.

Наразі реалізовуються міжвідомчі плани захисту критичної інфраструктури країни, проте існують проблеми, які знижують їх ефективність:

недостатня координація між різними відомствами та структурами, які займаються захистом критичної інфраструктури. Це може призвести до недооцінки певних загроз або дублювання робіт, що займають зайвий час та ресурси. Також, відсутність єдиного підходу до захисту критичної інфраструктури може призвести до несистемності заходів та зниження їх ефективності;

недостатня увага до кібербезпеки та захисту інформації, яка пов'язана з критичною інфраструктурою. За досвідом повномасштабного вторгнення російської федерації кібератаки можуть призвести до великих збоїв в роботі інфраструктури та вкрай негативно вплинути на безпеку населення та економіки;

недостатня розробка та впровадження механізмів реагування на кризові ситуації. В разі виникнення кризових ситуацій, необхідно відразу реагувати та діяти відповідно до заздалегідь розроблених планів дій;

недостатня кількість кваліфікованих кадрів та обмежені можливості для їх навчання та підвищення кваліфікації. Недостатній рівень кваліфікації персоналу може призвести до помилок у роботі та погіршення безпеки інфраструктури;

відсутність достатнього фінансування на розвиток та модернізацію критичної інфраструктури. Недостатнє фінансування може призвести до зростання ризиків техногенних катастроф та збоїв в роботі інфраструктури.

Наряду з зазначеними проблемами існує важливе завдання оцінювання техногенних загроз і ризиків для критичної інфраструктури України в умовах повномасштабного вторгнення російської федерації. Для її виконання необхідно мати належні теоретичні та методологічні основи.

Оцінювання техногенних загроз та ризиків полягає в ідентифікації потенційно-небезпечних подій, які можуть статися в результаті непередбачуваних факторів, технічних збоїв, катастроф, природних катаклізмів тощо. При оцінці ризиків необхідно визначити ймовірність того, що такі події стануться, а також їх наслідки для критичної інфраструктури та населення, що залежить від неї.

Оцінювання техногенних загроз і ризиків для критичної інфраструктури України в умовах повномасштабного вторгнення російської федерації може базуватися на наступних методологічних підходах [1]:

проведення аналізу можливих загроз для критичної інфраструктури України, що можуть виникнути під час ведення бойових дій. До таких загроз можуть відноситися вогневий вплив противника на об'єкти ядерної та хімічної промисловості, енергопостачання, водопостачання та інші інфраструктурні об'єкти;

оцінка можливих наслідків в разі реалізації цих загроз для критичної інфраструктури. Цей підхід дозволяє визначити потенційні наслідки техногенних загроз, таких як ядерний тероризм, виведення з ладу енергетичної системи країни, забруднення води та повітря, зниження мобільності та інші;

оцінка ризиків, пов'язаних з можливими загрозами для критичної інфраструктури. Цей підхід дозволяє визначити рівень ризику виникнення негативних наслідків техногенних загроз та спланувати заходи щодо їх управління;

визначення критичних об'єктів інфраструктури, які є ключовими для безперервного функціонування країни в умовах вторгнення. Цей підхід дозволяє спрямувати увагу та ресурси на найбільш вразливі об'єкти та забезпечити їх захист.

Виходячи з вищезазначеного розробка та впровадження заходів захисту критичної інфраструктури України в умовах повномасштабного вторгнення російської федерації може включати наступні кроки [2]:

розробка планів екстреного реагування та впровадження заходів щодо захисту критичної інфраструктури;

забезпечення захисту інформації про критичну інфраструктуру, що забезпечує безперервну роботу країни. Це може включати захист комп'ютерних систем, інформаційних мереж та інших інфраструктурних систем від кібератак;

забезпечення безпеки персоналу, який займається керуванням та підтримкою критичної інфраструктури. Це може включати проведення навчань та тренувань з евакуації, безпеки праці та інших аспектів безпеки;

розробка та впровадження систем моніторингу, які дозволяють вчасно виявляти загрози та вживати необхідні заходи щодо їх управління. Це може включати системи контролю ХБРЯ обстановки, якості води, повітря та інших елементів інфраструктури;

взаємодія з структурами управління та відповідними відомствами для координації заходів щодо захисту критичної інфраструктури. Це може включати взаємодію з Міністерством оборони, Міністерством внутрішніх справ, Міністерством енергетики та іншими структурами;

створення єдиного державного координаційного органу, який буде забезпечувати належну координацію між різними відомствами та структурами, які займаються захистом критичної інфраструктури. Цей орган має мати відповідальність за розробку та впровадження єдиного підходу до захисту критичної інфраструктури, а також за оцінку ризиків та виявлення загроз.

Висновки

Таким чином, зазначені теоретичні і методологічні основи оцінювання техногенних загроз і ризиків для критичної інфраструктури України дозволять підвищити ефективність реалізації існуючих планів захисту критичної інфраструктури країни в умовах повномасштабного вторгнення російської федерації.

Література

4. Методичні підходи до оцінки техногенних ризиків для критичної інфраструктури // В. В. Баканов, О. О. Лебедєва, А. А. Тіхонов, та ін. Військова гігієна та здоров'я. – 2016. – No 2 (44). – С. 44-50. https://www.researchgate.net/publication/313768316_Metodichni_pidkhodi_do_otsinki_tekhnogennikh_rizikiv_dlya_kritichnoi_infrastrukturi.

5. Оцінка ризиків техногенних катастроф на критичній інфраструктурі в умовах воєнного конфлікту // Є. В. Горовий, І. В. Старков, В. О. Ємець.

УДК 517.537.6

19.ДОСЛІДЖЕННЯ ГЕОМЕТРИЧНИХ ВЛАСТИВОСТЕЙ ДИФЕРЕНЦІАЛЬНИХ РІВНЯНЬ З КОМПЛЕКСНИМИ КОЕФІЦІЄНТАМИ

Медведєв М.Г.[1], Мулява О.М. [2]
1 Таврійський національний університет імені В.І. Вернадського
E-mail: medvediev.mykola@tnu.edu.ua
2 Національний університет харчових технологій, Київ, Україна
E-mail: oksanasheremeta42@gmail.com

INVESTIGATION OF GEOMETRIC PROPERTIES OF DIFFERENTIAL EQUATIONS WITH COMPLEX COEFFICIENTS

Pseudostar, pseudoconvex, and near-pseudoconvex Dirichlet series, which satisfy differential equations with exponential coefficients, are studied. For Dirichlet series with zero abscissa of absolute convergence, the concepts of pseudostardom, pseudoconvexity, and proximity to pseudoconvexity are introduced. The results obtained are applicable to the study of the properties of solutions of differential equations with exponential coefficients. Sufficient conditions are obtained for the parameters under which the Shach differential equation has convex meromorphic solutions of order $\alpha \in [0,1)$ *and type.* $\beta \in [0,1)$.

Для неоднорідного диференціального рівняння $z^2 w'' + (\beta_0 z^2 + \beta_1 z) w' + (\gamma_0 z^2 + \gamma_1 z + \gamma_2) w = A(z)$ з комплексними коефіцієнтами вивчені геометричні властивості в одиничному крузі його розв'язків (опуклість, зірковість, близькість до опуклості) [1].

Побудовано матричні відображення аналітичних послідовностей. Послідовність (x_n) комплексних чисел називається аналітичною стосовно зростаючої до $+\infty$ послідовності (λ_n) додатних чисел, якщо ряд Діріхле з коефіцієнтами x_n і показниками λ_n має абсцису абсолютної збіжності $\sigma_\alpha \in (-\infty; +\infty]$. Узагальненим порядком послідовності (x_n) називається узагальнений порядок відповідного ряду Діріхле. Знайдено необхідну і достатню умову для того, щоб матриця (a_{nk}) відображала клас цілих послідовностей узагальненого порядку $\leq \rho \in (0, +\infty)$ на клас цілих послідовностей узагальненого порядку $\leq \mu \in (0, +\infty)$ [2].

Для аналітичної в крузі $\square = \{z : |z| < 1\}$ функції $f(z) = z + \sum_{k=2}^{\infty} f_k z^k$ Г.С. Салагеан ввів диференціальний оператор D^j за допомогою рівностей $D^0 f(z) = f(z)$, $D^1 f(z) = z f'(z)$, $D^j f(z) = D^1 (D^{j-1} f(z))$ $(j \in N)$, а через $S_j(\alpha)$ позначимо клас функцій

f, для яких $\operatorname{Re}\frac{D^{j+1}f(z)}{D^j f(z)} > \alpha \in [0,1)$ для кожного $z \in \square$. Похідні Салагеана знайшли свої застосування у різних питання геометричної теорії функції. Безпосереднім узагальненням степеневих розвинень аналітичних в $\square$ функцій є абсолютно збіжні у півплощині $\Pi_0 = \{s : \operatorname{Re} s < 0\}$ ряди Діріхле. Припустимо, що $1 < \lambda_k \uparrow +\infty$ і через D позначимо клас абсолютно збіжних в Π_0 рядів Діріхле $F(s) = e^s + \sum_{k=1}^{\infty} f_k \exp\{s\lambda_k\}$ $(s = \sigma + it)$ з $f_k \geq 0$.

Будемо говорити, що функція F∈D належить до $D_j(\alpha)$, якщо $\operatorname{Re}\frac{F^{j+1}(s)}{F^j(s)} > \alpha$ для кожного $s \in \Pi_0$, належить до $D_j^+(\alpha)$, якщо $\frac{F^{j+1}(\sigma)}{F^j(\sigma)} > \alpha$ для всіх σ<0, і належить до $K_j(\alpha)$, якщо $\sum_{k=1}^{\infty} \lambda_k^j (\lambda_k - \alpha) f_k \leq 1 - \alpha$. Доведено, що $D_j(\alpha) \in D_j^+(\alpha) = K_j(\alpha)$. Для вказаного ряду Діріхле множина $O_{j,\delta}(F)$ таких рядів Діріхле $G(s) = e^s - \sum_{k=1}^{\infty} g_k \exp\{s\lambda_k\}$, що $\sum_{k=1}^{\infty} \lambda_k^{j+1} |g_k - f_k| \leq \delta$, називається околом функції F.

Досліджено, які функції входять до $O_{j,\delta}(F)$. Доведено, що диференціальне рівняння $\frac{d^2w}{ds^2} + \left(\gamma_0 e^{2s} + \gamma_1 e^s + \gamma_2\right) w = 0$ з дійсними параметрами має єдиний розв'язок $F(s) = e^s$, що належить до класу $D_j(\alpha)$ для будь яких $\alpha \in [0,1)$, $j \geq 0$. Інших розв'язків, які б належали до класу $D_j(\alpha)$ це рівняння не має, які б не були $\alpha \in [0,1)$, $j \geq 0$.

Для аналітичної в крузі $\square = \{z : |z| < 1\}$ функції

$$f(z) = z + \sum_{k=2}^{\infty} f_k z^k \qquad (1)$$

Г.С. Салагеан означив [3] $D^0 f(z) = f(z)$, $D^1 f(z) = z f'(z)$, $D^j f(z) = D^1\left(D^{j-1} f(z)\right)$ $(j \in N)$ і ввів клас $S_j(\alpha)$ функцій (1), для яких для кожного $z \in \square$.

$$\operatorname{Re}\frac{D^{j+1}f(z)}{D^j f(z)} > \alpha \in [0,1) \qquad (2)$$

Похідні Салагеана використані у працях багатьох авторів (див., наприклад, [4–10]). Якщо в ряді (1) зробимо заміну $z = e^s$, то отримаємо ряд Діріхле

$$F(s) = e^s + \sum_{k=1}^{\infty} f_k \exp\{s\lambda_k\},\ s = \sigma + it, \qquad (3)$$

з показниками $\lambda_k = k$. Зрозуміло, що такий ряд Діріхле буде абсолютно збіжним у півплощині $\Pi_0 = \{s : \operatorname{Re} s < 0\}$, а $F'(s) = e^s f'(e^s) = zf'(z) = D^1 f(z)$ і, отже, $F^{(j)}(s) = D^j f(z)$. При цьому умова (8) матиме вигляд

$$\operatorname{Re}\frac{F^{(j+1)}(s)}{F^{(j)}(s)} > \alpha \in [0,1),\ s \in \Pi_0 \qquad (4).$$

Припустимо тепер, що $1 < \lambda_k \uparrow +\infty$ і через D позначимо клас абсолютно збіжних в Π_0 рядів Діріхле

$$F(s) = e^s + \sum_{k=1}^{\infty} f_k \exp\{s\lambda_k\}\ (f_k \geq 0). \qquad (5)$$

Будемо говорити, що ряд (5) належить до класу $D_j(\alpha)$, як що він задовольняє умову (4), належить до класу $D_j^+(\alpha)$, якщо для всіх $\sigma < 0$

$$\frac{F^{(j+1)}(\sigma)}{F^{(j)}(\sigma)} > \alpha \in [0,1), \qquad (6)$$

і, нарешті, належить до класу $K_j(\alpha)$, якщо

$$\sum_{k=1}^{\infty} \lambda_k^j (\lambda_k - \alpha) f_k \leq 1 - \alpha,\ \alpha \in [0,1). \qquad (7)$$

Згідно з А. Гудманом [11] і С. Рушевеєм [12] околом функції (7) називається множина $N_\delta(f) = \left\{ g(z) = z + \sum_{k=2}^{\infty} g_k z^k : \sum_{k=2}^{\infty} k|g_k - f_k| \leq \delta \right\}$.

Дослідженню околів різних класів аналітичних функцій присвятили свої праці багато авторів (вкажемо тут тільки статті [13–16]). Якщо в (6) виберемо $\alpha = j = 0$, то отримаємо означення псевдозіркової функції (див. [11] і [12, с.147]). У цих працях знайдемо умови на дійсні параметри $\gamma_0, \gamma_1, \gamma_2$, за яких диференціальне рівняння

$$\frac{d^2 w}{ds^2} + \left(\gamma_0 e^{2s} + \gamma_1 e^s + \gamma_2\right) w = 0 \qquad (8)$$

має псевдозірковий розв'язок (5).

Вивчено зв'язок між класами $D_j(\alpha)$, $D_j^+(\alpha)$ і $K_j(\alpha)$, введено поняття околу функції з класу $D_j^+(\alpha)$ і досліджено його властивості, а також досліджено належність рівняння (8) до класу $D_j(\alpha)$.

Література

1. Mulyava, O.M., Sheremeta, M.M., Trukhan, Y. Properties of solutions of a heterogeneous differential equation of the second order // Carpathian Mathematical Publications Volume 11, Issue 2, 2019, Pages 379-398
2. Оксана Мулява, Юрій Трухан, Мирослав Шеремета Про матричні відображення аналітичних послідовностей // Вісник Львівського ун-ту. Серія мех.-мат. – 2017. – Вип..84. – С.87-95.
3. Salagean G.S. Subclasses of univalent functions//Lecture notes in Math. (Springer Verlag). - 1983, V. 1013. - P. 362-372.
4. Al-Oboudi On univalent functions defined by generalized Salagean operator // IJMMS. - 2004. - V. 27. - P. 1429-1436.
5. Joshi S.B., Sangle M.D. New subclasses of univalent functions defined by using generalized Salagean operator // J. Indones. Math. Soc. - 2009. - V. 15, No. 2. - P. 79-89.
6. Aouf M.K., Darwish H.E., Salagean G.S. On a generalization of starlike functions with negative coefficients // Mathematica (Cluj). - 2001. - V. 43. - P. 3-10.
7. Setinkaja A. Convolution properties for Salagean-type analytic functions defined by q-differential operator // Commun. Fac. Sci. Univ. Ank. Ser. A1 Math. Stat. - 2019. - V. 68, No. 2. - P. 1647-1652.
8. Caclar M., Deniz A. Initial coefficients for a subclass of bi-univalent functions defined by Salagean differential operator // Commun. Fac. Sci. Univ. Ank. Ser. A1 Math. Stat. - 2017. - V. 66, No. 1. - P. 85-91.
9. Addul Rahman S. Jumma, Kalkarni S.R. On univalent functions with negative coefficients by using generalized Salagean operator // Fac. Sci. Math., Univ. of Nis, Serbia. - 2007. - V. 21, No. 2. - P. 173-184.
10. Sheremeta M.M. Hadamard composition of Gelfond-Leont'tev-SaLˇ agean and Gelfond-ˇ Leont'tev-Ruscheweyh derivatives of functions analytic in the unit disc // Mat. Stud. - 2020. - V. 54, No. 2. - P. 115-134.
11. Goodman A.W. Univalent functions and nonanalytic curves // Proc. Amer. Math. Soc. -1957. - V. 8. - P. 598-601.
12. Ruscheweyh S. Neighborhoods of univalent functions // Proc. Amer. Math. Soc. -1981. - V. 81, No.4. - P. 521-527.
13. Fournier R. A note on neighborhoods of univalent functions // Proc. Amer. Math. Soc. -1983. - V. 87, No.1. - P. 117-121.
14. Silverman H. Neighborhoods of a class of analytic functions // Far East J. Math. Sci. -1995. - V. 3, No.2. - P. 165-169.
15. Altintas O., Neighborhoods of certain analytic functions with negative coefficients // Internat. J. Math. and Math. Sci. -1996. - V. 13, No. 4. - P. 210-219.
16. Altintas O., Ozkan O., Srivastava H.M. Neighborhoods of a class of analytic functions with negative coefficients // Applied Math. Lettr. - 2000. - V. 13. - P. 63-65

УДК 351.862

20.ПОРЯДОК ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЗАХОДІВ З ОЧИЩЕННЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД ВИБУХОНЕБЕЗПЕЧНИХ ПРЕДМЕТІВ ПІД ЧАС ВІЙНИ

Передрій О.В.[1], Комісаров М.В.[2]
1. Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ, Україна
2. Науково-методичний центр організації наукової та науково-технічної діяльності Національного університету оборони України імені Івана Черняховського, Київ, Україна
E-mail: pomichnik2@gmail.com, maksymkomisarov72@gmail.com

Procedure for assessing the efficiency of measures for cleaning critical infrastructure objects from explosive objects during war

Problematic issues related to the organization of measures to clean critical infrastructure objects (CIO) from explosive ordnance (EO) during the war were considered, with the aim of forming a procedure for evaluating the effectiveness of these measures by the Armed Forces (AF) of Ukraine and the State Emergency Service of Ukraine. Cleaning of critical infrastructure objects from explosive objects during wartime means a set of measures aimed at ensuring the survivability and sustainable functioning of CIO.

It is proposed to evaluate the effectiveness of measures to clean up CIOs from EO according to general indicators on the basis of data on the reduction of the area of dangerous zones, the time of activities, determination of the composition of groups for cleaning CIOs from EO, their equipment and methods of operation. The research results can be used as a basis for the development of a methodical approach to assessing the effectiveness of mine action measures in the AF of Ukraine and State Emergency Service of Ukraine in general.

Аналіз наслідків російського вторгнення в Україну , особливо де велися бойові дії, результати застосування противником засобів вогневого ураження та мінування є серйозною загрозою для живучості та стійкого функціонування ОКІ та персоналу, який виконує на цих об'єктах завдання за призначенням.

За початку повномасштабного вторгнення росії в Україні було пошкоджено 702 ОКІ, а загалом – 35 000 таких об'єктів, як електропідстанції, газопроводи, мости тощо. Наявність мін та боєприпасів, що не вибухнули, впливає на стійкість функціонування ОКІ [1].

Небезпека, пов'язана з мінами та боєприпасами, що не розірвалися, є ключовою проблемою у сфері захисту та становить загрозу ОКІ, перекриває доступ до засобів існування та обмежує можливості для вільного розвитку суспільства [2], [3].

Міністерство оборони України та Державна служба України з надзвичайних ситуацій (ДСНС) докладають всіх зусиль для якнайшвидшого

вирішення питань, що стосуються розмінування ОКІ. Тому актуальність питання визначається необхідністю забезпечення національної стійкості України та безперебійного функціонування ОКІ за рахунок ефективних заходів з їх очищення від (ВЗВ) в умовах агресії з боку рф.

Підвищення можливостей з очищення ОКІ від ВНП багато в чому залежить від результатів оцінювання ефективності заходів, які слід проводити, і ухвалення обґрунтованого рішення щодо їх організації. Це можливо за наявності відповідного методичного апарату, який враховує внутрішні і зовнішні фактори, що впливають на проведення очищення від ВЗВ та особливості їх організації.

З метою формування підходу до оцінювання ефективності заходів з очищення ОКІ від ВНП підрозділами ЗС України та ДСНС необхідно здійснити формалізацію цього процесу на основі вимог нормативно-правових і керівних документів щодо питань їх організації і проведення.

Очищення ОКІ від ВНП повинне ґрунтуватися на принципах:

раціонального поєднання централізованого та децентралізованого управління на основі єдності її планування;

тісної взаємодії суб'єктів виконання завдань, а також всебічного розвитку співпраці з міжнародними організаціями з протимінної діяльності інших держав;

раціонального співвідношення завдань між суб'єктами їх виконання;

єдиної системи підготовки та підвищення кваліфікації кадрів;

загальної інформаційно-аналітичної системи;

єдиної системи випробувань та контролю якості.

Основними складовими заходів з очищення ОКІ від ВНП під час війни є:

інформування про небезпеку від ВЗВ та навчання на ОКІ з попередження ризиків, пов'язаних із ВНП;

очищення від ВНП;

надання допомоги постраждалим особам;

знешкодження та знищення ВЗВ.

Основними завданнями, які стоять перед ЗС України та ДСНС за напрямом відновлення стійкого функціонування ОКІ під час війни, слід вважати такі:

створення ефективної системи очищення ОКІ від ВНП;

координація та контроль виконання заходів з знешкодження ВЗВ;

впровадження найсучасніших методів розмінування;

виконання заходів з очищення від ВЗВ з дотриманням міжнародних зобов'язань у сфері ПМД;

удосконалення методичної бази оцінювання ефективності заходів з очищення об'єктів від ВЗВ [4] – [9].

Структурну схему підходу до оцінювання ефективності заходів з очищення об'єктів критичної інфраструктури від вибухонебезпечних предметів під час війни наведено на рис. 1. показує, що на всій території

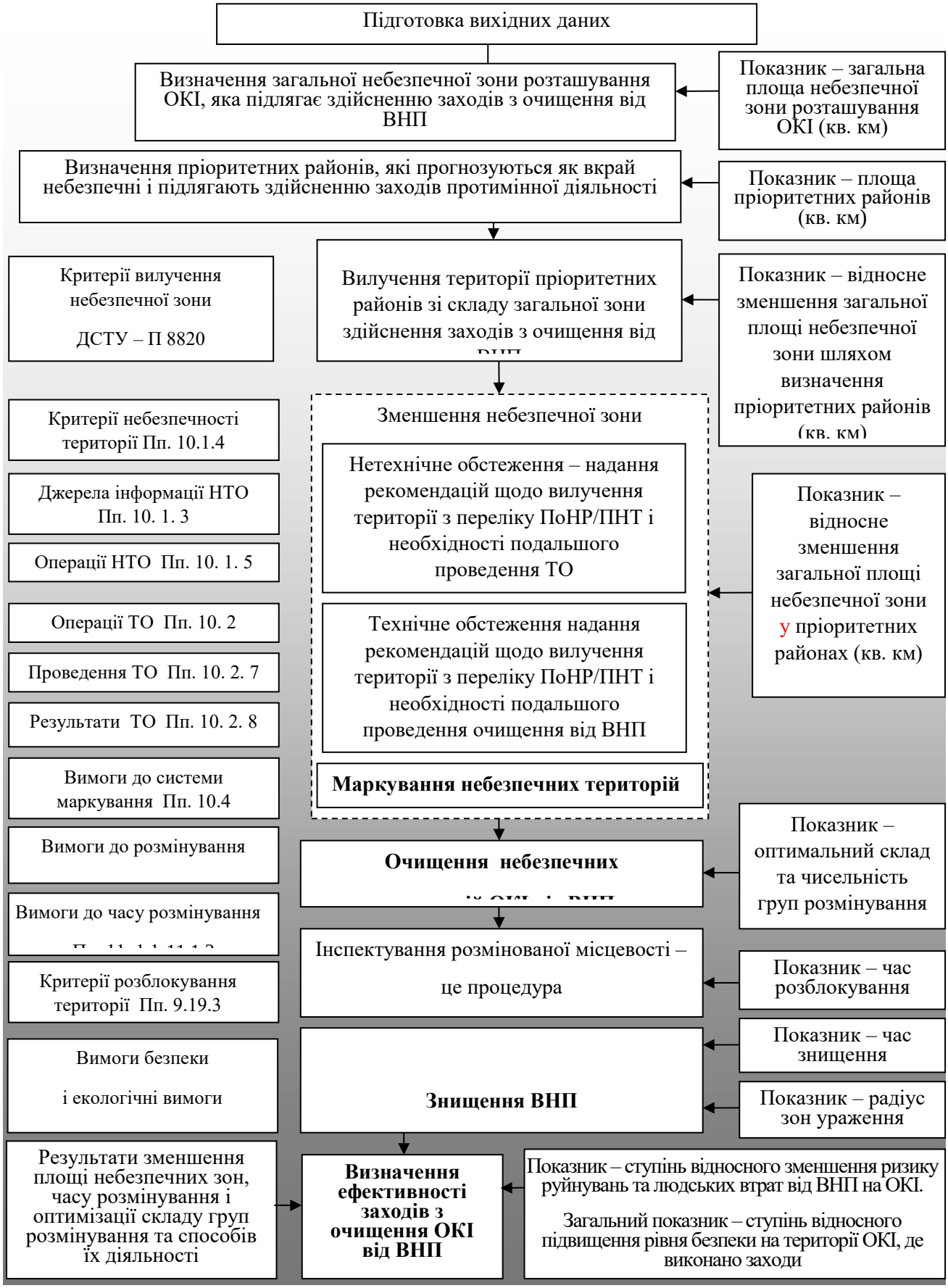


Рисунок 1 – Порядок оцінювання ефективності заходів з очищення об’єктів критичної інфраструктури від вибухонебезпечних предметів під час війни

Проведене дослідження виявило, що оцінювання ефективності заходів з очищення ОКІ від ВНП складається з таких етапів: підготовка вихідних даних; визначення загальної небезпечної зони, яка підлягає здійсненню заходів з очищення від ВНП; визначення пріоритетних районів, які характеризуються як вкрай небезпечні і підлягають здійсненню заходів з очищення від ВНП; нетехнічного обстеження (НТО); технічного обстеження (ТО); маркування небезпечних територій; очищення небезпечних територій ОКІ від ВНП; інспектування очищеної місцевості; знищення ВНП; визначення ефективності проведених заходів.

У лівій частині структурної схеми зазначено вимоги, які є основою для формалізації процесу очищення від ВНП. Права частина містить показники, за якими може здійснюватися оцінювання ефективності заходів очищення від ВНП.

На підставі вимог, які визначено у розглянутих нормативно-правових документах, та змісту заходів, спрямованих на **зниження ризиків** до рівня, коли ОКІ може безперервно функціонувати, а люди можуть виконувати покладені на них завдання **безпечно без обмежень,** пропонується ввести такі загальні показники ефективності:

ступінь ризику людських втрат від ВНП (R, $R \in [0; 1]$) на визначеній території ОКІ (s) або ступінь відносного зменшення цього ризику (δR) завдяки виконанню заходів з очищення від ВНП;

рівень безпеки перебування на ОКІ (B, $B \in [0; 1]$) або ступінь відносного підвищення цього рівня (δB) завдяки виконанню заходів з очищення ОКІ від ВНП.

Ступінь ризику (R) та рівень безпеки (B) можуть бути виражені у якісному та кількісному вигляді за допомогою базової п’ятиступеневої шкали Харрінгтона.

З метою реалізації запропонованої моделі оцінювання ефективності заходів очищення ОКІ від ВНП необхідно розробити комплекс методик, а саме:

1. Методика визначення пріоритетних районів, у яких необхідно здійснювати першочергові заходи очищення від ВНП.

2. Методика визначення площі небезпечної території ОКІ, яка підлягатиме очищенню від ВНП у визначених районах за результатами нетехнічного і технічного обстеження.

3. Методика обґрунтування складу підрозділів, які потрібно залучати до виконання заходів у небезпечних територіях.

4. Методика визначення радіуса зони ураження ВНП під час їх знищення.

Визначення ефективності заходів очищення ОКІ від ВНП здійснюється на підставі результатів зменшення площі небезпечних зон, часу виконання завдань з очищення, оптимізації складу груп розмінування (піротехнічних), їх оснащення та способів діяльності.

Висновки

Таким чином, розглянуто питання стосовно формалізації процесу та порядок оцінювання ефективності заходів очищення об’єктів критичної

інфраструктури (ОКІ) від вибухонебезпечних предметів (ВНП) під час війни. Результати проведених досліджень можуть бути покладені в основу розроблення методики оцінювання ефективності заходів протимінної діяльності у ЗС України та ДСНС.

Література

1. У МВС назвали кількість об'єктів критичної інфраструктури, які пошкодила Росія. URL: https://war.obozrevatel.com/ukr/u-mvs-nazvali-kilkist-obektiv-kritichnoi-infrastrukturi-yaki-poshkodila-rosiya.htm (дата звернення: 01.03. 23.)
2. Україна. Президент (2019– ; В. О. Зеленський). Стратегія національної безпеки України. Указ Президента України від 14.09.2020 № 392/2020. Київ. Офіс Президента України. URL: https://www.president.gov.ua. (дата звернення: 02. 03. 23.)
3. Україна. Президент (2019– ; В. О. Зеленський). Стратегія воєнної безпеки України. Указ Президента України від 25.03.2021 № 121/2021. Київ. Офіс Президента України. URL: https://www.president.gov.ua. (дата звернення: 02. 03. 23.)
4. Україна. Закони. «Про внесення змін до Закону України "Про протимінну діяльність в Україні"». Закон України від 17.09.2020 № 911-IX. Київ. Відомості Верховної Ради України. 2020.
5. Міжнародні стандарти протимінної діяльності. Організація національної програми. URL: https://www.osce.org/ukraine/149431?download=true. (дата звернення: 03. 03. 23.)
6. ДСТУ-П 8820:2018 "Протимінна діяльність". Національний стандарт України. Київ. ДП "УкрНДНЦ". 2019. 85 с.
7. Про затвердження Інструкції з організації та проведення робіт з розмінування місцевості на території України підрозділами та спеціалізованими підприємствами МНС. Наказ Міністерства України з питань надзвичайних ситуацій від 20.09.2010 № 791. Київ. МУ ПНС. 2010.
8. Стандартна оперативна процедура 09.10/ДСНС "Порядок проведення органами та підрозділами цивільного захисту очищення (розмінування) територій, забруднених вибухонебезпечними предметами". Київ. ДСНС. 2017.
9. Ясько В. А., Осадчий А. Н., Ясько А. В. Комплекс заходів з аналізу мінної безпеки та протидії мінній війні. Зб. наук. пр. нац. академії Державної прикордонної служби України. Серія: військові та технічні науки. 2015. № 3 (65). С. 14.

УДК 351: 65.012.8 (477)

21.АНАЛІЗ ФАКТОРІВ ЩО ВПЛИВАЮТЬ НА ПРИЧИНИ ВИНИКНЕННЯ АВАРІЙ НА ГІДРОТЕХНІЧНИХ СПОРУДАХ

Прощин І.В
Національний університет оборони України імені Івана Черняховського, Київ, Україна

ANALYSIS OF FACTORS WHICH ARE INVOLVED IN THE CAUSES OF ACCIDENTS AT HYDROTECHNICAL SPORTS

Hydrotechnical object lie up to the number of the most potentially unsafe man-made objects, their destruction can lead to the death of people, the confusion of dovkill and other irrevocable catastrophic consequences. Poshkodzhennya rowing and other hydrotechnical spores can be damaged, as in the presence of natural forces, they incur stamina, structural defects, violation of the rules of safety engineering during operation. At the present time, there is also a threat of a targeted attack on hydrotechnical disputes by the armed forces of the Russian Federation, even if the aggressor breaks the laws of the civil war to a critical structure during the entire hour of a full-scale war in Ukraine.

Гідротехнічні споруди (об’єкти) належать до числа найбільш потенційно небезпечних техногенних об’єктів, їх руйнування може привести до загибелі людей, забруднення довкілля та інших незворотних катастрофічних наслідків. Пошкодження гребель та інших гідротехнічних споруд може відбутися, як від дії природних сил так і внаслідок втрати ними стійкості, конструктивних дефектів, порушення правил техніки безпеки при експлуатації. Основним чинником гідродинамічної загрози в Україні тривалий час вважався незадовільний стан об'єктів ГТС – гребель, дамб, шлюзів, інших інженерних споруд, призначених для накопичення і концентрування значних об’ємів води. Але на даний час також постала загроза цілеспрямованого ураження гідротехнічних споруд збройними силами російської федерації, адже протягом всього часу повномасштабної війни в України агресор порушує закони та звичаї війни – від злочинів проти цивільного населення до руйнування критичної інфраструктури. Ворог може вдаватися не тільки до пошкодження споруд, а й використовувати їх технічні можливості, для затоплення територій в ході диверсійних операцій. Таким чином, вивчення факторів руйнування гідротехнічних споруд та наслідків такого руйнування в даний час є вкрай актуальним.

Гідротехнічні споруди – споруди для використання водних ресурсів, а також для боротьби з шкідливим впливом вод: греблі й дамби різного призначення та їхні конструктивні елементи; водоскиди, водоспуски, споруди водовідведення: тунелі, канали, труби, лотки; регуляційні споруди, накопичувачі промислових відходів, ставки, відкриті водозабори, гідромеханічне та механічне обладнання, призначене для нормального функціонування споруд [1].

Гідротехнічні споруди дуже різноманітні по конструкції і використовуваних матеріалах зважаючи на розходження їх призначення, місцевих умов будівництва й експлуатації. Гідротехнічні споруди поділяються на: річкові, озерні, морські.

Аварії на гідротехнічних спорудах представляють істотну загрозу для населення, господарських об’єктів та довкілля.

Основними причинами, які можуть викликати аварії на гідротехнічних спорудах, окрім загрози військового ураження, диверсій та терористичних актів, є наступні:

– стихійні лиха (землетруси, урагани, гірські обвали, повені, зливи, селі тощо);

– помилкові оцінки інженерногеологічних, гідрологічних, сейсмічних, кліматичних умов будівництва;

– помилки при проектуванні;

– неякісне виконання робіт (особливо при будівництві порівняно невеликих споруд, коли не забезпечений належний геотехнічний контроль з участю інженерів-гідротехніків);

– неправильна експлуатація споруди (у тому числі зумовлена недостатньою укомплектованістю штатами і технікою, низькою кваліфікацією персоналу, недоліками фінансування, недостатньою забезпеченістю експлуатаційно-методичною документацією тощо);

– відсутність або недостатній обсяг заходів щодо забезпечення готовності об'єкта до локалізації та ліквідації аварійної ситуації; відсутність своєчасних ремонтних робіт;

– техногенні катастрофи [4].

Безпека гідротехнічних споруд залежить від трьох складових:

– адекватність проекту навколишньому середовищу, тобто ступінь обліку природних і антропогенних факторів, що впливають на вибір матеріалів конструкцій і технічних рішень;

– якість будівництва;

– управління і експлуатація, що передбачають проведення постійного контролю за станом і поводженням гідротехнічної споруди.

До основних гідротехнічних споруд, руйнування яких приводить до гідродинамічних аварій, відносяться греблі, водозабірні і водоскидні споруди (шлюзи). Катастрофічне затоплення, що є наслідком гідродинамічної аварії, полягає в стрімкому затопленні місцевості хвилею прориву. Масштаби наслідків гідродинамічних аварій залежать від параметрів і технічного стану гідровузла, характеру і степені руйнування греблі, обсягів запасів води у водоймищі, характеристик хвилі прориву і катастрофічної повені, рельєфу місцевості, сезону і часу доби події і багатьох інших факторів [3].

Основними вражаючими факторами катастрофічного затоплення є: хвиля прориву (висота хвилі, швидкість руху) і тривалість затоплення.

Хвиля прориву – хвиля що утвориться у фронті потоку, що спрямовується в пролом потоком води, має, як правило, значну висоту гребня, швидкість руху, має велику руйнівну силу. Хвиля прориву утворюється при одночасному накладенні двох процесів: падіння вод водоймища з верхнього в ніжний б’єф, що викликає перетік води з цього місця в інші, де рівень води нижче.

Вплив хвилі прориву на об'єкти подібно впливу ударної хвилі повітряно-ядерного вибуху, але відрізняється від нього в першу чергу тим, що діючим тілом тут є вода.

Хвиля прориву з гідравлічної точки зору, є хвилею переміщення, що, на відміну від вітрових хвиль, які виникають на поверхнях великих водойм, має здатність переносити в напрямку свого руху значні маси води. Тому хвилю прориву варто розглядати як визначену масу води, що рухається вниз по річці і безупинно змінює свою форму, розміри і швидкість.

Висота і швидкість хвилі прориву залежать від гідрологічних і топографічних “умов річки”. Наприклад, для рівнинних районів швидкість хвилі прориву коливається від 3 до 25 км/год, а для гірських і передгірних місць має величини порядку 100 км/год. Лісисті ділянки сповільнюють швидкість і зменшують висоту хвилі.

Зона затоплення утворюється в такий спосіб: хвиля прориву у своєму русі уздовж русла ріки безупинно змінює висоту, швидкість руху, ширину й інші параметри. Ця хвиля має зони підйому рівнів води і зони їхнього спаду. Висота води починає інтенсивно збільшуватися, досягаючи через деякій проміжок часу максимальної, перевищуючої брівки берегів ріки, у результаті чого починається затоплення заплав. При цьому утворюються косі течії, що формують головний клин, якій має в плані форму криволінійного трикутника

Після припинення підйому рівнів по всій ширині потоку настає більш-менш тривалий період руху, близький до сталого. Цей період буде тим довше,чім більше обсяг водоймища. Останньою фазою утворення зони затоплення є спад рівнів.

Після проходження хвилі прориву залишається перезволожена заплава і сильно деформоване русло ріки.

У зонах можливого затоплення можуть бути виділені ділянки, що характеризуються ступенем небезпеки для населення, що там знаходиться, і характером впливу на об'єкти народного господарства

На території України зведено близько 1000 водоймищ з обсягом більш 1 млн. м^3 і площею дзеркала більше 1 млн. га. та 24 000, ставків, озер, зведено близько 200 великих гребель. Більшість гребель земляні (з місцевих матеріалів чи намивні). Тільки за останні 30 років в Україні зведено 7 великих каналів довжиною майже 2000 км з подачею на них більш 1000 м^3 води за секунду, 10

великих водоводів великого діаметра, по яких вода подасться в маловодні регіони України [2].

Значну гідродинамічну загрозу в Україні становить незадовільний стан об'єктів ГТС – гребель, дамб, шлюзів, тобто інженерних споруд, призначених для накопичення і концентрування значних об’ємів води. Так, у складі комплексу водозахисних споруд України налічується 3 500 тис. км дамб, 1 200 тис. км. берегоукріплення, понад 600 насосних і компресорних станцій для перекачування надмірних кількостей води, з них на Дніпрі – 308 км. дамб, 325 км берегоукріплювальних споруд, а також 31 насосна і 3 компресорні станції [4]. Через недостатнє фінансування багато з них втрачає надійність і загрожує виникненню надзвичайних ситуацій, аварій та катастроф. Найбільшу гідродинамічну загрозу для населення і навколишнього середовища створює каскад Дніпровських (Київське, Канівське, Кременчуцьке, Дніпродзержинське, Каховське) та Дністровське водосховище.

Висновки

Таким чином вирішення проблематики аварій на гідротехнічних спорудах має включати захисно-профілактичні заходи, налагодження системи попередження, і розробку планів ліквідації можливих наслідків аварій. Наукові розробки, спрямовані на розв’язання прикладних завдань щодо запобігання аваріям мають стати ефективним елементом захисно-профілактичних заходів.

Література

1. Методика обстеження і паспортизації гідротехнічних споруд систем гідравлічного вилучення та складування промислових відходів: затв. наказом Державного комітету України у справах містобудування і архітектури від 19.12.1995р. № 252. С.11.

2. Стан технічної та природної безпеки в Україні у 2001 році Міністерство з питань НС та у справах захисту населення від наслідків Чорнобильської катастрофи: довідник/ Київ. НАН України, 2002 рік. 75 с.

3. Положення про розслідування причин аварій (обвалень), споруд, їх частин та конструктивних елементів: ДБН.В. 1.2-1-95/ Державний Комітет України у справах містобудування і архітектури. Київ 1995 р. С.17-18.

4. Качинський А.Б, Агаркова Н.В. Оцінка ризику як основа стратегії управління безпекою гідротехнічних споруд, С.4-7.– URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/131750/16-Kachinskiy.pdf?sequence=12014(дата звернення: 5.11.2022).

УДК 351.861:338.49

22.МЕТОДИЧНІ ОСНОВИ ОЦІНКИ РИЗИКУ НАДЗВИЧАЙНИХ СИТУАЦІЙ НА ПОТЕНЦІЙНО НЕБЕЗПЕЧНИХ ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Сидоренко В.Л., Єременко С.А., Тищенко В.О., Власенко Є.А.
Інститут державного управління та наукових досліджень з цивільного захисту
E-mail: generals2007@i.ua, esamns@ukr.net, tva_5555@ukr.net, geniy20091@ukr.net

Methodological bases of risk assessment of emergency situations at potentially dangerous facilities of critical infrastructure

The definition of risk in relation to emergency situations at potentially dangerous objects of critical infrastructure is given, and its main components are given. The stages of the concept and the stages of risk analysis, the steps of emergency risk assessment are defined. A quantitative indicator of the risk of emergency situations - individual risk - was applied, and the initial data for its calculation were determined. A ratio has been formed regarding the determination of the quantitative value of the individual risk of man-made and natural emergency situations and the probability of their occurrence.

Як відомо, ризик – це ймовірність заподіяння шкоди життю або здоров'ю громадянина, майну фізичної чи юридичної особи, майну держави або муніципалітету, навколишньому природному середовищу з урахуванням тяжкості шкоди. У математичному формулюванні ризик R є функцією двох змінних: частоти небажаних подій F та небажаних наслідків U: $R=F\times U$. Таким чином, основними компонентами ризику є шкода (збиток), пов'язаний з певною ймовірністю та ймовірність настання цієї шкоди (втрат, збитків), що залежить від частоти прояву ризику, ймовірності настання небезпечного явища і можливості запобігання втратам.

Стосовно надзвичайних ситуацій (далі – НС) це визначення трансформується так: ризик – це міра небезпеки НС, що поєднує в собі ймовірність виникнення НС та її наслідки. Концепція аналізу ризику складається з таких стадій: цілі та основні поняття аналізу ризику, управління ризиками та їх класифікація, застосування аналізу ризику на різних етапах життєвого циклу. Процес аналізу ризиків складається з таких етапів: ідентифікація й оцінка ризиків, аналіз їх частоти, аналіз наслідків, розрахунок невизначеності, перевірка аналізу, комунікація про ризики, документальне обґрунтування та коригування і узгодження результатів аналізу.

Оцінка ризиків НС повинна проводитися для сельбищних територій, прилеглих до потенційно небезпечних об'єктів критичної інфраструктури (далі –

ПНОКІ). Тоді вихідні дані, припущення і гіпотези, а також результати оцінки ризиків НС на об'єктах критичної інфраструктури повинні бути задокументовані й оформлені таким чином, щоб розрахунки і висновки можна було неодноразово перевірити під час експертиз проектної документації чи незалежних аудитів.

Першим кроком в оцінці ризиків НС є процес їх ідентифікації. Ідентифікація ризиків НС передбачає визначення джерел ризику, інцидентів, причин та потенційних наслідків, що виникають до настання НС. Ідентифікація ризиків базується на аналізі основних і допоміжних небезпечних технологічних процесів на об'єктах критичної інфраструктури, об'ємно-планувальних рішень будівель і споруд, компонувальних рішень і конструктивних особливостей обладнання, розташування ПНОКІ по відношенню до сельбищних територій, природно-кліматичних умов, інтенсивності небезпечних природних процесів і явищ. На цьому етапі буде визначено наступне:

- для ПНОКІ – найнебезпечніші ділянки, технологічне обладнання, що містить велику кількість небезпечних речовин або працює під надлишковим тиском, аварії на яких спричиняють найнебезпечніші НС;
- гідротехнічні споруди – виявлення всіх небезпечних елементів гідротехнічних споруд, що можуть спричинити аварії;
- для радіаційно небезпечних об'єктів – небезпечні зони, де аварії, пов'язані з радіоактивним забрудненням навколишнього середовища, можуть спричинити надзвичайну ситуацію, якщо доза опромінення персоналу та населення в зоні спостереження перевищить встановлене значення, а також найбільш небезпечні зони – технологічне обладнання, що містить найбільшу кількість небезпечних речовин, або обладнання, що працює під надлишковим тиском, аварії на яких спричиняють найбільш небезпечні НС. Також визначаються категорії небезпеки процесів та природних явищ, що можуть спричинити НС на ПНОКІ. Наступним кроком є аналіз ризиків НС. Аналіз ризиків НС – це обґрунтоване визначення джерел ризику НС, ймовірності виникнення та наслідків НС.

Під час оцінки ризику НС на ПНОКІ рекомендується використовувати наступний кількісний показник ризику НС: індивідуальний ризик – імовірність загибелі за рік окремої людини на розглянутій території в результаті можливого впливу всієї сукупності уражаючих факторів джерел НС. Вихідними даними для розрахунку є:

1) результати визначення (розрахунку) меж і характеристик зон впливу уражаючих чинників аварій, що можуть привести до техногенної НС як на ПНОКІ, так і за його межами;

2) імовірності виникнення техногенних НС;

3) категорії небезпеки природних процесів і явищ, що можуть привести до виникнення НС на ПНОКІ.

При індивідуальному розрахунку ризику техногенних катастроф рекомендується враховувати найбільш небезпечні чинники аварій, що можуть спричинити техногенні НС, такі як повітряна ударна хвиля, хвилі, що руйнують гідротехнічні споруди, теплове випромінювання, іонізуюче випромінювання та токсичні впливи. У разі визначення кількісних показників ризику промислових

катастроф слід враховувати лише аварії, що спричиняють більше, ніж локальні руйнування. Під час обчислення кількісного значення індивідуального ризику НС пропонується враховувати небезпечні природні явища, такі як зсуви, селі, лавини, повені, урагани, землетруси тощо, що є джерелами природних катастроф. Кількісне значення індивідуального ризику НС у певній точці (x) житлового масиву поблизу ПНОКІ розраховується за наступною залежністю:

$$R(x)=R_T(x)+R_П(x),$$

де $RT(x)$ – кількісне значення індивідуального ризику техногенних НС в певній точці сельбищної зони (x); $RП(x)$ – кількісне значення індивідуального ризику природних НС в певній точці сельбищної зони (x).

Кількісне значення індивідуального ризику техногенних НС в певній точці сельбищної зони (x) поблизу ПНОКІ розраховується за залежністю:

$$R_T(x)=\sum_{i=1}^{N} P_{HC_i}\, Q_{HC_i}(x),$$

де P_{HCi} – імовірність виникнення техногенної НС від i-го джерела; $Q_{ЧСi}(x)$ – імовірність загибелі окремої людини в сельбищній зоні під час виникнення техногенної НС від i-го джерела; i – порядковий номер джерела техногенної НС.

Кількісне значення індивідуального ризику природних НС поблизу ПНОКІ розраховується за залежністю:

$$R_П(x)=\sum_{i=1}^{N} R_П(x)_i,$$

де $R_П(x)$ – значення індивідуального ризику за реалізації наступних природних небезпек: зсуви, селі, лавини, повені, урагани, землетруси, що визначаються за статистичними данням.

Величини кількісного значення ризику НС залежать від повноти і якості вихідних даних. Імовірності виникнення НС визначають за такою залежністю:

$$P_{HC}=Q_i\cdot Q_{HC},$$

де P_{HC} – імовірність виникнення НС; Q_i – частота реалізації протягом року i-го сценарію розвитку аварії, рік$^{-1}$; Q_{HC} – частота виникнення НС після аварії, що визначається за статистичними даними.

Загалом методологічні основи оцінки ризиків виникнення НС на ПНОКІ передбачають комплексний та системний підхід до виявлення, аналізу та управління ризиками, пов’язаними з виникненням аварій на цих об’єктах. Заходи із забезпечення кількісної або якісної оцінки ризику, пов’язаного з конкретною НС, і надання інформації для прийняття рішень удосконалюють стратегію управління ризиками.

Література

Захист критичної інфраструктури в умовах надзвичайних ситуацій: монографія / С.І. Азаров, В.Л. Сидоренко, С.А. Єременко, А.В. Пруський, А.М. Демків; за заг. ред. П.Б. Волянського. Київ, 2021. 375 с. іл.

УДК 351.861:338.49

23.РОЗВИТОК РИЗИКУ НЕБЕЗПЕК НА ПРОМИСЛОВИХ ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Сидоренко В.Л., Пруський А.В., Демків А.М.
Інститут державного управління та наукових досліджень з цивільного захисту
E-mail: generals2007@i.ua, prusskiy@ukr.net, kleo_dan@ukr.net

Development of the risk of hazards at industrial facilities of critical infrastructure

The reasons that increase the level of risk of accidents at industrial objects of critical infrastructure are given, as well as the necessary and sufficient conditions for its occurrence. A general algorithm for the formation of dangerous situations at the specified facilities is provided. A functional model of risk development at industrial facilities of critical infrastructure is presented. General features of objective risk and measures to reduce its level are indicated.

На процеси генерації та розвитку ризиків небезпек впливають різноманітні чинники та умови, що характерні промисловим об’єктам критичної інфраструктури (далі – ПОКІ) (рис.). Знайомство із заданим сценарієм дозволяє виявити багато причин ризику: вихід з ладу установок і обладнання через недоліки конструкції, неякісне технічне виготовлення або порушення правил обслуговування, відхилення від нормальних умов експлуатації, помилки персоналу, зовнішні впливи тощо. Через можливість виникнення вищевказаних причин ПОКІ часто перебувають у нестабільному стані, що особливо важливо для виробничої безпеки критичної інфраструктури в аварійних ситуаціях. Ризики виникають, коли виконуються такі необхідні та достатні умови: 1) наявність чинників ризику (джерела небезпеки); 2) чинник ризику присутній у певних небезпечних (чи шкідливих) дозах для робітників; 3) вплив на чутливість суб'єкта до чинників ризику.

Існує чітка схожість між аваріями у різних галузях. Часто інцидентам передують накопичення дефектів обладнання або відхилення від нормальних процесів експлуатації. Ця фаза може тривати хвилини, дні або навіть роки. Сама по собі несправність або відхилення не є причиною аварії, але вона закладає передумови для неї. Часто оператори не помічають цю фазу через неуважність до правил або відсутність інформації про роботу об'єкта, тому не відчувають небезпеки. На наступному етапі відбуваються несподівані або рідкісні події, що істотно змінюють ситуацію. Оператори намагаються відновити нормальний хід технологічного процесу, але без повної інформації і практичного досвіду часто лише посилюють розвиток аварійної ситуації. Нарешті, на завершальній стадії, ще одна несподівана подія, – часом дуже

незначна – дає поштовх, після якого технологічна система перестає слухатися людини і стається лихо.

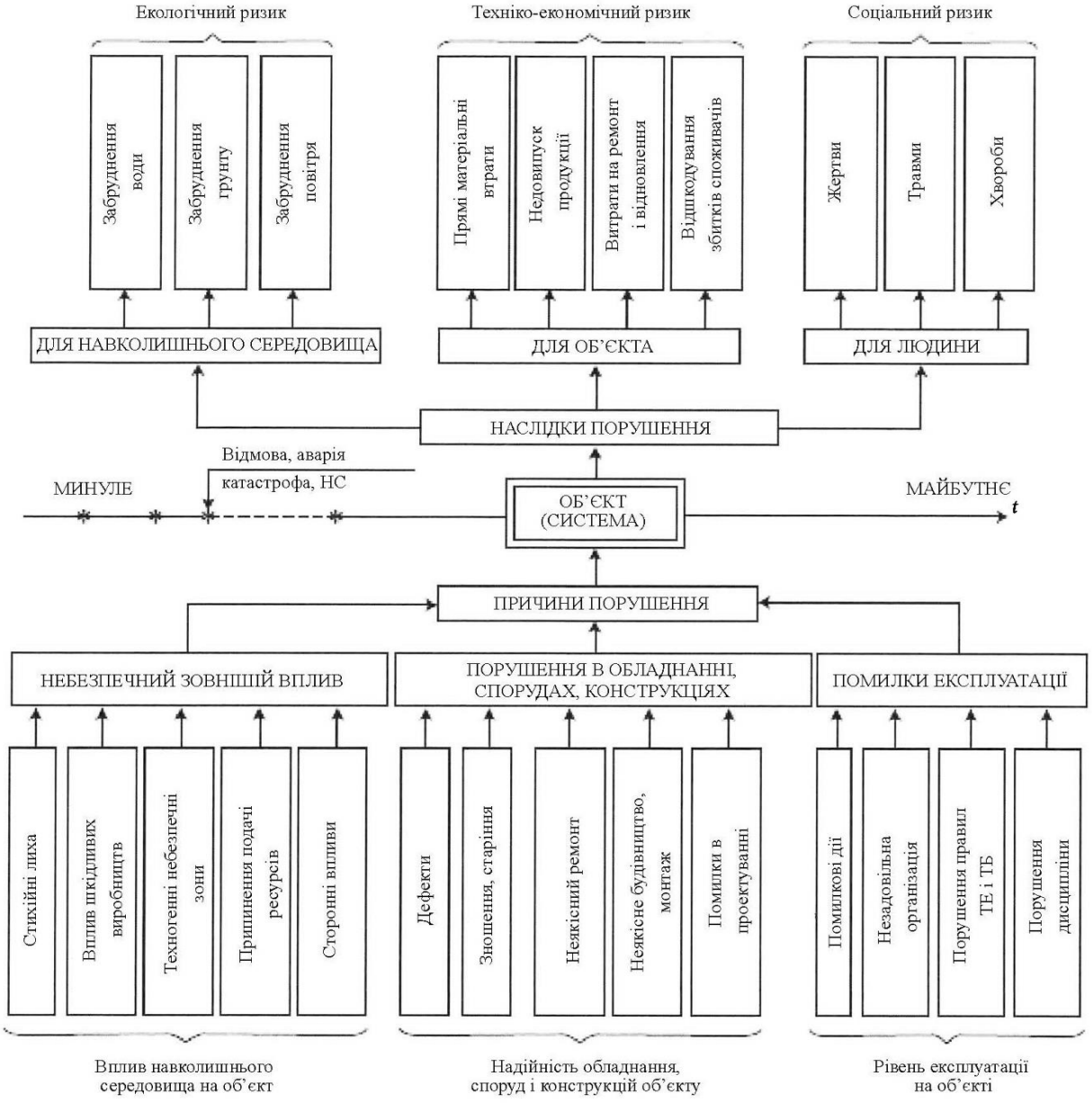


Рисунок. Функціональна модель розвитку ризику на ПОКІ

Ризик є неминучим, супутнім чинником промислової діяльності. Для об'єктивного ризику характерні несподіванка, раптовість настання, що передбачає прогноз ризику, його аналіз, оцінку і управління – ряд дій з недопущення посилення чинників ризику чи послаблення впливу небезпеки.

Отже, розвиток ризику небезпек на ПОКІ є постійним процесом, який потребує регулярної переоцінки та перегляду для врахування змін у робочому середовищі, нових небезпек і нових стратегій управління ризиками.

Література

Захист критичної інфраструктури в умовах надзвичайних ситуацій:

монографія / С.І. Азаров, В.Л. Сидоренко, С.А. Єременко, А.В. Пруський, А.М. Демків; за заг. ред. П.Б. Волянського. Київ, 2021. 375 с. іл.

УДК 004.056.5

24.ЗАХОДИ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ВІД КІБЕРЗАГРОЗ ТА КІБЕРАТАК

Юдіна Д. О.
Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Київ, Україна
E-mail: diana.yudina22@gmail.com, d.yudina@cip.gov.ua

Cybersecurity measures for critical information infrastructure facilities against cyber threats and cyber attacks

This report outlines the legal framework for cybersecurity of critical information infrastructure. The study of classes of cybersecurity measures for critical information infrastructure facilities was conducted and the cycle of cybersecurity management for critical information infrastructure facilities was explained. The division of categories of cybersecurity measures into two groups is proposed: organizational and technical categories of cybersecurity measures for their convenient processing when determining the state of cybersecurity of critical information infrastructure facilities.

Одним з основних чинників, що створює небезпеку об'єктам критичної інфраструктури (далі – ОКІ) є кіберзагрози та кібератаки. російська федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у війні проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно об'єктів критичної інформаційної інфраструктури (далі – ОКІІ) ОКІ. Таким чином, виникає гостра необхідність у забезпеченні на належному рівні кіберзахисту ОКІІ ОКІ.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» [1]; Стратегії кібербезпеки України, затвердженої рішенням Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України», уведеної в дію Указом Президента України від 26 серпня 2021 року № 447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» [2] кібербезпека ОКІІ визначена пріоритетним напрямком наукових досліджень.

Видами діяльності у сфері забезпечення кібербезпеки є: кібероборона, кіберзахист, протидія кібертероризму, кібершпигунству та кіберзлочинності, кіберрозвідка та кібердипломатія, а також координація діяльності за цими видами. Така діяльність спрямована на нейтралізацію різних видів джерел загроз та на захист людини, процесів та інформаційних технологій.

Кіберзахист, як складова забезпечення кібербезпеки держави, є сукупністю організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем [1].

Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 06 жовтня 2021 року (із змінами, внесеними згідно з наказами Адміністрації Держспецзв'язку від 12.10.2021 № 616 та від 10.07.2022 № 343) затверджено Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури (далі – Методичні рекомендації) [3]. Зазначені Методичні рекомендації розроблено з урахуванням Настанови для підвищення кібербезпеки критичної інфраструктури (Framework for Improving Critical Infrastructure Cybersecurity), виданої у 2014 році та оновленої у 2018 році Національним інститутом стандартів та технології Сполучених Штатів Америки (National Institute of Standards and Technology). Вони об'єднують найкращі світові практики та чинну нормативно-правову базу у сфері кібербезпеки. Методичні рекомендації визначають мету, складові рекомендацій, систему заходів кіберзахисту, що складається з чотирьох елементів: клас заходів кіберзахисту; категорія заходів кіберзахисту; підкатегорія заходів кіберзахисту; інформаційні посилання.

Діяльність із забезпечення кібербезпеки спрямована на зниження ризиків кібербезпеки, носить безперервний циклічний характер та формує цикл управління кібербезпекою, який складається з п'яти функцій кібербезпеки, які відповідають п'яти класам заходів кіберзахисту: Ідентифікація ризиків кібербезпеки, Кіберзахист, Виявлення кіберінцидентів, Реагування на кіберінциденти та Відновлення стану кібербезпеки.

Ціль класу заходів кіберзахисту «Ідентифікація ризиків кібербезпеки» - розвинути розуміння того, як краще керувати ризиками кібербезпеки (визначення важливих об'єктів та процесів, інвентаризація апаратного та програмного забезпечення, створення політики кібербезпеки з визначеними ролями та обов'язками, ідентифікація загроз та вразливостей тощо).

Ціль класу заходів кіберзахисту «Кіберзахист» - розробити та впровадити запобіжні заходи для забезпечення надання послуг (керування доступом до активів та інформації, захист конфіденційних даних, створення резервних копій, захист апаратного забезпечення, керування вразливостями, а також навчання персоналу тощо).

Ціль класу заходів кіберзахисту «Виявлення кіберінцидентів» - розробити та впровадити відповідні заходи для виявлення подій кібербезпеки (тестування

та оновлення процесів виявлення, ведення та моніторинг журналів, розуміння впливу подій кібербезпеки тощо).

Ціль класу заходів кіберзахисту «Реагування на кіберінциденти» - розробка та впровадження заходів щодо виявлених подій кібербезпеки (створення та оновлення планів реагування тощо).

Ціль класу заходів кіберзахисту «Відновлення стану кібербезпеки» - розробка та впровадження заходів для підтримки стійкості та відновлення можливостей та послуг, що були порушені в результаті подій кібербезпеки (створення та оновлення планів відновлення, зв'язок з громадськістю тощо).

Ці класи заходів кіберзахисту забезпечують: прийняття рішення з управління ризиками кібербезпеки на ОКІІ, вибір та впровадження заходів кіберзахисту, реагування на загрози кібербезпеки та удосконалення кіберзахисту, враховуючи набутий досвід. Система заходів кіберзахисту базується на нормативних документах, національних та міжнародних стандартах, усталеній практиці захисту інформації та забезпечення кібербезпеки, що розвиваються разом з технологіями забезпечення кібербезпеки. Загалом визначено 108 заходів кіберзахисту, що згруповані у категорії заходів кіберзахисту. У процесі обробки та практичного застосування всіх категорій заходів кіберзахисту виникає потреба в поділі зазначених категорій заходів кіберзахисту на групи, а саме на:

- Організаційні категорії заходів кіберзахисту;
- Технічні категорії заходів кіберзахисту.

Зазначена потреба обґрунтована необхідністю обробляти категорії заходів кіберзахисту різними групами фахівців ОКІІ ОКІ – як технічними фахівцями, так і фахівцями в галузі організації діяльності ОКІІ ОКІ.

В Таблиці 1 наведено розподіл категорій заходів кіберзахисту.

Таблиця 1

Клас заходів кіберзахисту	Організаційні заходи кіберзахисту	Технічні заходи кіберзахисту
Ідентифікація ризиків кібербезпеки (ID)	ID.AM Управління активами ID.GV Управління безпекою ID.RA Оцінка ризиків ID.RM Стратегія управління ризиками організації ID.SC Управління ризиками системи постачання	–
Кіберзахист (PR)	PR.AT Обізнаність та навчання	PR.AC Управління ідентифікацією,

	PR.MA Технічне обслуговування PR.PT Технології кіберзахисту	автентифікацією та контроль доступу PR.DS Безпека даних PR.IP Процеси та процедури кіберзахисту PR.MA Технічне обслуговування PR.PT Технології кіберзахисту
Виявлення кіберінцидентів (DE)	DE.AE Аномалії та кіберінциденти DE.DP Процеси виявлення кіберінцидентів	DE.AE Аномалії та кіберінциденти DE.CM Безперервний моніторинг кібербезпеки DE.DP Процеси виявлення кіберінцидентів
Реагування на кіберінциденти (RS)	RS.CO Комунікації RS.AN Аналіз RS.MI Мінімізація наслідків RS.IM Удосконалення	RS.RP Планування реагування RS.AN Аналіз RS.MI Мінімізація наслідків
Відновлення стану кібербезпеки (RC)	RC.IM Удосконалення RC.CO Комунікації	RC.RP Планування відновлення

Висновки

1. Проведено дослідження класів заходів кіберзахисту для об’єктів критичної інформаційної інфраструктури та роз’яснено цикл управління кібербезпекою для об’єктів критичної інформаційної інфраструктури.
2. Запропоновано поділ категорій заходів кіберзахисту на дві групи: організаційні та технічні категорії заходів кіберзахисту для зручного їх опрацювання при визначенні стану кіберзахисту об’єктів критичної інформаційної інфраструктури.

Література

1. Про основні засади забезпечення кібербезпеки України : Закон України від 17.08.2022 № 2163-VIII. *Голос України*. 2017. 9 листоп. (№ 208).
2. Офіційний портал Верховної Ради України: Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України».
3. Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури : затв. наказом Адміністрації Державної служби

спеціального зв’язку та захисту інформації України від 06 жовтня 2021 року № 601. URL: https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601 (дата звернення: 20.03.2023).

РОЗДІЛ 3

МЕТОДИ І ЗАСОБИ ОЦІНЮВАННЯ КІБЕРЗАГРОЗ, ТЕХНОГЕННИХ ТА ЕКОЛОГІЧНИХ ЗАГРОЗ І РИЗИКІВ ДЛЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ.

УДК 335.58

25.ON THE ISSUE OF ASSESSMENT OF TECHNOLOGICAL OR ENVIRONMENTAL RISKS OF CRITICAL INFRASTRUCTURE OBJECTS

V. N. Yelisieiev, E. V. Bykova

Institute of Public Administration and Scientific Research on Civil Protection
E-mail: elisev1941@ukr.net, ebykova63@gmail.com

Formulation of the problem. An indispensable condition for the successful functioning of the system of protection of the population and the territories of the state is the construction of an effective strategy for managing the risks of emergency situations and its implementation in order to increase the readiness and effectiveness of the functioning of the unified state system of civil protection.

The issue of state security in general, security in emergency situations (ES) in particular, and the management of this security has recently been considered as a strategic task of the state. The Code of Civil Protection of Ukraine defines that civil protection is the function of the state to protect the population and territories from emergency situations by preventing such situations, eliminating their consequences in peacetime and in special periods, and is carried out according to the principle of maximally possible, economically justified risk reduction occurrence of emergencies. A problematic issue is the scientific substantiation of the mechanism for assessing the risks of emergency occurrence. In modern conditions of hostilities, there is a need to take into account the effect of accumulation of losses.

An indispensable condition for the successful functioning of the system of protection of the population and territories of the state is the construction of an effective strategy for managing the risks of emergency situations (ES) and its implementation in order to increase the readiness and efficiency of the unified state system of civil protection. .

In modern conditions, the strategy has become an integral part of risk management in almost all developed countries of the world.

The issues of state security as a whole, security in emergency situations, including the management of this security, have recently been considered as a strategic task of the state. The Code of Civil Protection of Ukraine defines [1] that civil protection is a function of the state to protect the population and territories from emergency situations by preventing such situations, eliminating their consequences in peacetime and in a special period and is carried out according to the principle of the maximum possible, economically justified reduction in the risk of emergencies. Therefore, one of the priority areas for the development of the State Emergency Service has been the introduction of an effective emergency prevention system to reduce the loss of life. The Code of Civil Protection of Ukraine defines the term for preventing emergencies as a set of legal, socio-economic, political, organizational, technical, sanitary and hygienic and other measures aimed at fulfilling such basic tasks as assessing risk levels, regulating safety, and early response to the threat of emergencies.

Therefore, a problematic issue is the scientific substantiation of the mechanism for assessing the risks of emergencies, especially taking into account the effect of accumulation of damage.

In the Law of Ukraine " On the Basic Principles of State Supervision (Control) in the Sphere of Economic Activity" [2] risk is defined as a quantitative measure of danger, taking into account the likelihood of negative consequences from economic activity and the possible amount of losses from them. This can be represented by the formula

$$R_{ES} = R_{ES} * W_{ES}, \quad (1)$$

where R_{ES} - the risk of ES;

R_{ES} - probability of occurrence of ES;

W_{ES} - losses from ES.

When analyzing and evaluating human safety, it is advisable to consider it from the point of view of life activity in the natural-technogenic-social system. At the same time, it is very important to consider complex risks, which include various factors acting on different temporal and spatial scales, and, as a rule, risks have the effect of accumulating losses under the influence of several striking factors.

These risks as a whole create a risk for the life of the population in the state. Therefore, it is necessary to determine the quantitative indicators of these risks and, based on them, justify and develop measures to prevent emergency situations and reduce losses and damages from them.

Therefore, the task of the report is to develop a variant of the mathematical apparatus for calculating the risks of emergency environmental situations, taking into account the effect of the accumulation of losses.

In the current conditions of the state's vital activity, technogenic and environmental safety is affected by a significant number of permanent hazardous factors that increase the risks of disasters. Moreover, these factors can be repeated a significant number of times. Therefore, the authors set out to develop a mathematical apparatus that would take this situation into account and allow for risk assessment. The authors did not find solutions to these issues in recent research by scientists, so they offered this material.

Currently, there is growing concern in the world in connection with a tangible increase in the number of natural, man-made, social and military emergencies. This requires steps to be taken to improve the management of security levels.

Based on the risk formula (1), the main measure of the degree of danger is the probability with which it can manifest itself.

When calculating the probability of occurrence of emergencies using the methods of probability theory, we will take the designation of probabilities $P_{ES}(t)$ - the probability of occurrence of ES for a period of time t , $P_n(t)$ - probability of non-occurrence of ES for t and normalizing condition $P_{ES}(t) + P_n(t) = 1$. To simplify the calculations and writing formulas, we will accept the stationary mode of operation, i.e. $t \to \infty$, $P_{ES}(t) \to P_{ES}$ [3].

The main difficulty and laboriousness of risk forecasting is to determine the probability of an emergency, especially when this probability depends on several factors, and with the onset of destructive processes, this probability increases, taking into account the influence of these factors with the so-called damage accumulation effect.

In the beginning, we will consider the methodology for calculating the probability of an emergency, taking into account two factors, each of which can lead to an emergency with probabilities.

$$P^1_{ES} = P^1_o + P^1_m + P^1_r + P^1_d \quad (2)$$
$$P^2_{ES} = P^2_o + P^2_m + P^2_r + P^2_d$$

where are the indices o, m, r , d (o is the ES of the object level, m is the NS of the local level, r is the NS of the regional level, d is the NS of the state level).

Let us write down the total compatible probability of the occurrence of NS from two factors $P^{(2)}_{ES}$.

$$P^{(2)}_{ES} = 1 - (1 - P^1_{ES})(1 - P^2_{ES}) = P^1_{ES} + P^2_{ES} - P^1_{ES} P^2_{ES} \quad (3)$$

The normalizing conditions for the probabilities P^1_{ES} and P^2_{ES} are:

$$P^1_n + P^1_o + P^1_m + P^1_r + P^1_d = 1; \quad (4)$$
$$P^2_n + P^2_o + P^2_m + P^2_r + P^2_d = 1;$$

where P^1_n , P^2_n – probabilities of non-occurrence of emergencies from the first and second factors.

To solve the problem of determining the probabilities, we fill in the matrix of compatible probabilities of occurrence of emergencies (Table 1)

Table 1. Matrix of compatible probabilities of occurrence of emergencies

$P^n_{j\_}$	P^1_n	P^1_o	P^1_m	P^1_r	P^1_d
P^2_n	$P^1_d P^2_n$	$P^1_o P^2_n$	$P^1_m P^2_n$	$P^1_r P^2_n$	$P^1_d P^2_n$
P^2_o	$P^1_d P^2_o$	$P^1_o P^2_o$	$P^1_m P^2_o$	$P^1_r P^2_o$	$P^1_d P^2_o$
P^2_m	$P^1_d P^2_m$	$P^1_o P^2_m$	$P^1_m P^2_m$	$P^1_r P^2_m$	$P^1_d P^2_m$
P^2_r	$P^1_d P^2_r$	$P^1_o P^2_r$	$P^1_r P^2_r$	$P^1_r P^2_r$	$P^1_d P^2_r$
P^2_d	$P^1_d P^2_d$	$P^1_o P^2_d$	$P^1_m P^2_d$	$P^1_r P^2_d$	$P^1_d P^2_d$

We define the required probabilities as the sum of pairwise products of the matrix over rows and columns:

$$P^{(2)}_n = P^1_n P^2_n$$
$$P^{(2)}_o = P^1_n P^2_o + P^1_o P^2_n + P^1_o P^2_o \quad (5)$$
$$P^{(2)}_m = P^1_m + P^2_m - P^1_m (P^2_r + P^2_d) - P^2_m (P^1_m + P^1_r + P^1_d)$$

$$P^{(2)}{}_p = P^{1}{}_p + P^{2}{}_p - P^{1}{}_p P^{2}{}_r - P^{1}{}_r P^{2}{}_d - P^{1}{}_d P^{2}{}_r$$

$$P^{(2)}{}_d = P^{1}{}_d + P^{2}{}_d - P^{1}{}_d P^{2}{}_d$$

where $P^{\{2\}}{}_J$ - compatible probabilities of occurrence of emergencies from two factors (J=n, o, m, r, d).

We write down the total compatible probability of occurrence of ES from two factors $P^{(2)}{}_{ES}$

$$P^{(2)}{}_{ES} = P^{(2)}{}_o + P^{(2)}{}_m + P^{(2)}{}_r + P^{(2)}{}_d \quad (6)$$

Using these dependencies by the method of successive calculation of the next pair of factors, etc. we calculate the compatible probability of an emergency from n factors.

$$P^{(n)}{}_{ES} = P^{(n)}{}_o + P^{(n)}{}_m + P^{(n)}{}_r + P^{(n)}{}_d \quad (7)$$

Moreover, with each subsequent calculation of the probability of occurrence of ES, the probability $P^{(n)}{}_d$, the probability of the worst case of ES, will increase. That is, the damage will accumulate.

Using those given in the methodology, having calculated by formula (1) the probability of occurrence of ES from n -factors $P^{(n)}{}_{NES}$ and having determined the losses from the consequences of ES $W^{(n)}{}_{NES}$, we calculate the risk value of ES

$$R^{(n)}{}_{NES} = P^{(n)}{}_{NES} * W^{(n)}{}_{NES} \quad (8)$$

Conclusions

1. The development of an effective emergency risk management strategy and its implementation *is the main prerequisite* for improving the readiness and effectiveness of the functioning of the unified state system of civil protection to prevent and overcome the consequences of emergencies.
2. The developed model makes it possible to quantitatively predict the expected risks of emergencies and plan organizational, engineering, technical and sanitary measures to reduce the level of danger.
3. The complexity of the calculations describes the need to use computer technology in the implementation of this task. Therefore, *the further direction of scientific research* on this issue is the development of computer programs for calculating the probabilities of occurrence of emergency situations, taking into account the effect of accumulation of damage, possible material or financial losses, and on the basis of this, to determine the expected risks of emergency situations.

REFERENCES

1. Code of Civil Protection of Ukraine. (2012). Law of Ukraine of October 2, 2012 № 5403-VI.
2. On the basic principles of state supervision (control) in the sphere of economic activity. (2007). Law of Ukraine of April 5, 2007 № 877-V.
3. Wentzel, E.S. (1969). Theory of probabilities. M.: Nauka.

УДК 004.832.28

26.METHODOLOGIES IN UTILIZING NEURAL NETWORKS FOR ANALYZING CYBERSECURITY THREATS AND CRITICAL INFRASTRUCTURE OPERATIONS

Тищенко В.С.
Державний університет телекомунікацій
Київ, Україна
E-mail: tvs5vetal@gmail.com

Methodologies in utilizing neural networks for analyzing cybersecurity threats and critical infrastructure operations

The report outlines the latest advancements in using neural networks to model cyber threats and critical infrastructure activities. The paper highlights the importance of accurate modeling in the field of cybersecurity and critical infrastructure protection. It describes the tools and techniques used to develop and train neural networks for modeling these activities. The article also provides several examples of successful applications of neural networks in modeling cyber threats and critical infrastructure activities. This work is essential for developing more effective strategies to protect against cyber threats and to improve the overall security of critical infrastructure systems.

In recent years, there has been a growing interest in the use of neural networks for modeling cyber threats and critical infrastructure activities. Neural networks are a type of machine learning algorithm that can learn patterns from data and make predictions based on those patterns. This has led to the development of software tools and techniques that can aid in the analysis and prediction of cyber threats and critical infrastructure activities [1].

One of the key advantages of using neural networks for modeling these types of systems is their ability to learn from large amounts of data. This is particularly useful for cyber threat modeling, where there is often a vast amount of data to analyze. Neural networks can also be used to model the behavior of critical infrastructure systems, such as power grids or transportation networks, and predict the likelihood of failure or disruption [2].

Several software tools have been developed for modeling cyber threats and critical infrastructure activities using neural networks. These tools include NeuralToolBox [3], CyberDefender [4], and CRITISIM [5]. These tools offer a range of features, such as data visualization, model training, and prediction, which can be customized to meet the specific needs of the user.

Recent research has shown that neural networks can be effectively used for modeling and predicting cyber threats [3][4]. The use of neural networks for modeling environmental processes and man-made activities has also been well-established [5][6].

The combination of neural networks and software tools can provide a powerful solution for modeling and analyzing complex systems. Such tools have been used for modeling various critical infrastructure systems, such as energy and transportation systems [7][8].

The development of software tools for modeling cyber threats and critical infrastructure activities using neural networks has the potential to revolutionize the field of cybersecurity and critical infrastructure protection. By providing a more accurate understanding of these complex systems, such tools can help improve decision-making and response capabilities.

For example, neural networks can be used to model cyber attacks on critical infrastructure systems such as power grids or water treatment plants. By analyzing large amounts of data on past attacks and system vulnerabilities, these models can help identify potential future threats and suggest ways to mitigate them [9].

Neural networks can also be used to analyze environmental processes, such as weather patterns or natural disasters, and predict their impact on critical infrastructure. For instance, they can help predict the likelihood of flooding or landslides and provide early warning to prevent damage to infrastructure [10].

Furthermore, neural networks can assist in modeling man-made activities that can pose a threat to critical infrastructure, such as terrorist attacks or transportation accidents. By analyzing patterns in data on these activities, these models can help identify potential risks and inform decision-making around security measures and emergency response plans .

Overall, the use of neural networks in modeling and analyzing critical infrastructure activities holds great potential for enhancing security and resilience in the face of cyber threats, natural disasters, and man-made risks.

Conclusions

The neural networks approach can also be applied to the modeling of environmental processes, such as weather forecasting and natural disaster prediction. In recent years, various studies have demonstrated the effectiveness of using neural networks for modeling and predicting natural disasters, such as floods, hurricanes, and earthquakes.

Overall, the use of neural networks for modeling and analyzing complex systems has gained significant attention in recent years. The ability of neural networks to learn complex relationships between input and output data makes them a powerful tool for analyzing and predicting complex phenomena. The development of software tools for neural network modeling has made it easier for researchers and practitioners to apply this approach to various applications, including cyber threat modeling, critical infrastructure analysis, and environmental modeling.

References

1. M. Moustafa and S. Slay, "A Deep Learning Approach for Network Intrusion Detection System," in IEEE Access, vol. 5, pp. 21954-21961, 2017. DOI: http://dx.doi.org/10.21533/pen.v7i3.635
2. J. Zhu, Y. Gao and S. Mei, "Neural Networks for Predictive Maintenance of Critical Infrastructure," in IEEE Transactions on Industrial Informatics, vol. 15, no. 4, pp. 2384-2393, 2019.
3. NeuralToolBox, https://www.neuraltoolbox.org/
4. CyberDefender, https://www.cyberdefender.org/
5. CRITISIM, https://critisim.eu/
6. Gholami, A. et al. "A Software Tool for Modeling and Analyzing Energy Systems using Neural Networks." Energy, vol. 200, pp. 117530, Dec. 2020.
7. Nazemi, A. et al. "A Neural Network-Based Tool for Predicting Traffic Flow in Urban Transportation Networks." IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 4, pp. 2324-2337, Apr. 2021.
8. O. Abdullah, M. Hossain, N. Karim, and J. Zhang, "A survey on deep learning for cybersecurity," IEEE Access, vol. 6, pp. 65900-65918, 2018.
9. S. V. Suren and A. W. Min, "Application of artificial neural networks in predicting the impacts of extreme weather on critical infrastructure," Journal of Cleaner Production, vol. 189, pp. 202-214, 2018.
10. S. R. Hariri, M. A. Al-Fayoumi, and M. Al-Qutayri, "Intelligent intrusion detection system based on deep learning algorithms," Security and Communication Networks, vol. 11, pp. 1744-1757, 2018.

УДК 004.056.5

27.ОЦІНЮВАННЯ РІВНЯ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ КОМПЛЕКСУ ЗАСОБІВ ЗАХИСТУ ЇЇ ОБ'ЄКТІВ ВІД БПЛА

Заїка Н.В.[1], Попель В.А.[1], Чумаченко С.С.[2]

Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації? Київ, Україна
Київський університет ім. Бориса Грінченка? Київ, Україна

E-mail: Nazar2611@gmail.com, v.popel@cip.gov.ua, cumacenkosergij@gmail.com

В роботі проведено аналіз відомих підходів до оцінювання рівнів безпеки і обробки ризиків, пов'язаних із застосуванням терористами та ворогом безпілотних літальних апаратів для розвідки, пошкодження та віддаленої кібератаки по об'єктам критичної інфраструктури.

До чинників, що призводить до похибок оцінки цих ризиків, є вирішення задачі

своєчасного виявлення безпілотних літальних апаратів. Проблеми виявлення та розпізнавання цілей обумовлені їх малими розмірами та масо-габаритними характеристиками, що ускладнює їх виявлення навіть на малих відстанях. Це стосується як радіолокаційних засобів розвідки, так і оптико-електронних. Крім того, сам процес виявлення цілей залежить від ступеню його автоматизації. Процес ураження цілей залежить від точності наданих координат БПЛА засобам ураження, точності прицілювання цих засобів та їх тактико-технічних характеристик.

Пропонується розглянути інформаційну модель оцінки ефективності комплексу засобів захисту об'єктів критичної інфраструктури за критерієм ефективність-вартість, що допоможе приймати обґрунтовані рішення щодо побудови оптимальних схем захисту критичної інфраструктури і боротьби з безпілотними літальними апаратами.

Постановка проблеми. Безпілотні літальні апарати (БПЛА), або дрони є досить новими видами озброєнь на полі бою, починаючи з 1980-х років їх активно використовують збройні сили провідних країн світу і вже з'явилися результати їх ефективного застосування в останніх воєнних конфліктах.

Бурний розвиток БПЛА призвів до появи багатьох їх різновидів - від розвідників до ударних дронів «камікадзе», які відрізняються за розмірами та цільовим навантаженням. Відеокадри, що передають дрони-розвідники, і закладені у їх бортовий комп'ютер алгоритми маневрування та виявлення нових шляхів наближення до цілей, збільшують ризики ураження або проведення результативної атаки по об'єктам критичної інфраструктури (ОКІ). Застосування групи дронів-ретрансляторів – збільшує небезпечну зону віддаленої атаки.

Аналіз останніх досліджень і публікацій. Аналіз публікацій за напрямом протидії БПЛА показує, що наукових статей з даної тематики досить багато. У переважній більшості робіт в цій області переважають надмірно оптимістичні висновки щодо успішності ураження всіх видів БПЛА сучасними засобами ППО та РЕБ [1-3]. Разом з тим, різке та різноманітне вторгнення БПЛА в сучасні бойові дії, їх стрімкий технологічний розвиток виявили проблему ефективної боротьби з ними, особливо з малими БПЛА, яка на даний час залишається надзвичайно складною. Тільки одиниці держав світу мають частково в наявності та розвивають засоби, які спроможні достатньо ефективно протидіяти застосуванню сучасних БПЛА.

Встає питання у об'єктивному порівнянні ефективності технічних рішень захисту критичної інфраструктури і боротьби з сучасними та перспективними БПЛА з обґрунтуванням їх вартості.

Поява нового виду озброєння – БПЛА та їх застосування в останніх воєнних конфліктах виявили суттєві недоліки зенітних комплексів, що стоять на озброєнні в різних країнах. Аналіз характеристик зенітних комплексів протиповітряної оборони провідних країн світу показує, що багато різноманітних заявлених комплексів протиповітряної оборони нібито здатні вражати як БПЛА, так і крилаті ракети «повітря-земля», літаки, вертольоти. Однак, треба усвідомлювати, що боротьба з БПЛА різних класів суттєво відрізняється. Так, дійсно БПЛА великих та середніх розмірів (типу Predator и Reaper від General Atomics) виявляються, супроводжуються та вражаються з

досить високою ефективністю, а з БПЛА малих розмірів виникають суттєві проблеми. В [2] відмічається, що для виявлення малорозмірних БПЛА необхідно застосовувати спеціалізовані засоби розвідки, що мають кращі можливості виявлення та супроводження малорозмірних БПЛА, створювати спеціалізовані канали першочергової передачі розвідувальної інформації про дії малорозмірних БПЛА.

Мета статті - дослідження науково-методичного апарату для оцінювання ефективності системи захисту ОКІ від БПЛА та проведення техніко-економічного аналізу запропонованих технічних рішень ведення боротьби з ними за критерієм ефективність-вартість.

Викладення основного матеріалу. Кожна технічна система (комплекс) захисту ОКІ й боротьби з БПЛА, як складна система, повинна мати у своєму складі ряд технічних складових (підсистем), поєднаних у єдине ціле.

Кожна складна система складається з підсистем, що мають своє цільове призначення. Умовно, у складі складних технічних систем виділяють за призначенням інформаційну, керуючу, виконавчу підсистеми та підсистему забезпечення. Їх спільна робота і повинна забезпечити ефективну роботу всієї системи захисту ОКІ і боротьби з БПЛА.

Зрозуміло, що кожна з наведених підсистем повинна працювати належним чином, з відповідною ефективністю. Їх розробка та виготовлення потребують певного фінансування та визначають кінцеву вартість всієї складної системи. Таким чином, виникає потреба оцінки ефективності складної системи захисту ОКІ і боротьби з БПЛА шляхом оцінки ефективності роботи складових підсистем з оцінкою їх вартісних показників. Вважається, що «ефективністю» є спроможність системи утворювати системний ефект, але така спроможність має кількісну міру. Виходячи з цього, ефективність технічної системи безпеки ОКІ і боротьби з БПЛА (протидії) можна оцінити як результат (або рівень) функціонування всіх чотирьох підсистем, який прагне до максимального значення, за формулою:

$$\mathrm{E}_{\mathrm{TC}}^{\text{захисту}} = \mathrm{E}_j(i) = \ E_1^{B1} \times E_2^{B2} \times E_3^{B3} \times E_4^{B4} \to max, \qquad (1)$$

де E_1^{B1} , E_2^{B2} , E_3^{B3} , E_4^{B4} - відповідно, ефективності інформаційної, керуючої, виконавчої підсистем та підсистеми ресурсного забезпечення;

$B_1, .., B_4$- вагові коефіцієнти критеріїв ефективності інформаційної, керуючої, виконавчої підсистем та підсистеми ресурсного забезпечення,

$$\sum_{j=1}^{4} B_j = 1.$$

Вагові коефіцієнти B_j цільових (часткових) критеріїв ефективності наведених підсистем зазвичай визначаються методом експертних оцінок (і тільки при неможливості проведення експертного опитування, ваги усіх часткових критеріїв приймаються рівновагими $B_j = 1/4$).

За результатами оцінки ефективності способів протидії БПЛА доцільним є подальше порівняння способів за критерієм «ефективність - вартість». Оцінка використання декількох способів протидії зводиться до формування єдиного критерію шляхом згортки цільових критеріїв кожної з підсистем.

Авторами запропонована шкала оцінки ефективності системи безпеки ОКІ і боротьби з БПЛА, що наведена у таблиці 1.

Таблиця 1. Шкала оцінки ефективності системи боротьби з БПЛА і КР

Рівень ефективності	**Значення показника**
Дуже ефективна	$E_{ТС}^{захисту} \geq 0,8$
Ефективна	$0,8 > E_{ТС}^{захисту} \geq 0,6$
Недостатньо ефективна	$0,6 > E_{ТС}^{захисту} \geq 0,4$
Неефективна	$0,4 > E_{ТС}^{захисту} \geq 0,2$
Дуже неефективна	$E_{ТС}^{захисту} < 0,2$

Висновки

Засоби боротьби та протидії з БПЛА доцільно розглядати з системних позицій. Кожна з чотирьох підсистем, що входять до складу технічної системи безпеки ОКІ і боротьби з БПЛА , вносить свій внесок у ефективність цієї системи, що у свою чергу допомагає виявляти найбільш ефективні способи боротьби та протидії в різних умовах обстановки.

Література

1. Cang Liang, Ning Cao, Xiaokai Lu, Youjie Ye. UAV Detection Using Continuous Wave Radar // 2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP), 28-30 Sept. 2018, Singapore. DOI:10.1109/ICICSP.2018.8549736

2. Sineglazov V.M. Complex structure of UAVs detection and identification // Electronics and Control Systems, 2015, no. 3 (45), C. 28 - 32.

3. Igor Korobiichuk, Yuriy Danik, Oleksyj Samchyshyn The estimation algorithm of operative capabilities of complex countermeasures to resist UAVs // Simulation: Transactions of the Society for Modeling and Simulation Innternational, 7 August 2018, vol. 95, pp. 569 – 573. DOI: 10.1177/0037549718791264.

УДК 621.396.4

28.ЗАГРОЗИ БЕЗПЕЦІ МЕРЕЖІ НА КАНАЛЬНОМУ РІВНІ

Івченко О. В., Палагін В. В.

Черкаський державний технологічний університет

E-mail: palahin@ukr.net, o.ivchenko@chdtu.edu.ua

Network security threats at data link level

The article analyzes the main threats to the security of level 2 devices and methods of overcoming them. Analyzed CAM table overflow attacks, VLAN hopping, inter-VLAN and double-tagged VLAN attacks, DHCP related attacks, ARP attacks, address spoofing, STP attacks. The goal of such attacks is intercepting traffic and gaining access to more important confidential information.

Пристрої мережі, які працюють на другому рівні еталонної моделі OSI вважаються найслабшою ланкою в інфраструктурі безпеки [1-3, 6]. Розповсюджена IT-політика BYOD, використання віртуальних мереж і низки складних атак, збільшують вірогідність того, що мережі стають більш уразливими до проникнення саме на рівні L2.

Протоколи рівня L2 дуже часто залишаються без належної уваги і здебільшого працюють зі стандартною конфігурацією.

Слід пам’ятати, що порушення мережної безпеки на рівні L2 також впливатиме на всі рівні, розташовані вище. Таким чином, фахівцям з мережної безпеки потрібно також запобігати і вчасно нейтралізувати атаки на інфраструктуру LAN рівня L2. В роботі проведений аналіз основних загроз безпеці пристроїв рівня 2.

Основні загрози канального рівня

Атаки CAM Table Overflow [3]. До них належать атаки з переповнення таблиць MAC-адрес комутаторів(MAC-флуд). В результаті атаки комутатор починає розсилати кадри, що надходять на всі порти однієї VLAN, що викликає ідеальні умови для перехоплення. Такі атаки спираються на те, що у комутаторів обмежений розмір таблиць MAC-адрес. При заповненні таблиці MAC-адрес зловмисник зможе бачити всі кадри, що розсилаються, з усіх портів однієї VLAN. Атаки CAM Table Overflow можна здійснювати з використанням таких засобів, як macof, Scapy та ін.

Атаки типу VLAN hopping [1, 2] дозволяють зловмисному трафіку потрапляти з однієї VLAN до іншої без допомоги маршрутизатора. Така атака можлива, якщо порт основного мережевого комутатора знаходиться в режимі авто-транк, що характерно для комутаторів Cisco. За допомогою спеціальних засобів можна налаштовати хост на виконання ролі комутатора і скористатися

функцією автоматичного узгодження магістрального порту основного комутатора і отримувати трафік всіх дозволених VLAN.

В середовищі віртуальних машин за допомогою спеціальних засобів (наприклад yersinia) створюються та використовуються спеціальні інтерфейси з можливістю відправлення тегованого трафіку, в результаті чого забезпечується можливість обміну даними з вузлами в окремих мережевих сегментах, доступ до яких розмежовується комутатором за допомогою VLAN.

Атаки переходів між VLAN і VLAN з подвійними тегами. До них також належать атаки, що виникають між пристроями у спільній VLAN [2, 3].

Атаки, пов'язані з DHCP [2, 3]. Призводять до виснаження та підроблення DHCP.

ARP-атаки [3, 4]. До них належать атаки з підміни ARP і отруєння ARP-кешу.

В результаті такої атаки надсилається іншим хостам у підмережі самовільні ARP-відповіді, які містять MAC-адресу зловмисника і IP-адресу шлюзу за замовчуванням, що приводить до отруєння ARP-кешу і підміни шлюзу за замовчуванням.

Для створення атаки посередника з використанням ARP, можуть бути використані dsniff, Cain & Abel, ettercap, Yersinia та інші.

Підроблення адрес [4, 5]. Здійснюються через атаки з підміни MAC- і IP-адрес.

Атаки на STP [2, 3]. Покладаються на маніпуляції з протоколом Spanning Tree.

Висновки

Розглянуті загрози безпеці можуть спричинити перебої в роботи мережі і сприяти перехопленню трафіку зловмисниками, яким вдалося проникнути в область дії рівня L2. Тому залишається важливим захист мережних пристроїв канального рівня і моніторинг роботи мережі.

Література

1. Wendell Odom. CCNA 200-301 Official Cert Guide. Volume 1-2 Cisco Press, 2019. — 1095 p.
2. Chris Carthern, William Wilson, Richard Bedwell, Noel Rivera Cisco Networks: Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA. Apress Media, 2015. — 839 p.
3. Omar Santos, John Stuppi CCNA Security 210-260 Official Cert Guide. Apress Media, 2016. — 608 p.
4. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Юбилейное изд., СПб.: Издательский дом "Питер", 2020. – 1008 стр.
5. Комп'ютерні мережі: [навчальний посібник] / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. — Львів: «Магнолія 2006», 2013. — 256 с.
6. Абрамов В.О., Клименко С.Ю. Базові технології комп'ютерних мереж: навчальний посібник. - К.: Видавнича група «АТОПОЛ», 2014. - 262 с.

УДК 004.056

29.МЕТОДОЛОГІЯ ПІДТВЕРДЖЕННЯ МОЖЛИВОСТІ РЕАЛІЗАЦІЇ ВИЯВЛЕНИХ ВРАЗЛИВОСТЕЙ В КОРПОРАТИВНІЙ МЕРЕЖІ З ВИКОРИСТАННЯМ ПОЛІНОМІАЛЬНИХ ПЕРЕТВОРЕНЬ БЕРНШТЕЙНА

Киричок Р.В.[1], Лаптєв О.А.[2]

1 Київський університет імені Бориса Грінченка, Київ, Україна
2 Київський національний університет імені Тараса Шевченка, Київ, Україна
E-mail: r.kyrychok@kubg.edu.ua, alaptev64@ukr.net

METHODOLOGY FOR CONFIRMING THE FEASIBILITY OF EXPLOITING DETECTED VULNERABILITIES IN A CORPORATE NETWORK USING POLYNOMIAL TRANSFORMATIONS OF BERNSTEIN

This report presents the results of an experimental study of the modern vulnerability exploitation tools functioning. Based on this, general quantitative characteristics of the vulnerability validation process were identified, including the number of successfully and unsuccessfully validated vulnerabilities. To describe the dynamics of this process, taking into account the complex and changing nature of the environment, a mathematical model of the analysis of these characteristics based on Bernstein polynomials was developed. In particular, the proposed model allows to obtain analytical dependencies for the aforementioned characteristics, which in turn makes it possible to build probability distribution laws for them and predict the next values of their magnitudes.

Червень 2017 року – вірус NotPetya атакував інфраструктуру великих компаній, таких як Нова пошта, Нафтогаз, Київенерго, а також інфраструктуру багатьох банків та мобільних операторів.

Грудень 2020 року – в ході спланованої кібероперації було заражене комп'ютерним вірусом програмне забезпечення SolarWinds, яке використовують державні служби та великі корпорації багатьох країн світу.

Це лише пару прикладів найбільш гучних інцидентів кібернетичної безпеки, які призвели до значних фінансових, репутаційних збитків, а також погіршення життєзабезпечення населення відповідної країни на певний період часу, через основні цілі даних кібероперацій, серед яких, значна частина є об'єктами критичної інфраструктури. Щодня кількість об'єктів критичної інфраструктури, які атакують зловмисники, зростає. Особливо це стало актуальним під час пандемії, коли бізнес-процеси перейшли в онлайн-формат, що ще більше привернуло увагу кіберзлочинців. Згідно зі звітом ENISA [1], Агентства Європейського Союзу з кібербезпеки, в 2020-2021 роках зросла кількість атак на так звані «домашні офіси», тобто програмне забезпечення, що дозволяє створювати єдину корпоративну мережу та особисті кабінети працівників задля дистанційної форми праці. Це призвело до збільшення загрози витоку даних для бізнесу з 8,7% у 2020 році до 81% у другому кварталі 2021 року.

Крім того, компанія Accenture зафіксувала у своєму звіті [2] від листопада 2021 року, що 55% компаній (з річним доходом більше 1 млрд. доларів) недостатньо ефективно попереджають кібератаки, надто повільно виявляють та усувають уразливості.

Така тенденція зокрема стала можливою через відносну тривіальність подолання мережевого периметру, оскільки більшість атак носить рутинний характер, а їхня реалізація все ще залишається можливою лише через те, що компанії не здійснюють своєчасне оновлення свого програмного забезпечення, в результаті чого, відомі вразливості роками залишаються «незакритими». Водночас така ситуація ускладнюється динамічним зростанням кількості вразливостей та їх критичності [3], на ряду зі спрощенням проведення атак за рахунок вже готових експлойтів (програмних модулів, що використовують слабкі місця в компонентах інформаційно-комунікаційних систем та вразливості в ПЗ з метою реалізації несанкціонованого впливу на цільову систему, проведення атаки), які можна знайти у відкритих базах, або просто придбати, найчастіше в даркнеті.

За таких умов, для забезпечення безпеки інформаційних систем, важливим напрямком є впровадження превентивних механізмів. Серед таких механізмів, досить перспективними виявляються методи активного аналізу захищеності, оскільки вони дозволяють виявити та підтвердити можливість реалізації конкретних вразливостей. Це, в свою чергу, дозволяє визначити фактичний рівень безпеки інформаційних систем та мереж, на основі чого, вже формувати рекомендації щодо усунення підтверджених вразливостей.

Тому удосконалення технологій своєчасного виявлення та закриття вразливостей у корпоративних мережах, що дозволяють мінімізувати ризик проведення кібератаки, є актуальним питанням.

Отже, виходячи з вищезазначеного, було проведено експериментальне дослідження функціональних можливостей сучасних автоматизованих засобів експлуатації вразливостей в ході якого виявлено, що якість перевірки та підтвердження можливості реалізації вразливостей цільових об’єктів корпоративного мережного оточення можна представити у вигляді вектора (q_s, q_f, q_c) трьохвимірного векторного простору, де q_s – абсциса, яка визначає кількість успішно перевірених вразливостей, q_f – ордината, яка визначає кількість неперевірених вразливостей та q_c – аппліката, яка визначає кількість випадків перевірки вразливостей, що призвели до критичних помилок на цільовому об’єкті та подальшої втрати з ним зв’язку.

В результаті, було побудовано математичну модель аналізу кількісних характеристик процесу підтвердження можливості реалізації вразливостей інформаційних систем методом регресійного аналізу. Для цього, спершу оцінюючи статистичний зв’язок між змінними t і q_s, q_f, q_c з використанням коефіцієнта кореляції R, встановлено його лінійність.

При цьому слід зазначити, що найтісніший лінійний зв’язок спостерігався між значеннями t та q_f . Відповідно, можна стверджувати, що при збільшенні одного значення в середньому збільшується й інше.

Задля подання емпіричних залежностей між параметрами, що описують поведінку процесу підтвердження можливості реалізації вразливостей інформаційних систем в зрозумілій та стислій формі, було прийнято рішення апроксимувати експериментальні дані. Водночас, задля отримання найбільш достовірних коефіцієнтів апроксиманти, скористалися теоремою Бернштейна [4, 5].

Дана теорема полягає в тому, що довільну неперервну функцію *f(t)*, яка визначена і неперервно-диференційована на відрізку [0;1], можна представити у вигляді поліному:

$$B_n(f;t_н) = B_n(t_н) = \sum_{k=0}^{n} f\left(\frac{k}{n}\right) b_{k,n}(t_н), \tag{1}$$

де $b_{k,n}(t_н) = C_n^k t_н^{\,k}(1-t_н)^{n-k}$, $C_n^k = \dfrac{n!}{k!(n-k)!}$, $t_н$ – нормований час.

Виходячи з результатів проведеного експериментального дослідження, було встановлено, що час раціонального циклу перевірки вразливостей у випадку інструменту *Armitage* становить 345 секунд. Тому, спершу, слід нормувати часовий інтервал наступним чином:

$$t_н = \frac{t_i}{T} \tag{2}$$

де T – час перевірки вразливостей цільового об'єкта корпоративного мережного оточення за секунди (час раціонального циклу);

t_i – час, протягом якого відповідні характеристики (q_s, q_f, q_c) приймали свої значення в рамках раціонального циклу.

Після чого, наступним кроком, використовуючи отримані статистичні дані, розрахований нормований час $t_н$ та вираз (1), отримуємо початкові аналітичні залежності для кожної з характеристик. Так, до прикладу, для кількості успішно перевірених вразливостей $q_s=q_s(t_н)$ було отримано наступні початкові аналітичні залежності:

$$\begin{aligned} q_s(t_н) = {} & q_s(0)b_{0.11}(t_н) + q_s(0{,}168)b_{1.11}(t_н) + q_s(0{,}188)b_{2.11}(t_н) + q_s(0{,}206)b_{3.11}(t_н) + \\ & + q_s(0{,}238)b_{4.11}(t_н) + q_s(0{,}241)b_{5.11}(t_н) + q_s(0{,}249)b_{6.11}(t_н) + q_s(0{,}333)b_{7.11}(t_н) + \\ & + q_s(0{,}446)b_{8.11}(t_н) + q_s(0{,}849)b_{9.11}(t_н) + q_s(0{,}957)b_{10.11}(t_н) + q_s(1)b_{11.11}(t_н). \end{aligned}$$

Останнім кроком здійснюємо підстановку відповідних поліномів $b_{k,n}(t_н)$ та вираховуємо безпосередньо самі значення даних аналітичних залежностей:

$$\begin{aligned} q_s(t_н) = {} & b_{1.11}(t_н) + 2b_{2.11}(t_н) + 2b_{4.11}(t_н) + b_{5.11}(t_н) + 3b_{6.11}(t_н) + b_{7.11}(t_н) + \\ & + 3b_{9.11}(t_н) + 3b_{10.11}(t_н) + 3b_{11.11}(t_н). \end{aligned} \tag{3}$$

Аналогічним чином були отримані початкові аналітичні залежності для кількості неперевірених вразливостей $q_f=q_f(t_н)$, (4) та кількість випадків перевірки вразливостей, що призвели до критичних помилок $q_c=q_c(t_н)$, (5):

$$q_f(t_н) = 81b_{1.11}(t_н) + 80b_{2.11}(t_н) + 39b_{3.11}(t_н) + 92b_{4.11}(t_н) +$$
$$+45b_{5.11}(t_н) + 93b_{6.11}(t_н) + 61b_{7.11}(t_н) + 83b_{8.11}(t_н) +$$
$$+762b_{9.11}(t_н) + 777b_{10.11}(t_н) + 306b_{11.11}(t_н). \quad (4)$$
$$q_c(t_н) = b_{1.11}(t_н) + 3b_{2.11}(t_н) + 2b_{4.11}(t_н) +$$
$$+2b_{6.11}(t_н) + b_{7.11}(t_н) + b_{8.11}(t_н) + 3b_{11.11}(t_н). \quad (5)$$

Таким чином, в результаті було отримано наступні аналітичні залежності:

$$q_s(t_н) = \sum_{i=0}^{n} q_s(t_н^{(i)}) b_{k,n}(t_н),$$
$$q_f(t_н) = \sum_{i=0}^{n} q_f(t_н^{(i)}) b_{k,n}(t_н),$$
$$q_c(t_н) = \sum_{i=0}^{n} q_c(t_н^{(i)}) b_{k,n}(t_н).$$

які є остаточними виразами для досліджуваних характеристик процесу перевірки та підтвердження можливості реалізації вразливостей інформаційних систем.

Висновки

1. У ході експериментального дослідження функціонування сучасних засобів експлуатації вразливостей було виявлено узагальнені характеристики процесу перевірки вразливостей.

2. Розроблено математичну модель для аналізу кількісних характеристик процесу перевірки вразливостей з урахуванням складного та мінливого характеру середовища. Особливістю розробленої моделі є застосування поліноміальних перетворень Бернштейна.

3. У ході моделювання аналізу узагальнених кількісних характеристик процесу перевірки вразливостей було виведено їх аналітичні залежності, що повною мірою відображають динаміку цього процесу.

Література

1. ENISA Threat Landscape 2021 (European union agency for cybersecurity) [Електронний ресурс] – Режим доступу до ресурсу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

2. State of Cybersecurity Resilience 2021 (4th Annual Report): How aligning security and the business creates cyber resilience. Accenture. [Електронний ресурс] – Режим доступу до ресурсу: https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf

3. CVSS Severity Distribution Over Time [Електронний ресурс] – Режим доступу: https://nvd.nist.gov/vuln-metrics/visualizations/cvss-severity-distribution-over-time.

4. Approximation and Interpolation, by Philip J. Davis (Dover Publications, 1975), ISBN 3-486-62495-1. Originally published in 1963. "while [Bernstein's proof] is not the simplest conceptually", p. 108.

5. Bernstein Polynomials, by G. G. Lorentz (Chelsea Publishing Company, 1986), ISBN 978-0-8218-7558-2. Originally published in 1953.

УДК 004.056.53

30.ПАРАМЕТРИЧНИЙ МЕТОД СПЕКТРАЛЬНОГО АНАЛІЗУ СИГНАЛІВ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Лаптєв С.О.[1], Собчук А.В.[2], Пономаренко В.В.[2], Барабаш А.О.[3]
[1] Київський національний університет імені Тараса Шевченка, м. Київ, Україна
[2] Державний університет телекомунікацій, м. Київ Україна
[3] Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ Україна
e-mail: salaptiev@gmail.com, anri.sobchuk@gmail.com, Ur_suviator @ukr.net, andrew.barbsh@gmail.com

Parametric method of spectral analysis of signals of critical infrastructure objects

The research established that the method of spectral analysis, based on the classical Prony method, improved by replacing fading sinusoids with the use of non-fading sinusoids, allows you to very accurately isolate the signal and determine its characteristics in a space rich in interference. The method will be useful for tracking unauthorized access to information systems of critical infrastructure facilities. In order to confirm the chosen method of spectral analysis, simulations were carried out and graphs of spectrograms of the pulse signal were obtained using Fourier, Chebyshev, and Bessel methods. The obtained graphical data fully confirm the advantages of our proposed method for the spectral analysis of random short-term pulses

Проблематика моніторингу сигналів пристроїв несанкціонованого доступу до інформаційних систем об'єктів критичної інфраструктури залишається однією з найгостріших проблем сьогодення [1]. Стрімкий розвиток інформаційних технологій вимагає постійного вдосконалення методів моніторингу. Необхідно зазначити, що останнім часом зріс інтерес до параметричних методів спектрального аналізу. Методи спектрального аналізу випадкових сигналів діляться на два великі класи – непараметричні і параметричні. У непараметричних методах використовується тільки інформація, що міститься у даних аналізованого сигналу. Параметричні методи передбачають наявність деякої статистичної моделі випадкового сигналу, а процес спектрального аналізу в даному випадку містити визначення параметрів цієї моделі [2].

Значна роль в аналізі сигналів належить комплексному перетворенню Фур'є [3]. Перетворення Фур'є (ПФ) і його дискретні аналоги (ДПФ) добре відомі та широко застосовуються в техніці спектрального аналізу при стандартній

обробці радіосигналів. Воно ефективно в обчислювальному відношенні та просто в реалізації. Як правило, такі процедури дають хороші результати при аналізі частотного складу тривалих за часом радіосигналів. Однак відомі причини, що обмежують застосування перетворення Фур'є [4] при аналізі коротких сигналів, якими можуть бути цифрові радіоімпульси наприклад, використання ДПФ для усічених за часом сигналів призводить нас до ефектів Гіббса, які спотворюють інформацію про спектр сигналу і не дають можливості забезпечити високу точність в спектральної області при аналізі гармонійних компонент.

Використання віконного перетворення Фур'є покращує оцінювання спектрів, але не дає повного розв'язання зазначеної проблеми.

Виконані за останні кілька десятиліть всебічні дослідження з питань цифрового спектрального оцінювання привели до істотного розвитку сучасних технологій в цій галузі. Прагнення до знаходження перетворень, які краще відповідають невеликої тривалості сигналів, що володіють довільним тимчасово-просторовим становищем, призвело до появи вейвлет-аналізу [5]. В його основі лежать короткі функції, що володіють тимчасової (просторової) і частотною локалізацією, що дає кращу апроксимацію для коротких сигналів і дозволяє точніше визначати їх гармонійні компоненти. Однак використання вейвлет-аналізу при обробці радіосигналів може мати деякі обмеження з точки зору інтерпретації, що пов'язано з формальним вибором деяких ортогональних функцій як базису відповідного перетворення. З вищевикладеного можна зробити висновок що питання перетворення радіо сигналів з подальшим його аналізом остаточно не вирішене і вимагає постійного вдосконалення.

Одним з методів, що дозволяють вирішити вказані недоліки є параметричний метод спектрального аналізу Проні, що використовує уявлення спостережуваного процесу у вигляді комплексного експоненціального ряду. Метод дозволяє за відліком сигналу знайти параметри цих комплексних експонент, що, у свою чергу, дає можливість записати вираз для спектральної щільності досліджуваного сигналу. Широке застосування методу Проні стало можливим тільки останнім часом, оскільки він істотно нелінійний і вимагає великих обчислювальних витрат. У зв'язку з цим виникла необхідність детального дослідження даного методу з точки зору оптимальності його математичної реалізації, а також потенційної стійкості до флуктуацій відліків сигналу і шумів дискретизації.

Нами розглянуто методи спектрального аналізу засновані на використанні будь-якої моделі для опису сигналу, тобто при їх використанні робляться деякі припущення про поведінку сигналу поза інтервалу спостереження. Завдання спектрального оцінювання при цьому зводиться до знаходження параметрів використовуваної моделі, яка вибирається виходячи з наявної апріорної інформації про процес, який досліджується. Запропоновано метод спектрального аналізу, на основі класичного метода Проні, який удосконалений шляхом заміни загасаючих синусоїд на використання незгасних синусоїд, що дозволяє дуже точно виділити сигнал і визначити його характеристики на тлі дуже багатого на

перешкоди ефірного простору. Застосовано алгоритм швидкого перетворення для вирішення нормальних рівнянь знаходження змінних для послідовного визначення параметрів сигналу таких як амплітуда, частота та фаза.

Висновки

Огляд методів спектрального аналізу показав, що метод спектрального аналізу, на основі класичного метода Проні, який удосконалений шляхом заміни загасаючих синусоїд на використання незгасних синусоїд, дозволяє дуже точно виділити сигнал і визначити його характеристики на тлі дуже багатого на перешкоди ефірного простору. Даний метод буде корисним для відслідковування несанкціонованого доступу до інформаційних систем об’єктів критичної інфраструктури. З метою підтвердження обраного методу спектрального аналізу, проведено моделювання та отримані графіки спектрограм імпульсного сигналу за допомогою методів Фур'є, Чебішева, Бесселя. Отримані графічні дані цілком підтверджують переваги запропонованого нами метода, для спектрального аналізу випадкових короткочасних імпульсів.

Література

1. О.А. Лаптєв, В.В. Собчук, В.А. Савченко Метод підвищення завадостійкості системи виявлення, розпізнавання і локалізації цифрових сигналів в інформаційних системах // Колективна монографія Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2019. – Вип. 66. – С. 90 – 104.
2. Laptev A.A. Sachenko V.A., Barabash O.V. Sachenko V.V., Matsko A.I, The method of searching for digital means of illegal obtaining of information on the basis cluster analysis. Magyar Tudományos Journal. Budapest, Hungary № 31. 2019. pp.33 – 37.
3. A. Musienko, A. Laptev, V. Sobchuk, B. Borsuk Методика вибору оптимального вхідного сигналу радіомоніторингу для програмних засобів на базі перетворення Фур’є // Системи управління, навігації та зв’язку. Колективна монографія. – Полтава: ПНТУ, 2019. – Т. 4 (56). – С. 135-140.
4. V. Sobchuk, I. Kal’Chuk, Y. Kharkevych and G. Kharkevych, "Estimations of the Convergence Rate of the Fourier Transformation for Data Processing Efficiency Improvement," *2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT)*, Kyiv, Ukraine, 2021, pp. 76-79, doi: 10.1109/ATIT54053.2021.9678825.
5. Собчук В.В., Можаєв М.О. Застосування вейвлет перетворень для підвищення ефективності інформаційної системи судової експертизи // Телекомунікаційні та інформаційні технології. 2020. №4 (69). С.107–116.
УДК 504.03

31.ОЦІНЮВАННЯ РИЗИКІВ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ З УРАХУВАННЯМ ПОТЕНЦІАЛІВ ЗБИТКІВ ВІД ДЕСТРУКТИВНОГО ВПЛИВУ ПРОТИВНИКА

Мурасов Р.К.[1], Чумаченко С. М.[2].

1Національний університет оборони України імені Івана Черняховського, Київ, Україна

2Національний університет харчових технологій, Київ, Україна

E-mail: rustamm@ukr.net, s_chum@ukr.net

Risk assessment of critical infrastructure facilities, taking into account the potentials of losses from the destructive influence of the enemy

The paper explores the problem of approaches to creating a model for assessing risks from critical infrastructure in the direction of enemy influence. Using graph theory and probability theory, a model has been proposed for assessing risks from critical infrastructure facilities. This model allows to obtain quantitative estimates of the losses of critical infrastructure in the direction of enemy influence and to analyze various scenarios for the development of emergency. The concept of destructive-cumulative potentials of critical infrastructure objects has been introduced.

This work will be useful in the development of simulation models for assessing risks from critical infrastructure in the direction of enemy influence, modeling emergencies.

Актуальність проблеми [1,2] оцінювання ризиків обумовлена в першу чергу складною обстановкою в України, де значна кількість об'єктів критичної інфраструктури знаходиться в зоні впливу ракетно-дронових ударів Російської федерації, в межах ураження яких перебуває значна кількість цивільного населення та особовий склад Збройних сил. Для складних технічних систем, до яких також відноситься критична інфраструктури (системи електроживлення та енергопостачання, водопостачання та водовідведення і т.ін.), актуальною проблемою є забезпечення об'єктивності, достовірності та адекватності прогнозування і попередження надзвичайних ситуацій (НС) і можливих каскадних ефектів, що можуть суттєво вплинути на призвести до техногенних аварій і катастроф або суттєво вплинути на їх функціонування, живучість, еколого-техногенну безпеку. Імовірність виникнення та наслідки таких ситуацій, умов і чинників визначаються як цілеспрямованими (диверсія, бойові дії, саботаж) так і стохастичними процесами, що за своєю сутністю характеризуються як загрози.

В багатьох роботах провідних вчених розглядаються питання імовірнісного характеру – імовірності виникнення та розвитку техногенних катастроф. Але крім імовірності подій необхідно визначити ризик, які є похідною катастрофи. При великому обсязі наукових досліджень, нажаль відсутнє єдине визначення поняття ризику. В різних сферах він має своє специфічне визначення. В єдиному є згода, що це є імовірнісна величина. Вона має комплексний склад, який потребує оптимального врахування необхідних складових процесів, що

беруть участь у формуванні ризику. Для отримання оцінки ризику - R необхідно врахувати збитки, які будуть завдані внаслідок руйнування (пошкодження) об'єктів критичної інфраструктури. Використовується модель, яка пов'язує в собі імовірність виникнення катастрофи (несприятливої події) P_i (i=$\overline{1,n}$) та імовірність нанесених збитків W_i (i=$\overline{1,n}$) внаслідок цих подій:

$$R = \sum_i P_i \times W_i$$

Оцінка ризику [3,4] має передбачати різни розвитки сценаріїв P та імовірність потенційних збитків W. Відповідно кількісті сценаріїв i=$\overline{1,n}$.

Крім того, в дану формулу буде вірним включити різні імовірнісні величини, які мають місце у формуванні ризику. Наприклад пора року – яка має суттєвий вплив на виникнення пожеж, період сильних злів і ураганів. Тривалі низькі температури, які мають вагомий вплив на систему критичної інфраструктури.

$$R = \iiint_{i_{min}}^{i_{max}} P(I)F(x)F(y)F(z)dxdydz$$

Нажаль наведена методика має лише загальний характер визначення ризиків і не дає повного розуміння оцінки потенційних збитків.

Введемо поняття Деструктивно-кумулятивного потенціалу (ДКП) D під яким будемо розуміти інтегральну характеристику кореляційних процесів спрямованих на розвиток катастрофічних подій системи критичної інфраструктури, в глобальних масштабах з великими (понад 1000 чол.) людськими втратами та подальшою ланцюговою реакцією поширення еколого-техногенних катастроф, які також мають прямий вплив на соціальні та економічні сфери.

Деструктивно-кумулятивний потенціал потенційно-небезпечного об'єкту критичної інфраструктури реалізується через утворення площ вторинного ураження техногенними аномаліями і розвиток локальних небезпечних екзогенних геологічних процесів.

Крім того, всі об'єкти критичної інфраструктури мають різну фізичну природу, характер нанесення збитків, тому для унормування їх природи необхідно звести показники значення небезпеки до єдиного виміру, чим і буде ДКП. Необхідність нормалізації потенціалів викликано тим, що різні набори даних можуть бути представлені в різних масштабах і змінюватися в різних діапазонах. Наприклад, період катастрофи, який змінюється від 1 до 100 діб, і витрати на ліквідацію, змінюється від кількох тисяч до кількох мільйонів. У цьому випадку можливе порушення балансу між впливом вхідних даних, представлених у різних масштабах, на вихідній результат.

Оптимальним варіантом нормування є здійснення операції логарифмування. Це дозволить запобігти великому розходженню результатів

оцінювання ризиків потенційно-небезпечних об’єктів критичної інфраструктури Рис.1.

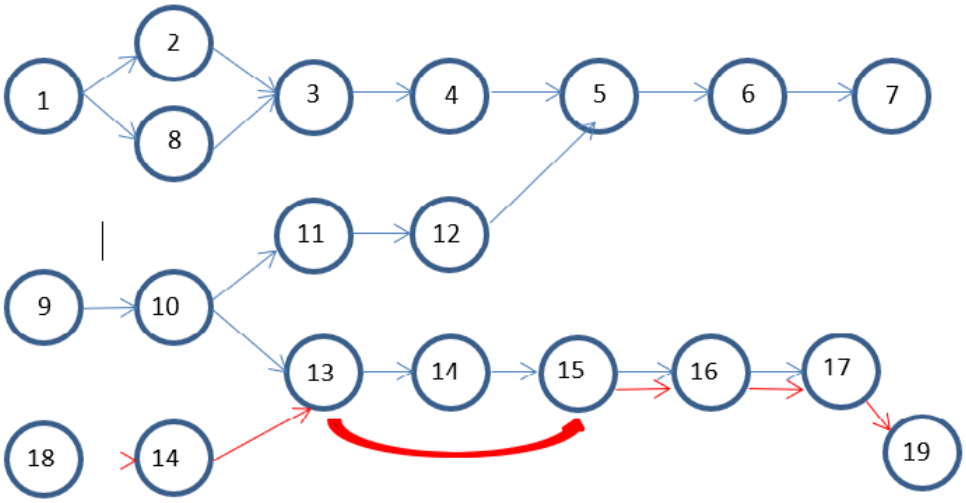


Рис.1. Узагальнена модель структури розвитку катастрофи в наслідок атаки на потенційно-небезпечні об’єкти критичної інфраструктури Авдіївського коксо-хімічного заводу у вигляді орграфу.

Таблиця 1. Характеристики вершин орграфа

№	Опис події
1	Прорив дамби шламонакопичувача
2	Затоплення села Красногорівка
3	Загибель людей і сільських тварин
4	Забруднення значної території відходами із шламонакопичувача
5	Забруднення річок Кам’янка й Очеретувата та р. Кривий Торець
6	Забруднення басейну річки Сіверський Донець
7	Транскордонне забруднення басейну нижнього Дону
8	Затоплення села Веселе
9	Влучення снаряду в хімічний накопичувач
10	Руйнування гідро бар’єру

11	Вторинне забруднення ґрунтових вод
12	Вторинне забруднення шламонакопичувача хім. речовинами з хім. накопичувача
13	Виникнення пожежі на хім. накопичувачі
14	Виникнення пожежі на породному відвалі
15	Забруднення приземного шару повітря
16	Задимлення прилеглої території (залізничного полотна і полігону тв. побут. відходів)
17	Перекидання пожежі на прилеглу територію (залізницю і полігон тв. побут. відходів)
18	Влучення снаряду в породний відвал
19	Перекидання пожежі на територію міста

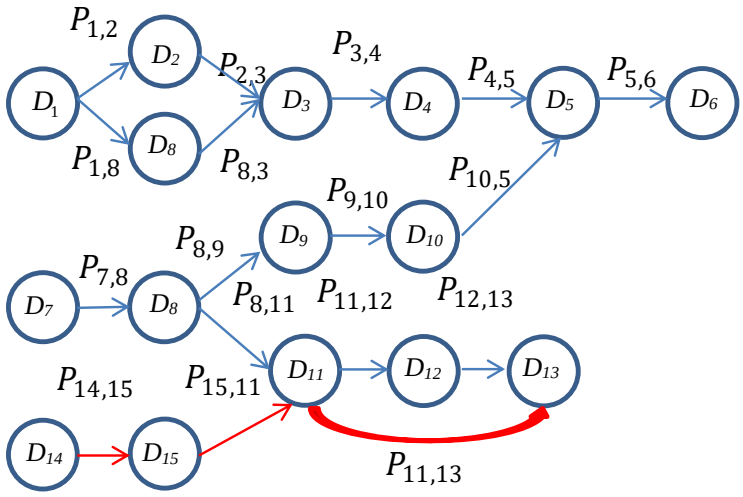


Рис.2 Схема орграфа розвитку катастроф з урахуванням імовірностей виникнення катастроф P і деструктивно-кумулятивних потенціалів D в зоні ведення бойових дій.

На Рис.2 показана модель розвитку катастроф потенційно-небезпечних об’єктів критичної інфраструктури в зоні ведення бойових дій у вигляді орграфа [7] з урахуванням імовірностей виникнення і розвитку катастроф і деструктивно-кумулятивних потенціалів збитків D потенційно-небезпечних об’єктів [5,6].

Також необхідно ввести ступень уразливості об’єкту Z в наслідок події P. Ступень уразливості визначають окремо для кожного потенційно-небезпечного об’єкту за допомогою емпіричних залежностей збитків у соціальній,

екологічний, економічній або біосфері залежно від інтенсивності даних процесів, отриманих за результатами моделювання або статистичної обробки.

Рівняння обчислення ризику набуває наступного виду:

$$R_n = \sum_{i=1}^{k} P_i \times D_{i+1}.$$

Ризики окремих розвитків сценаріїв будуть мати наступні формули:

$$R_1 = P_{1,2} \times D_2 + P_{2,3} \times D_3 + P_{3,4} \times D_4 + P_{4,5} \times D_5 + P_{5,6} \times D_6;$$

$$R_{1,2} = P_{1,8} \times D_8 + P_{2,3} \times D_3 + P_{3,4} \times D_4 + P_{4,5} \times D_5 + P_{5,6} \times D_6;$$

$$R_7 = P_{7,8} \times D_8 + P_{8,9} \times D_9 + P_{9,10} \times D_{10} + P_{10,5} \times D_5 + P_{5,6} \times D_6;$$

$$R_{7,2} = P_{7,8} \times D_8 + P_{8,9} \times D_9 + P_{15,11} \times D_{11} + P_{11,12} \times D_{12} + P_{12,13} \times D_{13};$$

$$R_{14} = P_{14,15} \times D_{15} + P_{15,11} \times D_{11} + P_{11,13} \times D_{13}.$$

Таблиця 2. Значення імовірностей переходу оргграфа на Рис.2

$\mathbf{P_{1,2}}$	$\mathbf{P_{2,3}}$	$\mathbf{P_{3,4}}$	$\mathbf{P_{4,5}}$	$\mathbf{P_{5,6}}$
0,2	0,1	0,3	0,1	0,3
$\mathbf{P_{1,8}}$	$\mathbf{P_{8,3}}$	$\mathbf{P_{3,4}}$	$\mathbf{P_{4,5}}$	$\mathbf{P_{5,6}}$
0,2	0,1	0,3	0,1	0,3
$\mathbf{P_{7,8}}$	$\mathbf{P_{8,9}}$	$\mathbf{P_{9,10}}$	$\mathbf{P_{10,5}}$	$\mathbf{P_{5,6}}$
0,1	0,4	0,1	0,1	0,3
$\mathbf{P_{7,8}}$	$\mathbf{P_{8,11}}$	$\mathbf{P_{11,12}}$	$\mathbf{P_{12,13}}$	
0,1	0,3	0,4	0,2	
$\mathbf{P_{14,15}}$	$\mathbf{P_{15,11}}$	$\mathbf{P_{11,13}}$		
0,3	0,5	0,2		

Відповідно до Методики оцінки збитків від наслідків надзвичайних ситуацій техногенного і природного характеру [8,9] були розраховані значення збитків при катастрофі потенційно-небезпечних об’єктів критичної інфраструктури ОКІ в зоні ведення бойових дій.

Таблиця 3. Значення деструктивно-кумулятивних потенціалів збитків D об’єктів критичної інфраструктури на Рис.2

Потенціал збитків об’єкту	**Значення *млн.грн***
D1	**10**
D2	**50**
D3	**100**
D4	**500**
D5	**100**
D6	**100**
D7	**100**
D8	**500**
D9	**5**
D10	**10**
D11	**100**
D12	**1**
D13	**1**
D14	**1**
D15	**5**
D16	**1**
D17	**6**
D18	**1**
D19	**10**

Рис. 3 Гістограма значень деструктивно-кумулятивних потенціалів збитків D OKI від впливу противника.

Таким чином отримуємо:

$R_1 = 0{,}2 \times 50 + 0{,}1 \times 50 + 0{,}3 \times 500 + 0{,}3 \times 100 + 0{,}3 \times 100 = 225$ млн.грн;

$R_{1,2} = 0{,}2 \times 500 + 0{,}1 \times 100 + 0{,}3 \times 500 + 0{,}3 \times 100 + 0{,}3 \times 100 = 320$ млн.грн;

$R_7 = 0{,}1 \times 500 + 0{,}4 \times 5 + 0{,}1 \times 10 + 0{,}1 \times 100 + 0{,}3 \times 100 = 93$ млн. грн;

$R_{7,2} = 0{,}1 \times 500 + 0{,}4 \times 5 + 0{,}5 \times 100 + 0{,}4 \times 1 + 0{,}2 \times 1 = 102.6$ млн. грн;

$R_{14} = 0{,}3 \times 5 + 0{,}5 \times 100 + 0{,}2 \times 1 = 51.7$ млн. грн.

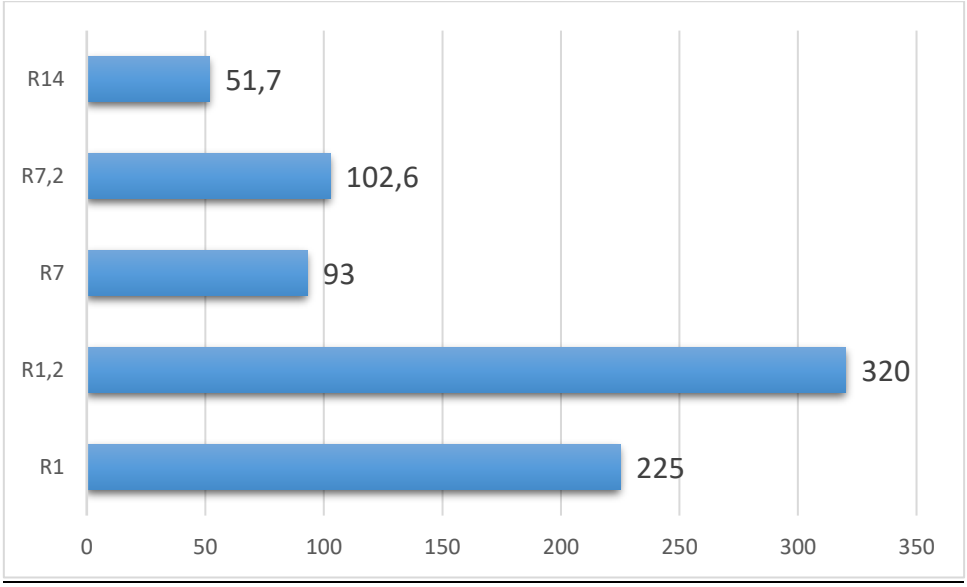


Рис.3 Діаграма значень ризиків за ситуаціями у млн.грн

Висновки

1. Для вирішення проблеми об'єктивності та адекватності отримання результатів розрахунків щодо оцінки ризиків об'єктів критичної інфраструктури з урахуванням потенціалів збитків запропоновано застосування деструктивно-кумулятивних потенціалів збитків, які повністю враховують вторинні деструктивні наслідки, що реалізуються у разі пошкодження чи руйнування ОКІ.
2. За допомогою запропонованої методики обчислені деструктивно-кумулятивні потенціали збитків, визначено найбільш критичні за ризиками (Рис.3) сценарії розвитку катастроф на ОКІ внаслідок впливу противника. Отримані результати дозволять оптимально здійснити розподіл ресурсів, сил і засобів для запобігання виникнення катастроф та визначити ключові ОКІ захист яких мінімізує втрати та деструктивні наслідки катастроф та в цілому дозволить припинити розвиток сценаріїв ланцюгових катастроф системи КІ.

Література

1. С.П. Іванюта Загрози критичній інфраструктурі та їх вплив на стан національної безпеки (моніторинг реалізації Стратегії національної безпеки). Аналітична записка. – К.: НІСД, 2017. 10 с.
2. Бірюков Д. С., Заславський В. А., Євгієнко В. В., Франчук О. В. Моделювання та оцінка сценаріїв загроз для об'єктів критичної інфраструктури // Наукові записки НаУКМА. Том 99. Комп'ютерні науки, 2009. – с. 97-101
3. Г.В. Лисиченко, Ю.Л. Забулонов, Г.А. Хміль Природний, техногенний та екологічний ризики: аналіз, оцінка, управління. Монографія. – К.: Наукова думка, 2008. - 542 с.

4. І.В. Уряднікова, С.М. Чумаченко, С.В. Кармазін, О.М. Тесленко Застосування експертно-аналітичних методів для оцінювання ризиків надзвичайних ситуацій на об’єктах критичної інфраструктури //Науковий вісник Академії муніципального управління. Серія: Техніка. Вип. 1, 2015. С. 206-2018
5. С.М. Чумаченко, Р.К. Мурасов, Я.В. Мельник Теоретико-методологічні основи інформаційного аналізу еколого-техногенних загроз для потенційно-небезпечних об’єктів критичної інфраструктури в умовах збройного конфлікту на Сході України // Сучасні інформаційні технології у сфері безпеки та оборони 118 № 1 (40)/2021, с. 117-122
6. Хвостосховища Донбасу. Звіт по проекту ОБСЄ. 2019. - 50 с. https://www.osce.org/uk/projectcoordinator-in-ukraine/456847
7. Робін Уілсон. Введення в теорію графів. 2019. 240 с.
8. Постанова Кабінету міністрів України від 15 лютого 2002 р. N 175 «Про затвердження Методики оцінки збитків від наслідків надзвичайних ситуацій техногенного і природного характеру», https://zakon.rada.gov.ua/laws/show/175-2002-%D0%BF/print.
9. С.М. Чумаченко, Р.К. Мурасов Математична модель оцінки загроз для об’єктів критичної інфраструктури в зоні ведення бойових дій // Прикладне програмне забезпечення, http://doi.org/10.15407/pp2022.03-04.446.

УДК 331.45

32.ВИМОГИ БЕЗПЕКИ ТА ТЕХНОГЕННІ ЗАГРОЗИ ДЛЯ ПІДПРИЄМСТВ ХАРЧОВОЇ ПРОМИСЛОВОСТІ ЯК ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Сірик А.О.[1], Євтушенко О.В.[1]

1 Національний університет харчових технологій, Київ, Україна

E-mail: 01033sao@gmail.com, 0677389857@ukr.net

Safety requirements and technological threats for food industry enterprises as critical infrastructure facilities

The work considers safety requirements and man-made threats for food industry enterprises as objects of critical infrastructure, taking into account the specifics of production. The issue of operation, identification and declaration of high-risk objects at food enterprises of Ukraine is quite relevant today. The essence of the work and the procedure for responding to man-made and natural emergency situations by subjects of economic activity of food enterprises related to the identification of hazards and the development of a plan for the localization and elimination of emergency situations and accidents were considered.

Експлуатація об’єктів підвищеної небезпеки становить потенційну небезпеку, оскільки при порушенні нормальних умов їх експлуатації або при

зберіганні хімічно-небезпечних речовин які можуть нанести значних збитків населенню, довкіллю, матеріальним цінностям тощо. План локалізації і ліквідації аварійних ситуацій і аварій (ПЛЛА), це документ, в якому: проведено аналіз можливих небезпек на підприємстві; виявлено можливі аварійні ситуації та аварії (в тому числі мало ймовірні), які можуть виникнути на підприємстві; розглянуто сценарій розвитку аварій і оцінені їх наслідки; описані заходи, прийняті на підприємстві для запобігання виникненню аварійних ситуацій; описані заходи, що вживаються працівниками та іншими службами для локалізації і ліквідації аварій та аварійних ситуацій; інша інформація, яка має бути в ПЛЛА, відповідно до чинного законодавства.

Метою плану локалізації і ліквідації аварійних ситуацій і аварій на харчових підприємствах, як об'єктах критичної інфраструктури є планування дій (взаємодії) персоналу підприємства, спецпідрозділів, населення, центральних і місцевих органів виконавчої влади та органів місцевого самоврядування щодо локалізації і ліквідації аварій та пом’якшення їх наслідків Відповідно до частини першої статті 20 Кодексу цивільного захисту України, статті 11 Закону України «Про об’єкти підвищеної небезпеки» [1], з метою встановлення порядку організації розроблення планів локалізації і ліквідації аварій та їх наслідків наказом ДСНС № 253 від 17 травня 2022 року було затверджено «Методичні рекомендації щодо розроблення планів локалізації і ліквідації аварій та їх наслідків».

Порядок віднесення об'єктів до об'єктів критичної інфраструктури, затверджений постановою Кабінету Міністрів України від 16 грудня 2022 р. № 1384 “...об'єкти, що провадять діяльність на ринках послуг, державне регулювання та нагляд за діяльністю яких здійснюють державні органи, віднесення яких до критичної інфраструктури здійснюється в порядку, встановленому такими державними органами”. Відповідно до наказу від 21.12.2022 № 1049 Міністерством аграрної політики та продовольства України утворено робочу групу з ідентифікації та категоризації об’єктів критичної інфраструктури в секторі харчової промисловості та агропромислового комплексу. Закон України “Про критичну інфраструктуру та її захист” із змінами і доповненнями, внесеними Законом України від 18 жовтня 2022 року № 2684-IX встановлює принципи та напрями розбудови державної системи захисту критичної інфраструктури, визначає правові та організаційні засади забезпечення її діяльності і є складовою частиною законодавства України у сфері національної безпеки.

Підприємства харчової промисловості, незалежно від форми власності, на яких виготовляються, переробляються, зберігаються чи транспортуються небезпечні речовини (хімічні, токсичні, вибухові, горючі тощо), повинні провести ідентифікацію та декларацію безпеки об'єктів підвищеної небезпеки (ОПН). У порядку реагування на надзвичайні ситуації техногенного та

природного характеру суб'єкт господарської діяльності, а також підприємства, установи, організації, одночасно з розробленням декларації безпеки розробляють і затверджують План локалізації і ліквідації аварійних ситуацій і аварій для кожного об'єкта підвищеної небезпеки, який вони експлуатують або планують експлуатувати. Робота з розроблення Плану локалізації і ліквідації аварійних ситуацій і аварій має базуватися на ретельно продуманих рішеннях, обґрунтованих розрахунках, специфіці та особливості діяльності промислового об'єкта. На підприємствах харчової промисловості використовується дуже багато різноманітних небезпечних речовин, таких як аміак (аміачні компресорні), бензин, ефіри та інші розчинники жирів (екстракційні відділення олієжирового виробництва та цехи виробництва медпрепаратів та амінокислот м'ясокомбінатів), сірчаний газ (приміщення зберігання клейових та желатинових бульйонів), природний газ (ГРП, котельні, топочні і обпалочні установки) тощо, для яких необхідно проводити вищезазначені роботи. Коротко сутність робіт, пов'язаних з проведенням ідентифікації та розробкою Плану локалізації і ліквідації аварійних ситуацій і аварій, полягає у наступному: при проведенні ідентифікації для кожного потенційно небезпечного об'єкта розраховується сумарна маса кожної небезпечної речовини із зазначених у нормативах порогових мас індивідуальних небезпечних речовин; суб'єкт господарської діяльності (керівник харчового підприємства), у власності або користуванні якого є хоча б один об'єкт підвищеної небезпеки, організовує розробку і складання декларації безпеки об'єкта підвищеної небезпеки, відповідно до встановлених вимог [2].

Декларація безпеки повинна включати: результати всебічного дослідження ступеня небезпеки та оцінки рівня ризику; оцінку готовності до експлуатації об'єкта підвищеної небезпеки відповідно до вимог безпеки промислових об'єктів; перелік прийнятих з метою зниження рівня ризику рішень і здійснених з метою запобігання аваріям заходів; відомості про заходи щодо локалізації і ліквідації можливих наслідків аварій.

Результати аналізу ступеня небезпеки та оцінки рівня ризику включають в себе: умови виникнення та розвитку ймовірних аварій, перелік факторів і основних причин, що сприяють виникненню та розвитку аварій; найменування та сумарна маса небезпечних речовин, що спричиняють аварії; розміри імовірних зон дії вражальних факторів; стислий опис сценаріїв імовірних аварій з урахуванням умови їх виникнення та розвитку; перелік моделей і методів розрахунку, що застосовуються під час дослідження ступеня небезпеки та оцінки рівня ризику; дані про ступінь небезпеки та рівень ризику, а також про ймовірність заподіяння шкоди населенню та довкіллю, очікувані збитки.

При розробленні Плану локалізації і ліквідації аварійних ситуацій і аварій можна виділити дві основні частини: аналітична (оцінка можливих рівнів руйнувань), оперативна (дії персоналу та оповіщення про загрозу аварії на

підприємстві і суміжні підприємства). В основу методики оцінки наслідків аварій вибухонебезпечних об'єктів покладено: моделювання вибухів засновано на закономірностях подібності; для оцінки вибухонебезпеки технологічних блоків харчових підприємств визначають орієнтовні значення енергетичних показників: енергетичний потенціал блоку, приведену масу, відносний енергетичний потенціал і умовні радіуси руйнування та розповсюдження хімічно-небезпечних речовин. В оперативній частині наводяться плани небезпечних блоків, опис дій персоналу, методика навчання, список робітників, що залучаються до локалізації аварії, перелік матеріальних засобів для ліквідації аварії, обов'язки відповідального керівника тощо.

План локалізації і ліквідації аварій та їх наслідків містить всі можливі ситуації, які можуть виникнути на харчовому підприємстві: пуск, робота, зупинка і ремонт. Інформація про План локалізації і ліквідації аварійних ситуацій і аварій надається оператором об'єкта підвищеної небезпеки місцевим органам виконавчої влади, органам місцевого самоврядування, об’єднаним територіальним громадам та територіальним органам ДСНС. При розробленні Плану локалізації і ліквідації аварійних ситуацій і аварій можна виділити дві основні частини: аналітична (оцінка можливих рівнів руйнувань) та оперативна (дії персоналу та оповіщення про загрозу аварії на підприємстві). Оператор об'єкту підвищеної небезпеки створює електронну версію Плану локалізації і ліквідації аварійних ситуацій і аварій (у тому числі з використанням ГІС-технологій), яка може використовуватися для оперативного отримання інформації, оцінки обстановки, що виникає під час аварії та прогнозування розвитку аварії. Положення Плану локалізації і ліквідації аварійних ситуацій і аварій обов’язкові для використання всіма працівниками, що працюють у виробничих, службових, допоміжних спорудах, приміщеннях і будинках, що знаходяться на території об'єкту підвищеної небезпек, у тому числі у порядку взаємодії з персоналом підприємства та залученими силами цивільного захисту, що визначені у Плані локалізації і ліквідації аварійних ситуацій і аварій, під час локалізації і ліквідації аварійних ситуацій (аварій) на технологічному устаткуванні та у виробничих приміщеннях підприємства [3].

Висновки

1. Розглянуто зміни у чинному законодавстві України від 2022 року: до частини першої статті 20 Кодексу цивільного захисту України, статті 11 Закону України «Про об’єкти підвищеної небезпеки», з метою встановлення порядку організації розроблення планів локалізації і ліквідації аварій та їх наслідків наказом ДСНС № 253 від 17 травня 2022 року було затверджено «Методичні рекомендації щодо розроблення планів локалізації і ліквідації аварій та їх наслідків» та порядок ідентифікації та категоризації об’єктів критичної

інфраструктури в секторі харчової промисловості та агропромислового комплексу.

2. Встановлено, що однією з важливих ланок діяльності харчового підприємства, як об’єкта критичної інфраструктури, є аналіз та оцінка ризику виникнення аварій та аварійних ситуацій. Тому постає необхідність перегляду та розробки системи управління безпекою функціювання харчового виробництва, що базується на визначенні ступеню ризику з подальшим оновленням заходів безпеки, що впроваджуються на виробництві з урахуванням вимог Методичних рекомендацій щодо розроблення планів локалізації і ліквідації аварій та їх наслідків.

Література

1. Кодекс цивільного захисту України поточна редакція від 01.01.2023. Режим доступу: https://zakon.rada.gov.ua/laws/show/5403-17#Text
2. Гуць В.С. Сучасні проблеми і вимоги безпеки при експлуатації об'єктів підвищеної небезпеки на підприємствах олієжирової, м'ясної, молочної галузей промисловості / В. С. Гуць, В. М. Фалес, О. В. Хівріч, Н. В. Володченкова // Мясное дело. – 2006. – № 7. – С. 14-15.
3. Методичні рекомендації щодо розроблення планів локалізації і ліквідації аварій та їх наслідків. Наказ Державної служби України з надзвичайних ситуацій від 17 травня 2022 року за №253. Режим доступу: https://zt.dsns.gov.ua/upload/6/7/9/2/4/6/cyGTvjQHgwmI14stiWecKAQiaFvjE3ealMqd5AQ0.PDF

УДК 004.056.53

33.МЕТОДИКА ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ СИСТЕМИ ВИЯВЛЕННЯ ТА РОЗПІЗНАВАННЯ РАДІОСИГНАЛІВ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Собчук В.В.[1], Пічкур В.В.[1], Лаптєва Т.О.[1], Копитко С.Б.[2]

[1] Київський національний університет імені Тараса Шевченка, м. Київ, Україна

[2] Державний університет інтелектуальних технологій і зв'язку, Одеса, Україна

e-mail: v.v.sobchuk@gmail.com, vpichkur@gmail.com, tetiana1986@ukr.net, kopytkosb@gmail.com

Method of increasing the immunity of the system of detection and recognition of radio signals for objects of critical infrastructure

The peculiarities of the use of low-frequency filters in order to improve the immunity of the automated system for the identification and recognition of digital radio broadcasts of critical infrastructure objects have been studied. It is shown that the principle of operation of filters is that the process of summation is performed. At the same time, the useful signal is summed up coherently, and the interference signal - incoherently. It has been proven that the use of low-pass narrow-band filters in the process of signal processing makes it possible to increase the immunity of the information system of critical infrastructure objects, the identification and recognition of digital signals by 17%.

Під завадою радіосигналу в роботі розуміється будь-який вид електричних коливань, який, проникаючи в радіоприймальні пристрої із зовні або виникаючи всередині його, ускладнює визначення радіосигналу. Сигнал і завада, одночасно діють на вході приймача, відтворюються на виході останнього у вигляді випадкового коливального процесу. В результаті цього неможливо точно визначити параметри сигналу. Нормальне визначення сигналу можливо тільки при певному співвідношенні потужності сигналу і завади на виході приймача [1]. Найменша потужність сигналу, при якій забезпечується задовільне визначення сигналу, залежить від рівня завад. Ця величина потужності характеризує чутливість приймача. Здатність радіоприймального пристрою приймати із заданою якістю сигнал при наявності завад називається завадостійкістю [2]. Покращення завадостійкості радіоприймальних пристроїв – одна з основних і найскладніших проблем як радіотехніки, так і проектування інформаційних систем для об'єктів критичної інфраструктури.

Питання подолання завад мають свої особливості і у процесі виявлення та розпізнавання цифрового сингалу радіоефіру. З цією метою розглянемо питання завадостійкості при дослідженні вищезазначених процесів.

Переважна більшість методів завадостійкості приймання сигналів засновані на принципі усереднення сигналу та завади. Даний принцип полягає у тому, що виконується процес підсумовування. При чому, корисний сигнал підсумовується когерентно, а сигнал завади – некогерентно. З метою усереднення корисного сигналу та завади застосовуються лінійні системи двох

типів: вузькосмугові фільтри та фільтри низької частоти. При цьому можливо оптимізувати фільтри низької частоти або вузькосмугові фільтри.

Для розгляду питання фільтрації завад, зробимо припущення, що сам вузькосмуговий фільтр не вносить спотворення в форму сигналу, який пройшов через нього. Ідеальний смуговий фільтр – це фільтр з амплітудно-частотною характеристикою виду:

$$K(\omega)=\begin{cases}1 \quad якщо \quad \omega_0-\dfrac{\Delta\omega}{2}\le|\omega|\le\omega_0+\dfrac{\Delta\omega}{2}\\ 0 \quad якщо \quad]-\infty,\omega_0-\dfrac{\Delta\omega}{2}[U]\omega_0+\dfrac{\Delta\omega}{2},\infty[\end{cases}, \tag{1}$$

де $\Delta\omega$ – полоса пропускання фільтру.

Для ідеального фільтру ефективна полоса $\Delta\omega_e$ та полоса на рівні $0,707-\Delta\omega_{\sqrt{2}}$, що дорівнює полосі прозорості фільтру $\Delta\omega$.

Для фільтрів вірним є припущення, що $\Delta\omega<<\Delta\omega_0$.

Частотна характеристика виразу для (1), це імпульсна перехідна характеристика, яка буде визначатися виразом:

$$h_\delta(t)=\frac{\Delta\omega}{\pi}\cdot\frac{\sin\dfrac{\Delta\omega t}{2}}{\dfrac{\Delta\omega t}{2}}\cos\omega_0 t\ . \tag{2}$$

З огляду на те, що цифрових сигнал не є чітким імпульсом [3], то можна обчислити огинаючу напруги на виході ідеального фільтра при впливі на нього прямокутного імпульсу тривалістю T:

$$x(t)=\begin{cases}X_m\cos\omega_0 t \quad якщо \quad 0\le t\le T\\ 0 \quad якщо \quad]-\infty,0[U]T,\infty[\end{cases}, \tag{3}$$

де X_m – огинаюча сигналу $x(t)$ на вході фільтру.

За допомоги теореми про огинаючу напруги вузькосмугового фільтру, запишемо вираз для огинаючою напруги на виході фільтру:

$$Y_m(t)=\frac{1}{2\pi}\int_{-\infty}^{\infty}K_{fn}(j\omega)S_{X_m}(j\omega)e^{j\omega t}dt,$$

(4)

де $S_{X_m}(j\omega)=\int_{-\infty}^{\infty}X_m e^{-j\omega t}dt$ – амплітудний спектр огинаючої сигналу $x(t)$,

K_{fn} – комплексний коефіцієнт передачі фільтра низької частоти:

$$K_{fn}(j\omega)=\begin{cases}1 \quad якщо \quad -\dfrac{\Delta\omega}{2}\le|\omega|\le\dfrac{\Delta\omega}{2}\\ 0 \quad якщо \quad \left]-\infty,\dfrac{\Delta\omega}{2}\right[U\left]\dfrac{\Delta\omega}{2},\infty\right[\end{cases}$$

(5)

Якщо підставити вираз (5) у вираз (4), то отримаємо вираз:

$$Y_m(t)=\frac{X_m}{2\pi}\left(Si(\Delta\omega t)-Si(\Delta\omega(t-T))\right),$$

(6)

де $Si(z)=\int_0^z\frac{\sin t}{t}dt$ – інтегральний синус [4].

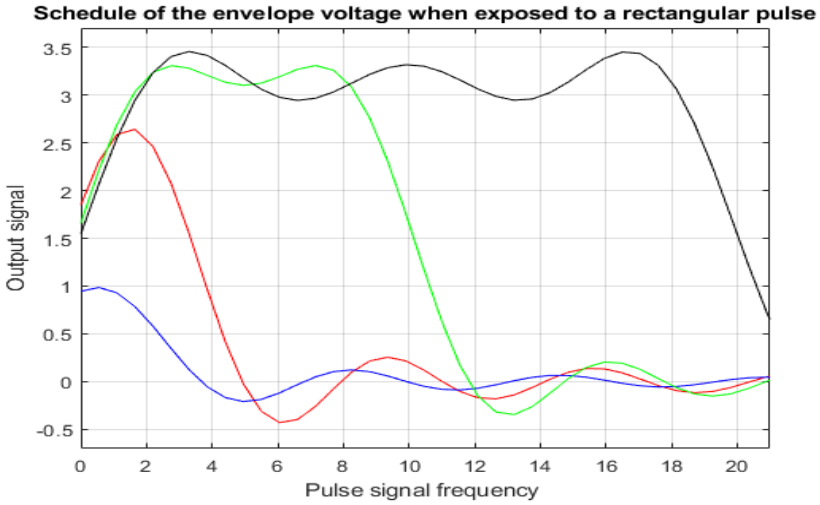


Рис.1. Графік огинаючої напруги при впливі прямокутного імпульсу сигналу

На рис. 1. наведено графіки залежності тривалості прямокутного імпульсу, що впливає на сигнал (блакитний колір – тривалість імпульсу T=1, червоний колір – T=10, зелений колір –T=15 та чорний колір – T=20) від діапазону частоти (полоси пропускання фільтру).

З наведених на рис. 1 графіків бачимо суттєві відмінності вхідного прямокутного імпульсу від вихідного сигналу. Спотворення вхідного імпульсу зростає при збільшення його тривалості. Це спотворення форми імпульсу можливо охарактеризувати співвідношенням тривалості фронту огинаючої імпульсу на виходи фільтра до тривалості огинаючої вихідного імпульсу.

Це свідчить про те, що короткочасні прямокутні сигнали можливо виділяти за допомогою смугового фільтру [5].

Таким чином з метою підвищення завадостійкості системи визначення та розпізнавання , потрібним є використання фільтра низьких частот. За допомогою цього значно понижуються або зовсім виключаються з аналізу завади низьких частот.

Аналіз напрямків розвитку сучасних засобів негласного отримання інформації показують тенденції переходу їх роботи у діапазон високих частот. Тобто сигнал передачі інформації зміщується у діапазон високих частот, у якому процес визначення та розпізнавання цифрових сигналів є доволі складним.

Виключивши з аналізу завади нижніх частот ми вже значно підвищимо завадостійкість інформаційної системи об'єктів критичної інфраструктури в цілому.

Висновки

1. Досліджено особливості використання фільтрів низьких частот з метою підвищення завадостійкості автоматизованої системи визначення та розпізнавання цифрових засобів радіоефіру об'єктів критичної інфраструктури. Показано, що принцип роботи фільтрів полягає у тому що виконується процес підсумовування. При цьому, корисний сигнал підсумовується когерентно, а сигнал завади – некогерентно. Тобто при підсумовуванні корисний сигнал збільшується, а сигнал завади зменшується.

2. Доведено, що використання у процесі обробки сигналів вузько-смугових фільтрів низької частоти дозволяє досягти підвищення завадостійкості інформаційної системи об'єктів критичної інфраструктури, визначення та розпізнавання цифрових сигналів радіоефіру на 17 %.

Література

1. Sobchuk A.V., Sobchuk V.V., Barabash O.V., Liashenko I. Functionally sustainable wireless sensor network technologies aspects analysis Science and Education a New Dimension. Natural and Technical Sciences, VII (23), Issue: 193, 2019 pp 46-48.
2. Лаптєв О.А., Собчук В.В., Савченко В.А. Метод підвищення завадостійкості системи виявлення, розпізнавання і локалізації цифрових сигналів в інформаційних системах. // Колективна монографія Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2019. – Вип. 66. – С. 90 – 104.
3. Laptiev O.A., Barabash O.V., Savchenko V.V., Savchenko V.A., Sobchuk V.V. The method of searching for digital means of illegal reception of information in information systems in the working range of Wi-Fi. International Journal of Advanced Research in Science, Engineering and Technology. India. 2019. Vol. 6, Issue 7. P. 10101 – 10105.
4. Laptiev O., Shuklin G., Savchenko V., Barabash O., Musienko A., Haidur H. The Method of Hidden Transmitters Detection based on the Differential Transformation Model.. International Journal of Advanced Trends in Computer Science and Engineering. 2019. Vol. 8, №6, November- December. P. 538 – 542.
5. Laptiev O.A., Polovinkin I.M, Klyukovskiy D.V., Barabash A.O. Model poshuku zasobiv neglasnogo otrimannya informatsiyi na osnovi diferentsialnyh peretvoren. Sciences of Europe. Praha, Czech Republic. 2019. Vol. 1. No 43. P. 59 – 62.

РОЗДІЛ 4

ПРОГРАМНІ ЗАСОБИ ДЛЯ АНАЛІТИКИ, СИСТЕМИ МОДЕЛЮВАННЯ КІБЕРЗАГРОЗ, ТЕХНОГЕННИХ ТА ЕКОЛОГІЧНИХ ПРОЦЕСІВ І ДІЯЛЬНОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ.

УДК 351.862

34.ОЦІНКА ЗНАНЬ, СТАВЛЕННЯ ТА ПРАКТИКИ ВИКОРИСТАННЯ ПУБЛІЧНИХ БОМБОСХОВИЩ У КИЇВСЬКІЙ ОБЛАСТІ

Гончаренко І.О., Кучма Т.Л., Проданюк Д. М.

Міжнародна неурядова некомерційна організація «ACTED» (www.acted.org), Київ, Україна

E-mail: ihor.honcharenko@reach-initiative.org

Knowledge, attitudes, and practices assessment of public bomb shelter use in Kyivska Oblast

The report outlines the knowledge, attitudes, and practices assessment results of individual interviews and focus group discussions with community members from the Kyiv city agglomeration. The proposed research seeks to generate primary data on the behaviour of residents during air alerts in different places including homes, streets, and workplaces. Additionally, the research aims to investigate the knowledge, attitudes, and barriers related to bomb shelter usage in Kyivska oblast as well as suggestions for their improvement. This assessment was conducted by IMPACT Initiatives with the financial support of the European Union.

Станом на січень 2023 року Управління Верховного комісара ООН з прав людини [1] зафіксувало 18358 жертв серед цивільного населення в Україні з початку повномасштабної війни 24 лютого 2022 року. Для захисту цивільного населення від нападів і військових дій в країні існує мережа публічних бомбосховищ та інших захисних споруд [2]. Однак інформація про сприйняття та бар'єри, пов'язані з використанням бомбосховищ серед населення, обмежена. Отримання прямих даних від населення має важливе значення для подальшого врахування в планах розвитку та відновлення громад, особливо у сфері цивільного захисту.

В національному законодавстві замість терміну «бомбосховище» використовується термін «захисні споруди цивільного захисту», маючи на увазі інженерні будівлі, призначені для укриття і тимчасового захисту людей, обладнання, майна від надзвичайних ситуацій [3]. Ці споруди включають сховища, протирадіаційні укриття, найпростіші укриття та захисні споруди подвійного призначення. Зона доступності для бомбосховищ визначається як радіус 500 метрів або 10 хвилин ходьби [4]. Згідно з національними правилами, за утримання та експлуатацію бомбосховищ відповідають балансоутримувачі об'єктів, до яких належать керівники підприємств, установ та організацій, у тому числі навчальних закладів [5].

З 2018 року Державна служба України з надзвичайних ситуацій більше не відповідає за утримання цих об'єктів [6]. Поточна діяльність служби зосереджена на участі в комісійних перевірках бомбосховищ з подальшим наданням рекомендацій балансоутримувачам захисних споруд. Така ситуація призвела до відсутності єдиної системи управління захисними спорудами, що спричинило проблеми з їх доступністю та пропускною здатністю. Наприклад, у місті Ірпінь є деякі житлові райони в яких відсутні бомбосховища на відстані 500 м, як показано на Рис. 1.

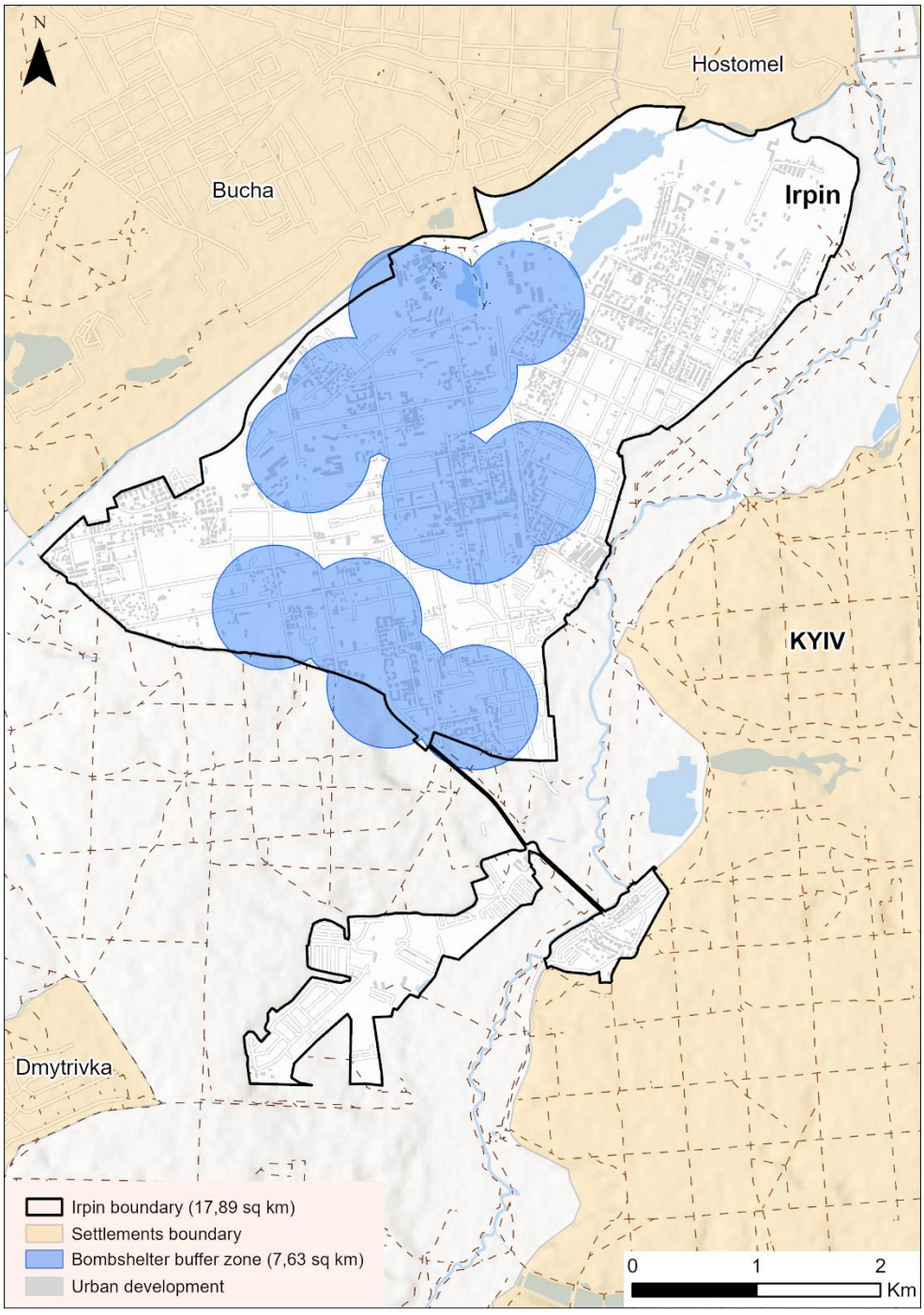


Рисунок - 1. Покриття зон доступності бомбосховища в Ірпені

Методологія

Дослідження включало збір первинних даних (кількісних та якісних) шляхом структурованих опитувань респондентів та напівструктурованих фокус-групових дискусій (ФГД) з членами міських населених пунктів в 20 км від межі міста Києва. Оцінка охоплювала райони, які сильно постраждали від бойових дій (Ірпінь, Буча та Вишгород), а також менш постраждалі райони (Боярка, Бориспіль та Обухів) (див. Рис. 2).

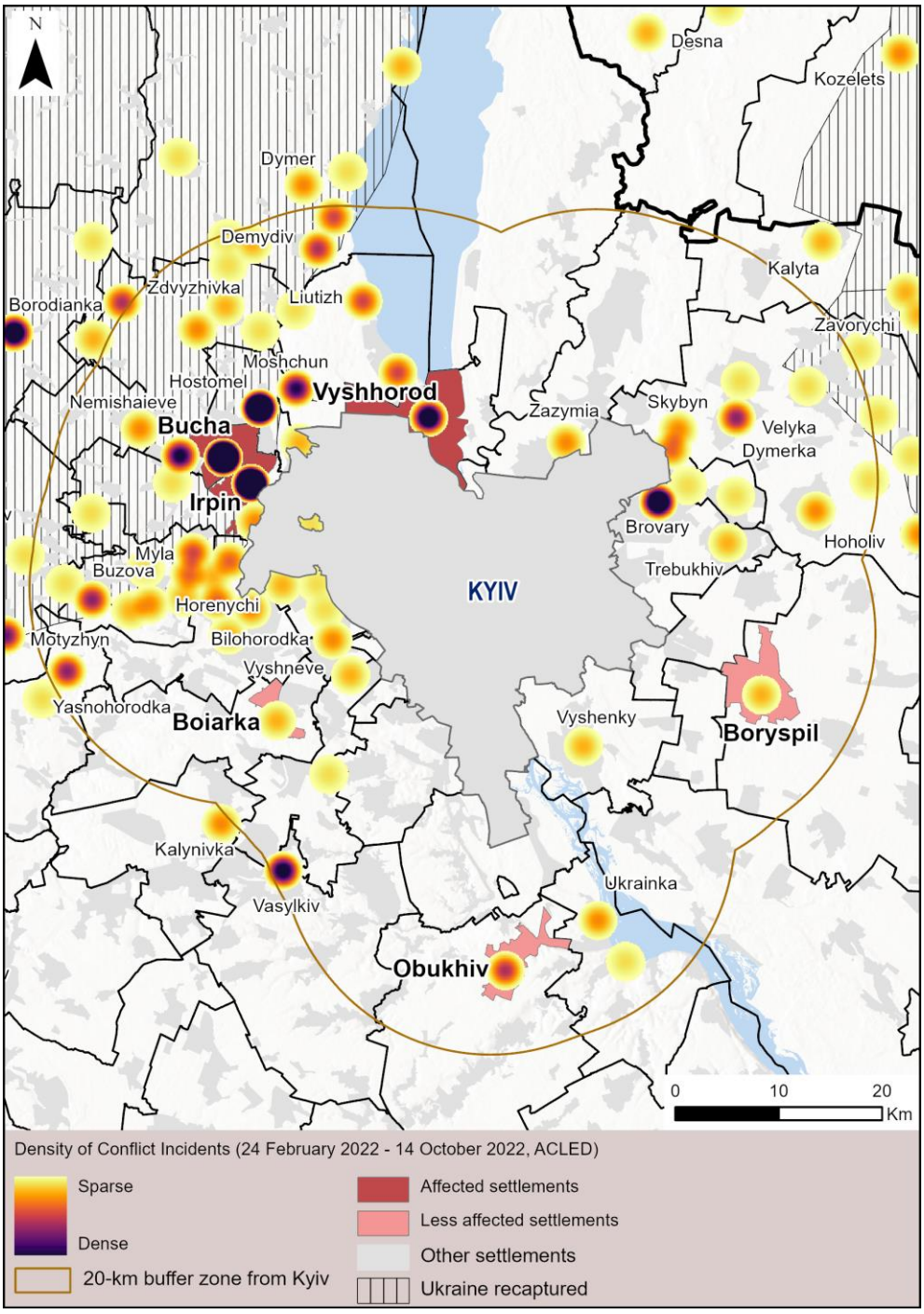


Рисунок - 2. Локації населених пунктів в Київській області

Оцінка зосереджена на міських населених пунктах через більш високу щільність забудови та населення, а також наявність мережі бомбосховищ. Такий підхід дає можливість порівняти відповіді респондентів, які перебували в більшій небезпеці (більше 14 інцидентів), з тими, хто живе в більш безпечних містах (2-3 інциденти). Кількість інцидентів отримана з відкритих джерел The Armed Conflict Location & Event Data Project (ACLED) [7].

Збір даних відбувся в період з 21 листопада по 2 грудня 2022 року і включав 398 особистих інтерв'ю та 6 ФГД, які були рівномірно розподілені в більш- та менш- постраждалих населених пунктах. ФГД проводилися з метою деталізації дослідницьких питань і сприяння поліпшенню використання бомбосховищ. Основним критерієм вибору учасників ФГД був вік, що відповідає віковій класифікації Всесвітньої організації охорони здоров'я (молодий - від 25 до 44, середній - від 45 до 60 і похилий – від 60 років) [8].

Для отримання різноманіття відповідей щодо використання бомбосховищ враховано суб'єктивні характеристики респондентів такі як стать, статус зайнятості та вік, оскільки досвід та сприйняття можуть відрізнятись залежно від цих характеристик. Результати оцінювання показують відсоток респондентів, які дали конкретну відповідь на питання дослідження. Отримані дані не можна екстраполювати на частку населення та слід розглядати як орієнтовні (індикативні), а не репрезентативні.

Результати дослідження

Інформація щодо розподілу учасників кількісного опитування з врахуванням суб’єктивних характеристик представлена в Табл. 1.

Таблиця – 1. Характеристика респондентів

Характеристика	Сильно постраждалі території	Менш постраждалі території	Всього
Жінки	72%	61%	67%
Чоловіки	28%	39%	34%
Вік від 18 до 24 років	7%	8%	7%
Вік від 25 до 44 років	35%	31%	33%
Вік від 45 до 60 років	32%	34%	33%
Вік від 60 років	27%	28%	27%
Працевлаштовані	53%	52%	52%
Безробітні	48%	48%	48%

Уявлення респондентів про місця розташування та відстань до бомбосховищ

Відповідно до отриманих результатів та з огляду на те, що всі інтерв'ю проводились в 10-хвилинній зоні доступності до бомбосховищ, більшість респондентів (59%) повідомили про відсутність або незнання щодо розташування захисної споруди в 10 хвилин від місця перебування. Викладене свідчить про недостатній рівень поінформованості місцевого населення про розташування бомбосховищ.

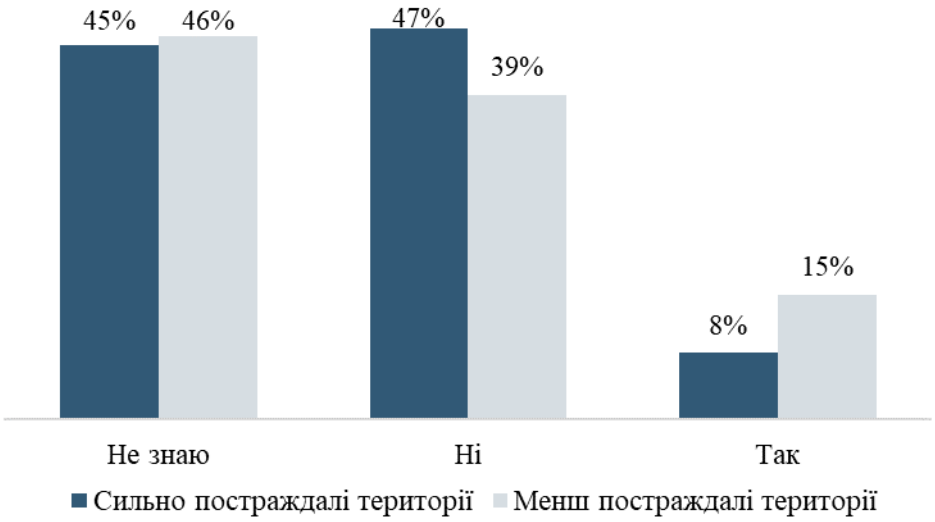


Рисунок - 3. Розподіл відповідей респондентів, що повідомили про наявність бомбосховища в безпосередній близькості (в межах 10 хвилин ходьби)

Результати опитування свідчать про те, що, незважаючи на обмежене використання бомбосховищ, респонденти зазвичай вважають кількість укриттів недостатньою, про що також повідомляли учасники опитування у всіх ФГД.

Рисунок - 4. Розподіл відповідей респондентів, що вважають кількість бомбосховищ у своєму місті достатньою

В середньому 26% респондентів повідомили, що вважають відстань до найближчого бомбосховища одним зі основних бар'єрів доступу, вказуючи на те, що відстань до бомбосховищ може бути одним із ключових факторів, що впливають на рішення не використовувати укриття під час оголошення повітряної тривоги. Учасники ФГД також часто згадували, що найбільш прийнятна відстань до укриття повинна бути в межах 500 метрів та запропонували організувати додаткові бомбосховища в громадських місцях, таких як зупинки громадського транспорту, а також в підвалах або підвалах.

Рисунок - 5. Розподіл відповідей респондентів про бажану відстань до бомбосховища за якої вони будуть готові скористатись захисною спорудою

Учасники всіх ФГД повідомили, що інформацію про місця розташування бомбосховищ вони отримують з онлайн-ресурсів або інших людей. Вони також зазвичай повідомляли, що використовують Інтернет, а також плакати та інформаційні знаки та інші види публічної інформації від місцевих адміністрацій або Державних служб з надзвичайних ситуацій як бажані способи отримання інформації про розташування бомбосховища.

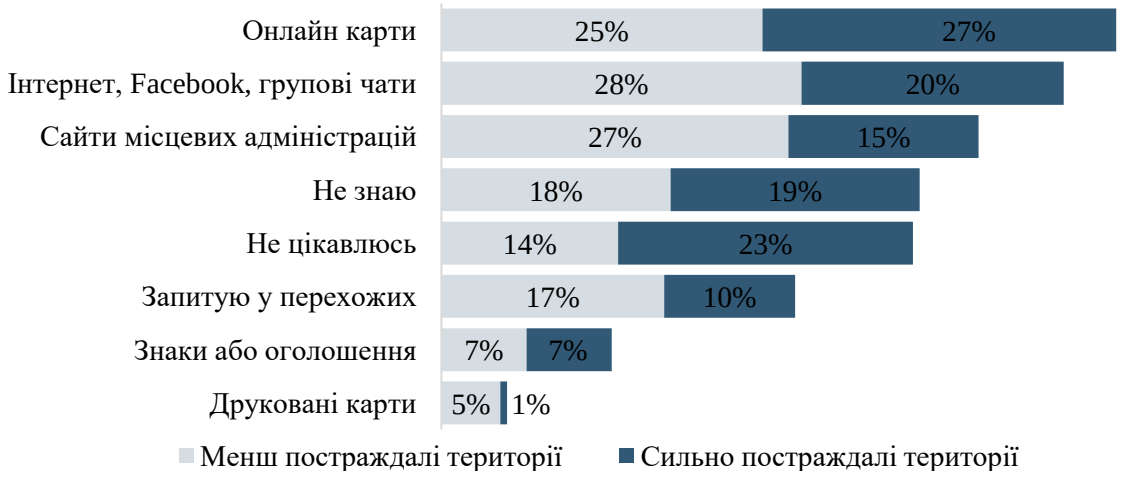


Рисунок - 6. Розподіл відповідей респондентів про джерела інформації, які найчастіше використовуються для з'ясування місцезнаходження бомбосховища (декілька варіантів відповідей)

Повідомлені обставини та перешкоди для використання бомбосховищ

За даними он-лайн ресурсу "Укриття для населення Києва" [9], лише 13% або 485 бомбосховищ Києва обладнані пандусами. Бар'єри для доступу до бомбосховищ можуть сприяти вразливості людей з інвалідністю.

Якісні дані дослідження вказують на два типи бар'єрів серед населення, що стосуються використання бомбосховищ:

- психологічні бар'єри, у тому числі низький рівень довіри до захисних споруд, відчуття небезпеки при використанні захисних споруд або страх незнайомців;

- фізичні або інфраструктурні бар'єри, такі як відсутність достатньої кількості укриттів та відстань до них, а також відсутність додаткових (аварійних) виходів та/або пандусів.

Рисунок - 7. Розподіл відповідей респондентів про обставини за яких вони «ні в якому разі» не були б готові використовувати бомбосховище (декілька варіантів відповідей)

На поведінку учасників ФГД щодо використання бомбосховищ в основному впливає інформація про рівень небезпеки. Через часті повітряні сповіщення, більшість з яких є попереджувальними, люди спочатку перевіряють інформацію щодо фактичного рівня загрози. Учасники зазначили, що є певна адаптація до ситуації загалом.

Рисунок - 8. Розподіл відповідей респондентів про обставини, що впливають на рішення використати бомбосховище (декілька варіантів відповідей)

Учасники також зазначили, що відстань до найближчого укриття та наявність альтернативних варіантів укриття, окрім інших бар'єрів, також впливають на рішення використовувати бомбосховище. У більшості ФГД учасники повідомили, що сприймають підвал/льох загальнодоступним альтернативним типом укриття.

Основним серед повідомлених психологічних бар’єрів є недовіра до здатності бомбосховищ забезпечити належний захист (див. Рис. – 9).

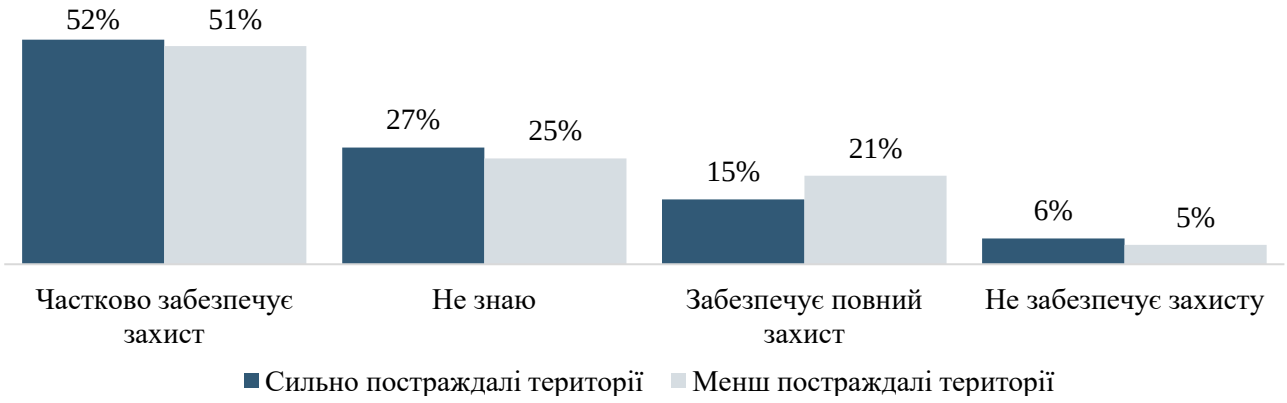


Рисунок - 9. Розподіл відповідей респондентів за сприйняттям здатності бомбосховищ забезпечити належний захист

Підтвердженням вказаного твердження також є інформація респондентів стосовно відчуття захищеності вдома в порівнянні із захисною спорудою, про що вказували 57% респондентів. Інформація щодо розподілу відповідей в залежності від території дослідження представлено на Рис. – 10.

Рисунок - 10. Розподіл відповідей респондентів щодо більшого відчуття захищеності вдома ніж у бомбосховищі

Використання бомбосховища

Серед респондентів, які повідомили, що зазвичай не користуються бомбосховищами - 90%, більшість повідомили про імісця для перечікування повітряної тривоги (див. Рис. – 11).

Рисунок - 11. Розподіл відповідей респондентів про місця перечікування повітряної тривоги

Майже у всіх ФГД були респонденти, які вважають за краще залишатися вдома або ігнорувати сповіщення про повітряну тривогу. Учасники зазвичай повідомляли про використання захисних споруд тільки на робочому місці.

93% респондентів повідомили, що ніколи/майже ніколи не користувалися бомбосховищами, коли повітряна тривога оголошується вночі.

Найпоширеніша поведінка на робочому місці згідно з результатами опитування представлена на Рис. – 12 та Рис. – 13.

Рисунок - 12. Розподіл відповідей респондентів про можливість використовувати бомбосховище під час роботи В цілому 64% респондентів повідомили, що знають про місцезнаходження найближчого бомбосховища до їхнього робочого місця.

Рисунок - 13. Розподіл відповідей респондентів що стосуються перебування в бомбосховищі як поважної причини запізнення/відсутності на роботі

Інформація щодо поведінки під час пересування містом згідно з наданою респондентами інформацією представлена на Рис. – 14 та Рис. – 15.

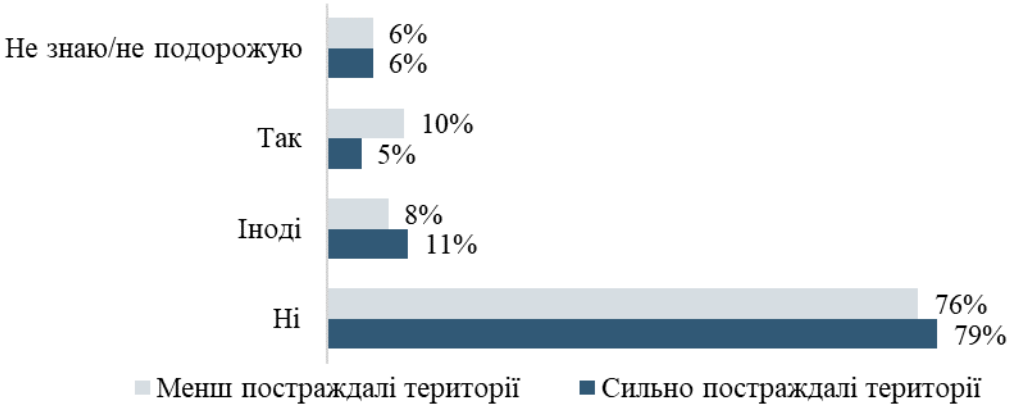


Рисунок - 14. Розподіл відповідей респондентів про врахування місця розташування бомбосховищ при плануванні поїздок по місту

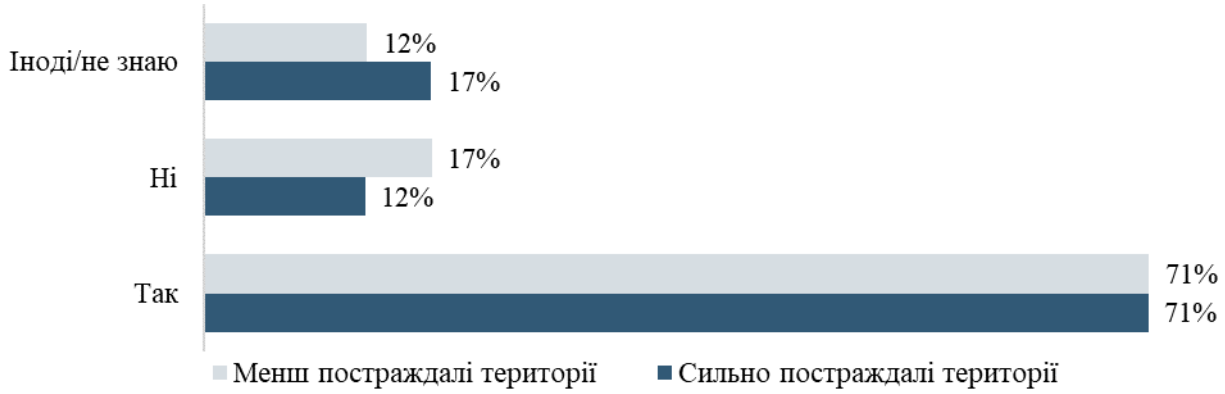


Рисунок - 15. Розподіл відповідей респондентів, що продовжують рух до місця роботи під час оголошення повітряної тривоги (відповіді виключно працевлаштованої категорії респондентів)

Повідомлені пропозиції та рекомендації

Національні правила щодо облаштування бомбосховищ достатньо чітко встановлюють перелік технічних характеристики та майна, яким необхідно укомплектовувати захисні споруди [5].

Одночасно з цим існує низка причин економічного, організаційного та технічного характеру, що заважають забезпечити облаштування укриттів відповідно до встановлених нормативів. З огляду на викладене важливо пріоритезувати потреби користувачів (населення) шляхом з'ясування першочергових заходів з покрашення захисних споруд, що також сприятиме практики їх використання.

Повідомлені пропозиції респондентів щодо покращення бомбосховищ представлені в Табл. – 2.

Таблиця – 2. Повідомлені пропозиції респондентів щодо покращення бомбосховищ (декілька варіантів відповідей)

Типи пропозицій	Сильно постраждалі території	Менш постраждалі території	Всього
Місця для сидіння або лежання	84%	84%	84%
Достатня кількість санітарних вузлів	85%	77%	81%
Наявність опалення та/або обігрівачів	81%	79%	80%
Наявність водопостачання та водовідведення	82%	76%	79%
Загальний санітарний стан (чистота)	65%	71%	68%
Доступ до зв'язку/інтернету	56%	51%	53%
Вода/їжа	42%	16%	29%
Вентиляція	39%	15%	27%
Приміщення для окремого перебування сімей або з дітьми	32%	20%	26%
Нічого з перерахованого вище	2%	0%	1%

Загалом респонденти повідомили, що для забезпечення комфортного використання бомбосховищ вони повинні бути обладнані достатніми місцями для сидіння або лежання, санітарними вузлами, а також забезпечені джерелами тепла та води. Респонденти також зазначили, що бомбосховища повинні бути обладнані запасами води та їжі, але це, швидше за все, пов'язано з очікуваннями щодо тривалого перебування в бомбосховищах. Про це частіше згадували респонденти з сильно постраждалих районів (42% проти 16% у менш

постраждалих районах), оскільки раніше такі респонденти мали тривалий досвід перебування у бомбосховищах під час окупації Київської області.

Потреби людей у вдосконалених бомбосховищах, серед іншого, також можуть впливати на тривалість перебування або невикористання захисної споруди (див. Рис. – 16).

Рисунок - 16. Розподіл відповідей респондентів щодо тривалості перебування в бомбосховищі

Учасники ФГД від 60 років часто наголошували на важливості забезпечення безперешкодного доступу до захисних споруд для людей похилого віку та з обмеженими можливостями, що сприятиме безпеці вразливих категорій населення.

Висновки

Незважаючи на інтенсивні бойові дії, результати дослідження свідчать про низьке використання громадських бомбосховищ серед мешканців міських поселень Київської міської агломерації, а саме:

- 90% респондентів повідомили, що зазвичай не відвідують найближче бомбосховище під час сповіщення про повітряну тривогу;
- 77% респондентів повідомили, що не враховують місця розташування бомбосховищ при плануванні поїздок. Більшість респондентів повідомили, що вважають за краще залишатися вдома під час тривоги.

Результати опитування свідчать про те, що низьке використання бомбосховищ може бути пов'язане як з психологічними, так і з фізичними або інфраструктурними бар'єрами. Респонденти, як правило, повідомили про неможливість існуючих бомбосховищ забезпечити належний захист, зазвичай згадуючи про недовіру та відчуття небезпеки при користування ними. Серед повідомлених фізичних бар'єрів також слід зазначити про відсутність достатньої кількості укриттів, значну відстань до них та брак вільного місця.

Проведений аналіз результатів опитування свідчить про обмежену обізнаність місцевих мешканців про місця розташування бомбосховищ та їх доступність. Хоча опитування проводилось в нормативній зоні доступності до

бомбосховищ, що відповідає 500 м або 10 хвилин ходьби, 59% респондентів повідомили, що не знають про розташування найближчих захисних споруд.

Значна частка респондентів (89%) повідомили про недостатність або відсутню інформацію щодо достатності бомбосховищ в населеному пункті. Респонденти зазвичай пропонували будувати додаткові захисні споруди в місцях скупчення людей, наприклад, зупинки громадського транспорту, або соціальних будівлях (магазини, аптеки, лікарні тощо).

Результати проведеного оцінювання свідчать про те, що може бути вжито кілька заходів для сприяння використанню бомбосховищ шляхом підвищення обізнаності людей та подолання повідомлених бар'єрів. Такі заходи можуть включати організацію інформаційно-просвітницьких кампаній включно із встановленням інформаційних стендів чи вказівників напрямку руху, а також експертної перевірки стану укриттів з подальшою чіткою комунікацією через офіційні інформаційні канали про дотримання стандартів укомплектованості захисних споруд, у тому числі спроможності забезпечити належну безпеку.

При будівництві або реконструкції бомбосховищ важливо враховувати пріоритетні потреби користувачів основними з яких відповідно до результатів опитування були - місця для сидіння/лежання, наявність каналізації, опалення, достатньої кількості санітарних вузлів та приміщень для окремого перебування сімей з дітьми, доступ до засобів зв'язку а також запасів води та харчування.

Література

6. Ukraine: Civilian casualties as of 15 January 2023. the Office of the UN High Commissioner for Human Rights (OHCHR). Link - https://ukraine.un.org/en/215396-ukraine-civilian-casualties-15-january-2023.

7. Захисні споруди цивільного захисту. Офіційна інтернет сторінка Міністерства освіти і науки України. Джерело - https://mon.gov.ua/storage/app/media/civilniy-zahist/2022/15.06/Zakh.sporudy.tsyvilnoho.zakhystu.15.06.2022.pdf

8. Кодекс цивільного захисту України. Джерело - https://zakon.rada.gov.ua/laws/show/5403-17#Text.

9. ДБН В.2.2-5-97 Захисні споруди цивільної оборони. Будинки і споруди. Джерело - https://www.minregion.gov.ua/wp-content/uploads/2017/05/DBN-V.2.2-5-97.pdf.

10. Вимоги щодо утримання та експлуатації захисних споруд цивільного захисту, затверджені наказом Міністерства внутрішніх справ України 09 липня 2018 року № 579. Джерело - https://zakon.rada.gov.ua/laws/show/z0879-18#n770.

11. Постанова Кабінету Міністрів України «Деякі питання використання захисних споруд цивільного захисту» від 10 березня 2017 р. № 138. Джерело - https://zakon.rada.gov.ua/laws/show/138-2017-%D0%BF#Text.

12. The Armed Conflict Location & Event Data Project (ACLED). Джерело - https://acleddata.com/ukraine-conflict-monitor.

13. Dyussenbayev, A. (2017). Age Periods Of Human Life. Advances in Social Sciences Research Journal, 4(6). Джерело - https://doi.org/10.14738/assrj.46.2924.

14. Он-лайн ресурс «Укриття для населення Києва». Джерело - https://wdc-ukraine.maps.arcgis.com/apps/webappviewer/index.html?id=e4d3b96d62f740c388c27a77cf69e8c2&extent=3355972.8714%2C6506143.496%2C3437301.8695%2C6542298.2103%2C102100.

УДК 658

35.МОДЕЛЮВАННЯ ПОКАЗНИКІВ ІНВЕСТИЦІЙНИХ СИСТЕМ

Зарецький І.С.[1]

1 Харківський національний економічний університет імені Семена Кузнеця
E-mail: zaretskyj.ivan.s@hneu.net

Modeling indicators of investment systems

In the work, the system of investment development of Ukraine is built and the value of export and import is predicted, as the indicators that most depend in the system on the change in the indicator of direct foreign investment. At the current stage of direct foreign investment in the Ukrainian economy, there is a decrease in the intensity of attraction of direct foreign investment, which is caused by a number of factors of an economic and political nature. Representatives of the private sector of foreign countries are mainly interested in highly profitable areas, in particular the financial sector and industry, which currently account for about half of foreign investments accumulated in the country's economy.

Найбільш бажаною формою інвестування для країн, що розвиваються, є залучення прямих іноземних інвестицій (ПІІ). Така форма довгострокових інвестицій сприяє інтенсифікації виробництва, розвитку національної економіки, впровадженню інноваційних технологій, зростанню експортного потенціалу. Реалізація політики інвестиційної привабливості України стимулює залучення прямих іноземних інвестицій в економіку України. Гіпотезою дослідження існування взаємозалежності між обсягом прямих іноземних інвестицій та макроекономічними факторами: обсягом експорту та імпорту, ВВП, курсом долара США, індексом споживчих цін, фактором часу. Виявлення та їх моделювання є основним предметом дослідження.

Основою кореляційно-регресійного аналізу є оцінка парних коефіцієнтів кореляції між залежною та незалежною змінними, які покажуть щільність зв'язку між досліджуваними економічними показниками. Розрахунок коефіцієнтів кореляції дозволить визначити ступінь впливу основних макроекономічних факторів на обсяг капітальних інвестицій [1].

Прямі іноземні інвестиції тісно пов'язані із зовнішньоекономічною діяльністю країни, розвиток експортно-імпортних операцій характеризує їх зв'язок із зовнішнім ринком і міжнародним поділом праці. Валовий внутрішній продукт є результатом економічного циклу виробничої діяльності, обсяг ПІІ залежить від курсу долара на ринку, а рівень інфляції є показником економічної стабільності.

Від залучення в країну іноземних інвестицій залежить стан національного виробництва, рівень технологічного розвитку, структурна перебудова

національної економіки. Іноземні інвестиції мають позитивні наслідки входження в країну, і супроводжуються загрозами економічному розвитку держави.

Особливу роль в активізації інвестиційної діяльності в Україні має відіграти залучення прямих іноземних інвестицій на взаємовигідних умовах, насамперед з метою реалізації спільних проектів для вирішення завдань структурної трансформації економіки, впровадження новітніх технологій у виробництво та збільшення обсягів виробництва, конкурентоспроможність українських товарів [2]. Сьогодні залучення інвестицій здійснюється різними способами і залежить від економічного середовища інвестування. Найпоширенішими способами залучення інвестицій в Україну є придбання іноземним інвестором місцевої організації; створення іноземної філії, а також змішаного або спільного підприємства; залучення коштів міжнародних фінансових організацій та проведення конкурсів, які передбачали б зобов'язання щодо розвитку підприємств та додаткову емісію акцій [3]. Найбільш яскраво зміну інвестиційного клімату демонструє динаміка інвестицій, особливо прямих іноземних, що вважається індикатором зміни рівня довіри та рейтингу країни.

Таким чином, із галузевих пріоритетів інвестування економіки України випливає, що основні представники приватного сектору іноземних держав дотримуються єдиної для України інвестиційної стратегії, при цьому основний інтерес становлять фінансовий сектор та промисловий сектор.

Для моделювання інноваційного розвитку України було обрано показники, що проаналізовано в першому розділі. Вихідні дані наведено в таблиці 1.

Таблиця 1 Вихідні дані для проведення факторного аналізу

Роки	ПІІ, млн. дол. США	Експорт, млн. дол. США	Імпорт, млн. дол. США	ВВП, млн. грн	Курс долара США за одиницю (грн/USD)	Індекс споживчих цін, %
	X1	X2	X3	X4	X5	X6
2010	45370,0	63341,5	72678,5	1079346	7,96	109,1
2011	48197,6	82574,5	96788,5	1299991	7,98	104,6
2012	51705,3	82926,6	98813,8	1404669	7,99	99,8
2013	53704,0	77553,9	91220,0	1465198	7,99	100,5
2014	38356,8	65422,5	65949,5	1586915	15,77	124,9
2015	32122,5	47863,7	47253,0	1988544	24,00	143,3
2016	31230,3	46229,7	49117,8	2385367	27,19	112,4
2017	31606,4	53979,0	60321,5	2981227	28,07	113,7
2018	32905,1	58972,9	63496,4	3560302	27,69	109,8
2019	35809,6	65683,5	67742,4	3977198	23,69	104,1
2020	54210	63465	65176	4194102	25,8	105
2021	52091	80026	82233	5459574	27,8	110

Результати факторний аналіз наведено на рисунках 1-4.

Data: DATA (6v by 12c)

	1 X1	2 X2	3 X3	4 X4	5 X5	6 X6
1	45370	63341,5	72678,5	1079346	7,96	109,1
2	48197,6	82574,5	96788,5	1299991	7,98	104,6
3	51705,3	82926,6	98813,8	1404669	7,99	99,8
4	53704	77553,9	91220	1465198	7,99	100,5
5	38356,8	65422,5	65949,5	1586915	15,77	124,9
6	32122,5	47863,7	47253	1988544	24	143,3
7	31230,3	46229,7	49117,8	2385367	27,19	112,4
8	31606,4	53979	60321,5	2981227	28,07	113,7
9	32905,1	58972,9	63496,4	3560302	27,69	109,8
10	35809,6	65683,5	67742,4	3977198	23,69	104,1
11	54210	63465	65176	4194102	25,8	105
12	52091	80026	82233	5459574	27,8	110

Рис. 1. Вихідні дані для аналізу.

Factor Loadings (Varimax normalized) (DATA)
Extraction: Principal components
(Marked loadings are >,700000)

Variable	Factor 1	Factor 2
X1	0,882767	0,100756
X2	0,935164	0,187019
X3	0,914944	0,336871
X4	0,101985	-0,981760
X5	-0,495213	-0,858528
X6	-0,810658	0,100025
Expl.Var	3,403734	1,869538
Prp.Totl	0,567289	0,311590

Рис. 2. Факторні навантаження

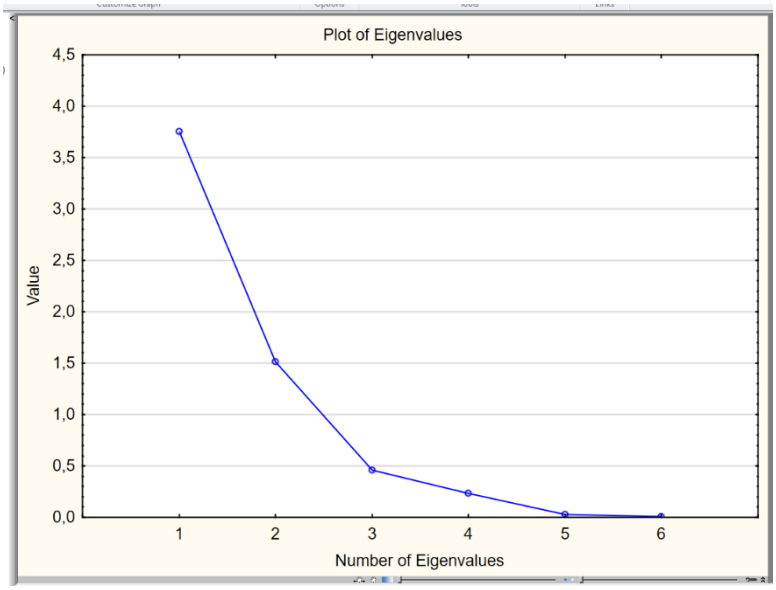


Рис. 3. Кам'яна осип

Eigenvalues (DATA)
Extraction: Principal components

Value	Eigenvalue	% Total variance	Cumulative Eigenvalue	Cumulative %
1	3,756589	62,60981	3,756589	62,60981
2	1,516683	25,27805	5,273272	87,88787

Рис. 4. Власні числа

Таким чином, виявлено взаємозалежність між показниками першого фактору X1, X2, X6 та в другому факторі між X4 та X5.

Для вивчення інноваційного розвитку проаналізуємо залежності першого фактору таким чином, де показник прямих іноземних інвестицій є незалежним, та впливає на таки: експорт, імпорт, індекс споживчих цін. Результати цих моделей наведено на рис. 5 – 7.

Regression Summary for Dependent Variable: X2 (DATA)
R=,813780 R2=,662238 Adjusted R2=,628462
F(1,10)=19,607 p<,00128 Std.Error of estimate:7835,6

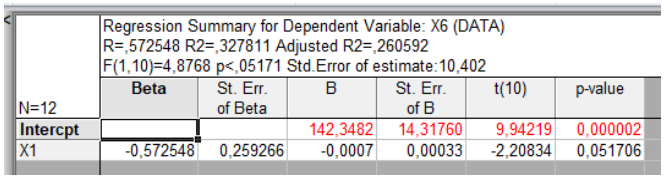
N=12	Beta	St. Err. of Beta	B	St. Err. of B	t(10)	p-value
Intercpt			18977,94	10784,72	1,759707	0,108955
X1	0,813780	0,183783	1,10	0,25	4,427942	0,001278

Рис. 5. Побудова залежності експорту X2 від інвестицій X1

Regression Summary for Dependent Variable: X3 (DATA)
R=,781317 R2=,610456 Adjusted R2=,571502
F(1,10)=15,671 p<,00269 Std.Error of estimate:11257,

N=12	Beta	St. Err. of Beta	B	St. Err. of B	t(10)	p-value
Intercpt			11760,23	15494,23	0,759007	0,465363
X1	0,781317	0,197369	1,42	0,36	3,958670	0,002692

Рис. 6. Побудова залежності імпорту X3 від інвестицій X1



Regression Summary for Dependent Variable: X6 (DATA)
R=,572548 R2=,327811 Adjusted R2=,260592
F(1,10)=4,8768 p<,05171 Std.Error of estimate:10,402

N=12	Beta	St. Err. of Beta	B	St. Err. of B	t(10)	p-value
Intercpt			142,3482	14,31760	9,94219	0,000002
X1	-0,572548	0,259266	-0,0007	0,00033	-2,20834	0,051706

Рис. 7. Побудова залежності індексу споживчих цін X6 від інвестицій X1

За результатами проведеного факторного аналізу, та побудованих моделей залежності побудуємо систему кореляційно-регресійних моделей інноваційного розвитку України(таблиця 2).

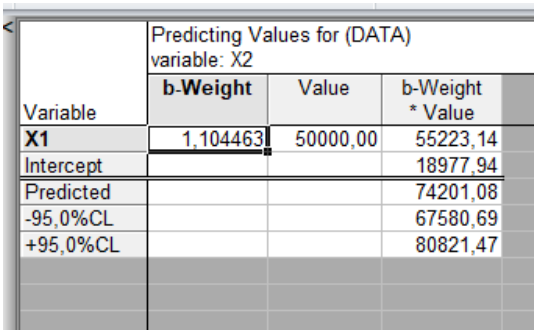
Таблиця 2 Система кореляційно-регресійних моделей інноваційного розвитку України

Економічна сутність показників	Математична модель
Залежність експорту України від ПІІ	X2 = 18977,94+1,10*X1
Залежність імпорту України від ПІІ	X3 = 11760,23+1,42*X1

Таблиця 2.3 Аналіз побудованих моделей

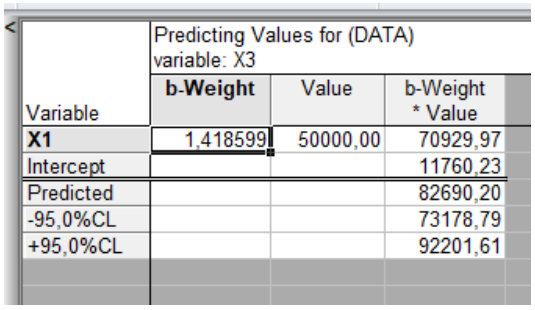
Математична модель	Коефіцієнт кореляції	Коефіцієнт детермінації	p-level
X2 = 18977,94+1,10*X1	0.81	0.66	0.0012
X3 = 11760,23+1,42*X1	0.78	0.61	0.0026

Оцінки побудованих моделей дозволяють використати рівняння для прогнозування, що є останнім етапом алгоритму дослідження. Для прогнозування показників експорту та імпорту приймаємо значенні показника ПІІ на рівні 50 000 млн. дол. США., це показник нижчий за рівень останніх двох років, але вищий за середній рівень за 2010 – 2021 роки. Результати прогнозування наведено на рис. 8 та 9.



Variable	Predicting Values for (DATA) variable: X2 b-Weight	Value	b-Weight * Value
X1	1,104463	50000,00	55223,14
Intercept			18977,94
Predicted			74201,08
-95,0%CL			67580,69
+95,0%CL			80821,47

Рис. 8. Прогнозування експорту X2 від інвестицій X1



Variable	Predicting Values for (DATA) variable: X3 b-Weight	Value	b-Weight * Value
X1	1,418599	50000,00	70929,97
Intercept			11760,23
Predicted			82690,20
-95,0%CL			73178,79
+95,0%CL			92201,61

Рис. 9. Прогнозування імпорту X3 від інвестицій X1

Таблиця 4 Результати прогнозування системи моделей інвестиційного розвитку

Математична модель	Нижня границя прогнозного значення	Верхня границя прогнозного значення
X2 = 18977,94+1,10*X1	67585.69	80821,47
X3 = 11760,23+1,42*X1	73178,79	92201,61

Прогнозні значення за кожною з моделей:

X2 = 18977,94+1,10*50 000 = 74201,08 (млн. дол. США)

X3 = 11760,23+1,42*50 000 = 82690,20 (млн. дол. США)

Висновки

Пріоритетним напрямом інвестування є інновації. Інвестування в розвиток інтелектуального, промислового, управлінського, маркетингового, цифрового, інноваційного потенціалів створюють умови для формування та розвитку стратегічних конкурентних переваг підприємства.

Пара рівнянь лінійної регресії свідчить про наступний вплив досліджуваних факторів на показники економічного зростання. Із зростанням ПІІ у промисловість сектора на 1%, темп зростання експорту країни може зрости на 0,47%. При темпах зростання ПІІ у промисловий сектор та сектор фінансового посередництва на 1% темпи зростання імпорту можуть зрости на 0,51% та 0,43% відповідно. Прискорення темпів зростання ПІІ у секторах фінансового посередництва, торгівлі на 1% може призвести до зниження рівня безробіття в країні на 0,3%, 0,51%.

Література

15. Лукінов І. І. Економічні трансформації (наприкінці XX сторіччя) / НАН України; Інститут економіки. – К., 1997.

16. Михайленко О. Г., Красникова Н. А. Вплив іноземних інвестицій на розвиток економіки України в умовах глобалізації. Ефективна економіка. 2020. № 7. – URL: http://www.economy.nayka.com.ua/?op=1&z=8046 (дата звернення: 28.02.2023). DOI: 10.32702/2307-2105-2020.7.54.
17. Васєчко О. О. Питання оцінювання опосередкованого впливу прямих іноземних інвестицій на економіку України [Електронний ресурс] / О. О. Васєчко, О. М. Мотузка // Статистика України. - 2016. - № 4.

УДК 623:355

36.ОБҐРУНТУВАННЯ КОМПОНЕНТІВ ДЛЯ СТВОРЕННЯ ПРОГРАМНО-АПАРАТНОГО КОМПЛЕКСУ З ВИЯВЛЕННЯ РАДІАЦІЇ ТА БОЙОВИХ ОТРУЙНИХ РЕЧОВИН

Карпенко М.І., Чумаченко С.М., Мошенський А.О.

Національний університет харчових технологій, Київ, Україна

E-mail: sapta@ukr.net

Substantiating of the components for creating a software and hardware complex for detection of radiation and chemical warfare agents

The report is devoted to the theoretical substantiating of the relevance of developing a hardware and software complex for the detection of radiation and CWA, including elements necessary for its operation (radiation and gas sensors). An analysis of the state of informatization of environmental monitoring was carried out; specified and characterized threats; analyzed specialized means for detecting radiation and CWA; problems for the creation of a new complex were identified; the best components are selected.

Під час російського вторгнення в Україну з боку агресора було зроблено низку заяв, які широко сприймаються як погрози використання ядерної зброї. Численні обстріли атомної та теплової електростанцій Енергодару можна класифікувати як акти ядерного тероризму, внаслідок чого тривалий час світ був на межі екологічної катастрофи.

Окрім актів ядерного тероризму, російські загарбники нехтують Конвенцією про хімічну зброю, обстрілювавши «Азовсталь» невідомим хімічним типом боєприпасів, а також фосфорними бомбами, які заборонені для використання. Зокрема фосфорні бомби неодноразово застосовувались у боях за Київ та Краматорськ у березні, а також проти оборонців «Азовсталі» у Маріуполі у травні і це лише випадки, яким надали розголос.

Згідно Федерації американських вчених (FAS) російської армії на момент 18 листопада залишилося 4 477 ядерних боєголовок, з яких 1 912 тактичні. Згідно даних Організації із заборони хімічної зброї (OPCW) 27 вересня 2017 р. було завершено верифікацію знищення російської програми хімічної зброї. Проте,

попередні дані про ураження захисників «Азовсталі» боєприпасом з невідомим хімічним складом змушує піддати сумніву факт утилізації хімічної зброї.

Взявши до уваги сам факт схильності російських військових до терористичних актів, постає необхідність у способах та засобах раннього виявлення загроз, а також оповіщення цивільного населення й військовослужбовців ЗСУ.

Як вказувалось вище, загрози постають у вигляді радіації та небезпечних газів. В англійській мові отруйні речовини (ОР) прийнято називати Chemical agents (скорочено CA). Бойові отруйні речовини (БОР) відповідно Chemical warfare agents (CWA). До класичних CWA відносяться хімічні речовини нервово-паралітичної дії: (Табун (GA), Зарин (GB), Зоман (GD), Етилзарин (GE), Циклозарин (GF), O-ethyl- S-diisopropyl amino methyl methylphosphonothiolate (VX), S-(Diethyl amino)ethyl O-ethyl ethylphosphonothioate (VE), Амітон або Tetram (VG), Фосфітна кислота та methyl-, S-(2-(diethyl amino)ethyl) O-ethyl ester (VM); шкірнонаривної дії: Іприт (H, HD), Азотний іприт (HN-1, HN-2, HN-3), Люїзит (L),Іприто-Люзиїт (HL), Фенілдихлороарсин (PD), Фосгеноксим (CX); крововсмоктуючі (blood agents): Синильна кислота (AC), Хлороціан (CK), Арсин (SA); задушливої дії: Хлор (Cl), Фосген (CG), Дифосген (DP), Хлорпікрін (PS).

В умовах російсько-української війни найбільш небезпечними та вірогідними для застосування слід вважати наступні класи ОР: нервово-паралітичної та шкірнонаривної дії.

Для виявлення таких речовин необхідні спеціальні датчики. Пересічному громадянину майже неможливо такі дістати.

Типи БОР можна виявити за допомогою детекторів, принцип роботи яких заснованих на наступних технологіях:

Ion Mobility Spectroscopy (IMS). Flame Photometry (FDP (Flame Photometric Detection Technology)). Infra-Red (IR) Spectroscopy (Photoacoustic IR spectroscopy, Filter IR spectroscopy, Passive infrared detection, Differential absorption light detection and ranging). Raman Spectroscopy. Surface Acoustic Wave (SAW). Colorimetric. Photo Ionisation Detection (PID). Flame Ionisation Detection (FID). [1]

Кожна з таких технологій має свої переваги та недоліки. Варто зазначити, що до уваги бралися всі технології, окрім Colorimetric detection. Кольорометричний спосіб виявлення використовується військовими за найпростіший, найдешевший та найлегший тип детекторів для використання в польових умовах. Являє собою спеціальні пробірки, талони або папірці, оброблені реагентами, які реагують на БОР. На відміну від усіх інших способів, даний неможливо (або вкрай складно) автоматизувати, оскільки щоб обробити результат потрібне візуальне сприйняття його людиною.

Висновки щодо технологій виявлення БОР: Найбільш нежиттєздатною для польових умов є технологія FID. Найкращою ж є технологія SAW. SAW та PID мають високу чутливість навіть до малих концентрацій ОР, а розмір детектора можна зменшити до мінімального розміру та ваги до 1 кг. Вони обидва мають недоліки у вигляді впливу водяної пари та вологості на показники, однак, детектори SAW значно дешевші у виготовленні.

Photo Ionisation Detection (PID) – вкрай чутливий спосіб виявлення ОР, дозволяє виявляти сполуки в дуже низьких концентраціях (ppb до ppm). PID детектори зазвичай використовується у випадках екстреного реагування для надання попередньої інформації про різні хімічні речовини, оскільки вони можуть реагувати на випари конкретних неорганічних сполук, в той час як інші детектори не здатні на це. Принцип роботи PID полягає в іонізації зразка речовини за допомогою УФ випромінювання поглинутим атомом або молекулою.

Переваги PID: висока чутливість; коли межі виявлення досягають низьких значень ppm, вони автоматично конвертуються в ppb; можуть виявляти не лише БОР.

Недоліки PID: значно схильний до впливу водяної пари; слабко розрізняють гази. Дорогі у виготовленні та складні.

Surface Acoustic Wave (SAW) – поверхнева акустична хвиля - технологія, побудована на вимірюванні змін у властивостях акустичних хвиль, коли вони проходять на ультразвукових частотах у п’єзоелектричних матеріалах.

Відомі пристрої: детектори від Thermo Electron Corporation (TVA 1000B Toxic Vapour Analyser), HazMat, RAE Systems (MiniRAE 2000, MiniRAE 3000, ppbRAE, ppbRAE 3000, ppbRAE Plus, MultiRAE Plus, ToxiRAE Plus PID)

Переваги SAW

Відносно низька ціна виготовлення, швидке реагування на речовини, вкрай мала кількість помилкових тривог, виявляють навіть низькі рівні нервово-паралітичних та шкірно-наривних речовин. Детектори SAW можна використовувати для ефективного виявлення ОР в різноманітних умовах навколишнього середовища.

Недоліки SAW

На продуктивність можуть впливати коливання температури та вологості; чутливі до пошкодження деякими високоактивними парами. Полімерні покриття можуть фізично змінюватися, коли пристрій піддається впливу умов, що виходять за межі діапазону робочих температур, і після того, як покриття фізично змінюється, здатність датчика ефективно виявляти потрібні ОР стає під загрозою.

Відомі пристрої: HAZMATCAD, ChemSentry 150C, CW Sentry Plus, SAW MINICAD mk II та the Joint Chemical Agent Detector (JCAD). [4]

Проблеми полягають у закупівлі або створенні обладнання, заснованого на даних технологіях, а також їх освоєнню.

Для індикації та вимірювання радіоактивного випромінювання застосовують прилади радіаційної розвідки. Вітчизняними блоками детектування є серія БДБГ: БДБГ -Т/-09С/ -15С та БДПН-07; приладів для спецтехніки: ДРГ-Т, СВНГ-Т, КДУ-6БМ, МКС-УМ VRS та ГеоРад. Кожен з них має високий ступінь захисту та масу від 500г до 20 кг.

На відміну від професійних готових приладів, існують трубки Гейгера, які доступні для придбання та показують хороші результати, наприклад: SBM-20/-

19/-10, SI-180G, M4011, SI-29BG/-8b, VAZ-115.1, SBT-9/-11A, LDN 712 / 5979 / 7317, CI-8b.

SI-180G найкраще показує себе для виміру фонової радіації; LND 7317 найбільш чутливий до Cs137, Radium, Thorite, Am 241: 223000,45700,39200,90500 CPM (count per minute) відповідно. Окрім того, вони мають досить невелику масу (наприклад LDN7317 важить 125 г). [2]

Необхідністю побудови ІС програмно-апаратного комплексу є ряд причин. Першою є рівень охоплення виявлення речовин, де БПЛА можуть в десятки разів перевищити показники стаціонарного (станції) чи мобільного (наземний, водний транспорт), ручного обстеження. Другою є безпека: оператор дрона знаходитиметься на безпечній відстані від зони зараження в той час, як іншим необхідно мати при собі спеціальне захисне спорядження та ризикувати власним життям. Третьою є те, що у ручних детекторах кількість виявленої радіації послаблюється за рахунок захисних кожухів для безпеки оператора, зменшуючи виміряну інтенсивність на 20–35% [3]. Для оператора дрону немає потреб у такому зменшенні. Важливими факторами для побудови ІС є вага, точність, надійність пристроїв та їх вартість. Вага є одним з ключових факторів, оскільки усі дрони мають власні обмеження по вазі.

Література:

1. Sferopoulos R. (2009) A Review of Chemical Warfare Agent (CWA) Detector Technologies and Commercial-Off-The-Shelf Items publisher Human Protection and Performance Division DSTO Defence Science and Technology Organisation 506 Lorimer St Fishermans Bend, Victoria 3207 Australia.
2. https://sites.google.com/site/diygeigercounter/technical/gm-tubes-supported
3. D. Connor, P. G. Martin & T. B. Scott (2016) Airborne radiation mapping: overview and application of current and future aerial systems, International Journal of Remote Sensing, 37:24, 5953-5987, DOI: https://doi.org/10.1080/01431161.2016.1252474
4. Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response. Institute of Medicine (US) Committee on R&D Needs for Improving Civilian Medical Response to Chemical and Biological Terrorism Incidents. Washington (DC): National Academies Press (US); 1999.

УДК 004.056.53

37.МОДЕЛЬ ВІДНОВЛЕННЯ ТЕРИТОРІЙ З КРИТИЧНОЮ ІНФРАСТРУКТУРОЮ, ЩО ПОСТРАЖДАЛА ВІД ВІЙСЬКОВИХ ДІЙ

Хоперський С.В.[2], Чумаченко С.М.[1], Пономаренко С.О.[2], Попель В.А[3], Масленнікова Т.А.[3]

1 ГО «Інститут дослідження кіберпростору», м. Київ
2 ГО «Асоціація спеціалістів цивільного захисту», м. Київ
3 Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, м. Київ
E-mail: s_chum@ukr.net, tmaslennykova@gmail.com, ssvh@ukr.net, v.popel@cip.gov.ua

A model for the restoration of territories with critical infrastructure damaged by military actions

The paper examines the problems of restoring territories with critical infrastructure that have suffered as a result of military actions and emergency situations. To solve these problems, a number of legal, methodological, technical, organizational and other issues are being considered, which require the coordination of different countries. Such coordination should be based on a systematic analysis of emergency situations. For this, an expert system for assessing natural and man-made threats and risks, as well as an information system for substantiation and selection of possible ways of rehabilitation of the affected areas, is proposed.

Проблеми реабілітації територій з критичною інфраструктурою, що постраждали внаслідок військових дій та надзвичайних ситуацій, є актуальними для багатьох країн світу. Вирішення цих проблем ускладнюється, коли такі території є транскордонними та їх реабілітація може бути реалізована лише завдяки міжнародним зусиллям. У цьому випадку виникає низка юридичних, методологічних, технічних, організаційних та інших питань, що потребують узгодження зусиль різних країн. Таке узгодження має ґрунтуватися на системному аналізі надзвичайних ситуацій. Для цього пропонується технологія оцінки природно-техногенних загроз та ризиків, а також шляхів реабілітації постраждалих територій [1], яка буде застосована для кількох країн одночасно.

Ключовими елементами запропонованої технології є:

- систематизовані бази даних існуючих нормативно-правових документів щодо оцінки загроз виникнення надзвичайних ситуацій природно-техногенного характеру країн-учасниць;
- систематизовані бази даних методик розрахунку шкоди, спричиненої техногенними аваріями, катастрофами та природними стихійними лихами,

бойовими діями, терактами, соціально-політичними зіткненнями, що використовуються країнами-учасницями;

- нова розроблена (пілотна) методика розрахунку збитків, що враховує переваги існуючих методик різних країн-учасниць;

- інформаційний Веб-Гео-портал для обміну інформацією між країнами-учасницями про рівні загрози виникнення надзвичайних ситуацій природно-техногенного та воєнно-техногенного характеру;

- система оперативного моніторингу територій та показників якості людського життя на основі мобільних вимірювальних лабораторій із сучасним аналітичним обладнанням;

- науково-обґрунтовані механізми та технології з відновлення та реабілітації постраждалих територій.

В результаті буде запропоновано науково-обґрунтовані рекомендації щодо відновлення та реабілітації цих територій. Реалізація запропонованої технології включатиме такі дії:

- визначення пріоритетних територій для здійснення збору додаткової інформації на територіях країн-учасниць та відображення їх кордонів у розділі електронного Веб-Гео-порталу;

- збір інформації про рівень соціо-еколого-економічних збитків, що виникли внаслідок надзвичайних ситуацій природно-техногенного характеру та внаслідок бойових дій;

- польові дослідження територій, що постраждали від надзвичайних ситуацій та військових дій, їх обробка та аналіз;

- оцінка рівня соціо-еколого-економічного збитку, що виник внаслідок надзвичайних ситуацій природно-техногенного характеру та внаслідок бойових дій на територіях країн-учасниць;

- розробка пропозицій щодо впровадження інноваційних технологій відновлення та реабілітації постраждалих територій для країн-учасниць;

- прогнозування можливого розвитку соціо-еколого-економічної ситуації на територіях країн-учасниць, які постраждали внаслідок надзвичайних ситуацій техногенного характеру та внаслідок бойових дій.

- розробка стратегій захисту критичної інфраструктури територій, що постраждали.

Додатковою перевагою запропонованої технології є реалізація принципу суспільно-державного партнерства у сфері відновлення якості життя на реабілітованих територіях. Цьому сприяє підхід до побудови інформаційного Веб-Гео-порталу системи. У порталі відсутній початковий власник і ним зможуть користуватися як органи державної влади, так і органи місцевого самоврядування, населення, громадські організації та рухи. Такий підхід до побудови Веб-Гео-порталу сприятиме залученню ініціативи громадян для використання, розвитку та розширення можливостей системи на основі суспільно-державного партнерства.

Веб-Гео-портал створюється шляхом об'єднання кількох передових інформаційних технологій, таких як:

- технологія захищеного зберігання паспортизованих даних, документів, електронних каталогів. При цьому сховища в системі розподіляються відповідно до володіння інформацією - фізично дані знаходяться на майданчику власника, а портал отримує доступ до даних відповідно до параметрів запиту та наданих повноважень;

- геоінформаційні технології, що поєднують дані зі сховищ із даними географічної локації. Ця система формує уявлення, засновані на географічному просторі.

Запропонована комплексна технологія може стати базовою не лише для реабілітації територій з критичною інфраструктурою після завершення військових дій, але і для розбудови нового соціо-еколого-економічного середовища розвитку суспільства.

Подальші дослідження стосуються того, що потрібно робити в умовах військового конфлікту чи НС середньої чи низької інтенсивності [2]:

1. Створення розподіленої безпроводової мережі екологічного моніторингу на базі стійких автономних елементів, що добре виживають (може спеціальних терміналів, до існуючої техніки, можна додати відео і сенсорні реєстратори, може системи коптерів - реєстраторів).

2. Системна інтеграція та банк даних з критичної інфраструктури та інфраструктури взагалі (найповніший банк низового шару елементів-складових - до останнього стовпа, світлофора, водороздавальної колонки) одночасно сумісний з геоінформаційними системами.

3 Визначення можливості створення резерву та резервної мережі базових елементів (автономне джерело електропостачання, води, сурогат релейної мережі розумний стовп, релейна та моніторингова станція на базі аеростатного або БПЛА підвісу (баржуючий режим до заміни постійним елементом).

4. Створення повністю автономних ланок життєзабезпечення з можливістю інтеграції в паралельну інфраструктурну мережу (щось на зразок пунктів незламності, але з можливістю інтеграції за територіальним або функціональним принципом).

5. Паралельна модель оцінки вартості переходу з тимчасових елементів на автономні, а потім стаціонарні системи життєзабезпечення.

Література

1. Y. Bodryk, S. Chumachenko, A. Nevolnichenko, V. Shevchenko The Procedure of military sites rehabilitation with optimal planning of tender orders // F. Brechignac, G. Desmet Equidosimetry, Amsterdam: Springer, 2005. – p. 281-284.

2. Лисенко О.І, Чумаченко С.М., Чеканова І.В., Турейчук А.М. Математическая постановка задачи оптимального управления экологическим состоянием техногенно нагружаемых территорий. / Адаптивні системи автоматичного управління. Міжвідомчий науково-технічний збірник. – Дніпропетровськ: Системні технології, 2002. - Вип. 5(25) - С. 45-55.

РОЗДІЛ 5

ІНФОРМАЦІЙНІ СИСТЕМИ ДЛЯ ОЦІНЮВАННЯ КІБЕРЗАГРОЗ, ТЕХНОГЕННИХ ТА ЕКОЛОГІЧНИХ ЗАГРОЗ І РИЗИКІВ ДЛЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ.

UDC 351.861

38.INFORMATION TECHNOLOGIES FOR PREVENTING EMERGENCY SITUATIONS AT CHEMICAL INDUSTRY FACILITIES

Vovchuk T., Shevchenko R., Shevchenko O.

National University of Civil Defense of Ukraine, Kharkiv, Ukraine
E-mail:shevchenko605@i.ua

The paper considers the solution to the task of developing information technology for analytical support of the process of preventing man-made emergencies at chemical industry facilities under conditions of excessive man-made load, taking into account the modern capabilities of QR-coding technologies.

The analysis of the current state of the issue convincingly proves that, taking into account Ukraine's orientation towards European standards in the field of civil protection, there is a need for generalization and implementation of international experience in the creation and operation of management systems in emergency situations, based on modern information and communication technologies, primarily emergency situations of man-made nature at the facilities of the chemical industry in conditions of excessive man-made load.

The conditions for the integration of existing domestic approaches to the prevention of man-made emergencies at chemical industry facilities under conditions of excessive man-made load into the information and analytical space of the European Community countries were determined, which made it possible to form the foundations of a methodical apparatus for the development of information technology for the prevention of man-made emergencies at ects of the chemical industry in the conditions of excessive man-made load, taking into account the modern capabilities of QR - coding, and to determine a group of boundary conditions, which are formed as appropriate limitations of the derivative consequences of an emergency situation.

The information technology of analytical support for the management of an emergency situation of a man-made nature at the facilities of the chemical industry in conditions of excessive man-made load has been developed, which allows to introduce innovative emergency management approaches into the daily activities of the practical units of the State Emergency Service of different hierarchical levels of subordination.

The further development of this study consists in the development of a number of practical recommendations, which primarily relate to the harmonization of domestic approaches and practices to the requirements of the countries of the European Community. However, such harmonization may face difficulties in the formation of general principles of comprehensive assistance to the population in the event of emergency situations that threaten health, life, property or the surrounding natural environment, or other dangerous and catastrophic events.

УДК 004.056.9

39.ІНФОРМАЦІЙНІ СИСТЕМИ ДЛЯ ОЦІНЮВАННЯ КІБЕРЗАГРОЗ

Гуйда О. Г., Кисельов В. Б., Омецинська Н.В.
Таврійський національний університет імені В.І. Вернадського
E-mail ometsynska.nataliia@tnu.edu.ua, kyselov.volodymyr@tnu.edu.ua, guydasg@ukr.net

INFORMATION SYSTEMS FOR EVALUATING CYBERSECURITY THREATS

In the digital age, cybersecurity threats pose a serious risk to organizations' operations, data, and reputation. To mitigate these risks, cybersecurity risk assessment techniques have been developed, with the help of information systems. This article provides an overview of the latest research on information systems for cybersecurity risk assessment, published over the past five years. The article discusses various techniques, including intelligent models, deep learning, and cyber threat intelligence frameworks, and their applications in critical infrastructure protection and cloud computing. The article also highlights the challenges and future research directions in this field. Overall, this article emphasizes the importance of information systems in enhancing cybersecurity risk assessment and promoting effective risk management.

В сучасному світі інформаційна безпека стає все важливішою темою, оскільки кіберзагрози можуть спричинити значну шкоду компаніям, організаціям та приватним особам. Інформаційні системи для оцінювання кіберзагроз можуть допомогти виявити та запобігти кібератакам. У цій статті розглянуто різні інформаційні системи, які використовуються для оцінювання кіберзагроз.

Перш за все, необхідно визначити, що таке кіберзагрози. Згідно з Національним інститутом стандартів та технологій США (National Institute of Standards and Technology, NIST), кіберзагроза - це будь-яка подія, яка може завдати шкоди інформаційній системі або даним [1]. Кіберзагрози можуть бути викликані різними чинниками, такими як хакерські атаки, віруси, фішинг, розкрадання даних тощо.

Існує кілька інформаційних систем, які допомагають виявляти кіберзагрози та відстежувати їх наслідки. Одна з таких систем - це система моніторингу захисту мережі (Network Protection Monitoring, NPM), яка використовується для виявлення кіберзагроз в режимі реального часу [2]. Система NPM забезпечує постійний моніторинг мережі та виявляє незвичайну активність або спроби вторгнення. Якщо система виявляє загрозу, вона негайно сповіщає про це адміністратора мережі, який може прийняти відповідні заходи для запобігання атаки.

Інша інформаційна система, яка використовується для оцінювання кіберзагроз - це система ризик-аналізу (Risk Analysis System, RAS), яка допомагає визначити потенційні загрози та оцінити їх рівень ризику [3]. Система RAS аналізує різноманітні джерела інформації про кіберзагрози, включаючи інформацію про нові вразливості та атаки, та надає відповідні рекомендації щодо захисту мережі.

Інша інформаційна система - це система детекції загроз (Threat Detection System, TDS), яка використовується для виявлення вразливостей та аномальної активності в мережі [4]. Система TDS використовує різноманітні методи детекції, включаючи машинне навчання та статистичний аналіз, для виявлення потенційних загроз. Якщо система виявляє загрозу, вона негайно сповіщає про це адміністратора мережі, який може прийняти відповідні заходи для запобігання атаки.

Одним з найбільш важливих елементів інформаційних систем для оцінювання кіберзагроз є бази даних про кіберзагрози та вразливості. Існує кілька баз даних, які містять інформацію про кіберзагрози та вразливості, включаючи бази даних Відкритої кібербезпеки (Open Cybersecurity Alliance, OCA) та Відкритих вразливостей та експлойтів (Open Vulnerability and Assessment Language, Oval) [5]. Ці бази даних дозволяють адміністраторам мережі бути в курсі останніх кіберзагроз та вразливостей та приймати відповідні заходи для запобігання атак.

Однією з головних переваг інформаційних систем для оцінювання кіберзагроз є можливість автоматизації процесу виявлення та реагув ання на кібератаки. Автоматизація дозволяє швидко виявляти потенційні загрози та реагувати на них негайно, що може значно зменшити шкоду від атаки. Крім того, інформаційні системи дозволяють збирати, обробляти та аналізувати великі обсяги даних, що не може бути зроблено вручну.

Недоліком інформаційних систем для оцінювання кіберзагроз є їх висока вартість та складність впровадження. Крім того, інформаційні системи не можуть гарантувати повну безпеку мережі, оскільки кіберзлочинці постійно шукають нові методи та техніки для зламу мережі.

У підсумку, інформаційні системи для оцінювання кіберзагроз є важливим елементом кібербезпеки. Вони дозволяють адміністраторам мережі виявляти потенційні загрози та приймати відповідні заходи для запобігання атак. Інформаційні системи для оцінювання кіберзагроз можуть бути використані у різних сферах, включаючи фінансову, медичну та державну сфери. Незважаючи на деякі недоліки, інформаційні системи для оцінювання кіберзагроз є необхідним інструментом для забезпечення кібербезпеки в сучасному світі.

Література

1. Choi, H., Lee, J., Kim, J., Kim, H., & Kim, S. (2018). Cyber risk assessment system based on attack scenarios. Journal of Communications and Networks, 20(2), 197-204. [https://doi.org/10.1109/JCN.2018.000025]

2. Zhou, Q., Huang, Z., Liu, Y., & Chen, L. (2021). Cybersecurity risk assessment model based on attack graph and Bayesian network. Computer Networks, 197, 108061. [https://doi.org/10.1016/j.comnet.2021.108061]

Duan, Y., Wu, J., X ., & Wang, Y. (2020). An intelligent intrusion detection and response system based on machine learning and software defined networking. Journal of Network and Computer Applications, 161, 102636. [https://doi.org/10.1016/j.jnca.2020.102636]

4. Shabtai, A., Fledel, Y., & Elovici, Y. (2018). Cyber defense competitions and information security education: An overview. Journal of Cybersecurity, 4(1), tyx007. [https://doi.org/10.1093/cybsec/tyx007]

5. Rass, S., Karygiannis, T., & Antonakakis, M. (2017). Enhancing cyber threat information sharing. Computer, 50(8), 44-51. [https://doi.org/10.1109/MC.2017.3011216]

УДК 681.5.01: 629.52.7

40.ОЦІНКА РАДІАЦІЙНОГО РИЗИКУ ЗАБРУДНЕННЯ МІСЦЕВОСТІ ДЛЯ НАСЕЛЕННЯ ВНАСЛІДОК ВІЙСЬКОВИХ ДІЙ

Триснюк Т.В., Конецька О.О., Нагорний Є.І., Марущак В.М., Волинець Т.В., Приступа В.В.

Інститут телекомунікацій та глобального інформаційного простору НАН України
taras24t@ukr.net

Assessment of the radiation risk of contamination of the area for the population as a result of military operations

Radioactive contamination of the area is a powerful factor influencing the life of the population, the work of administrative structures and state administration bodies as a whole. Detection of radioactive contamination of the area will be the primary task of eliminating the consequences of radioactive contamination. The proposed method of determining the radiation risk of contamination of the area in the zone of influence of military operations based on radiation reconnaissance data will allow to assess and in some cases improve the quality of the forecast of the study area.

Питання постійного контролю радіаційної обстановки (РО) і своєчасного виявлення радіоактивного забруднення місцевості (РЗМ) продовжують залишатися актуальними і в наш час. У випадку військових дій з боку Росії неможливо виключити можливість атаки терористів на об’єкти атомної енергетики, підприємства атомної енергетики, а також могильники радіоактивних відходів. Таким чином, можливе виникнення ситуації, коли значні території будуть радіоактивно забрудненні від декількох джерел. Радіоактивне забруднення місцевості є потужним фактором впливу на життєдіяльність

населення, роботу адміністративних структур і органів державного управління в цілому. Виявлення радіоактивного забруднення місцевості буде являтися першочерговою задачею ліквідації наслідків радіоактивного забруднення [1]. Розвідувально-контролюючі органи призначені для ведення розвідки і контролю за станом і зміною обстановки в зонах можливого чи реального прояву уражаючих впливів за допомогою військових формувань:

- інженерної розвідки для виявлення меж і ступеня руйнування житлових будинків і виробничих споруд, визначення вторинних наслідків уражаючих впливів, знаходження місць перебування потерпілих і підходів до них;
- хімічної розвідки для виявлення меж хімічного зараження, визначення концентрації отруйних речовин і напрямку поширення зараженого повітря, спостереження і лабораторного контролю за зміною хімічної обстановки;
- радіаційної розвідки для виявлення меж і рівнів радіоактивного забруднення, встановлення режимів радіаційного захисту, спостереження і дозиметричного контролю за зміною радіаційної обстановки;
- медичної розвідки для виявлення постраждалих людей, визначення їхнього стану й умов надання першої медичної і лікарської допомоги;
- ветеринарної та агротехнічної розвідки для виявлення постраждалих тварин і рослин, визначення їхнього стану й умов надання ветеринарної й агротехнічної допомоги.

У процесі горіння об’єктів критичної інфраструктури, лісової рослинності, забрудненої радіонуклідами, у навколишнє середовище у вигляді диму викидаються радіоактивні продукти згоряння, які, перемішуючись в атмосфері разом з повітряними масами, завдають серйозної шкоди здоров'ю населення [2].

Стохастичний характер процесів виникнення, розвитку і поширення лісових пожеж та варіювання ступеня горіння рослинності на лісових масивах з малою щільністю радіоактивного забруднення залежно від пожежного навантаження, сезону року й інших пожежотехнічних і метеорологічних факторів, утруднюють оцінку радіаційної обстановки та прогноз після радіаційних наслідків [3].

У процесі математичного моделювання виникнення і розвитку низової, перехідної і верхової лісової пожежі аналізували наступні процеси:

- перенос летучих часток радіаційно-пилового забруднення, який був спрямований атмосферним плином;
- розвиток струменя при викиді нагрітих газів в атмосфері, що характеризувався поняттям швидкості вітру, температури і тиску, а також постійним перемішуванням нагрітих газів з навколишнім повітрям;
- розсіювання мілкодисперсних часток радіаційно-пожежного забруднення, що відбувається за рахунок атмосферної турбулентної дифузії та їхньої седиментації в полі тяжіння, а також взаємодією з підстилаючою поверхнею.

Остаточна картина радіоактивного забруднення місцевості формувалася за час, який залежав від відстані до точки пожежі і метеорологічних параметрів (з урахуванням рози вітрів) [4].

У результаті проходження радіоактивної хмари диму через населені пункти жителі будуть піддані впливу наступних радіаційно небезпечних факторів:

- зовнішнього впливу гамма-випромінювання від шлейфа диму;
- зовнішнього гамма-випромінювання нуклідів, що осіли зі шлейфа диму на поверхню навколишнього середовища;
- внутрішнього опромінення, обумовленого вдиханням радіоактивних часток радіаційно-пилового забруднення, що виходять із димової хмари;
- внутрішнього опромінення за рахунок вдихання радіоактивних часток золи;
- внутрішнього опромінення, обумовленого надходженням радіонуклідів в організм людини з харчовими продуктами.

Колективний радіаційний ризик у зоні впливу радіоактивного диму від місця пожежі розраховувався за формулою:

$$R_c(L) = \int_0^2 \int_0^{\pi} \int_0^{l} \rho(L,V) R(L) H\left[F(L)Q\right] f(Q) L dL dQ, \qquad (1)$$

де $\rho(L,V)$ – густина населення, що проживає в зоні впливу радіаційно-пожежного забруднення.

Тут
$$R_c(L) = K(L) \int H\left[F(LQ)\right] f(Q) L dL dQ, \qquad (2)$$

де $K(L)$ – фактор, що враховує рівну імовірність напрямку вітру при пожежі;

$H[F(L)Q]$ – умовна густина імовірності пожежі, що приводить до дози зовнішнього і внутрішнього опромінення при активності викиду;

$f(Q)dQ$ – частота пожеж, що активізує викид в інтервалі $(Q \div Q+dQ)$.

Дозу зовнішнього опромінення, обумовлену впливом i-го радіонукліда, що перебуває в продуктах згоряння, розраховували за формулою:

$$H\left[F(L)_{ef}\right] = \sum \xi \sigma / V_h \theta_i \int_0^{\tau} Q_i(\tau) / h_{ef}(\tau) d\tau, \qquad (3)$$

де ξ – частка i-го радіонукліда в продуктах згоряння, значимого для зовнішнього опромінення;

Θ_i – ширина сектора забруднення i-м радіонуклідом;

V_h – середня швидкість вітру на висоті шару перемішування;

$Q_i(\tau)$ – сумарна активність i-го радіонукліда в хмарі диму;

h_{ef} – ефективна висота підйому димової хмари. Тут

$$\theta_i = \theta_w + \theta_f; \qquad (4)$$

$$\theta_w = 1{,}1\tau^{0{,}67} L^{-0{,}125}; \qquad (5)$$

$$Q_f = 1{,}1\tau^{0{,}5} L^{-0{,}16}; \qquad (6)$$

$$h_{ef} t = K_h q(\tau)^{0{,}25} / V_0; \qquad (7)$$

де τ – час викиду радіаційно-пилового забруднення в атмосферу;

K_h – коефіцієнт, що дорівнює 530;

$q(\tau)$ – потужність теплового потоку над місцем пожежі;

V_0 – швидкість вітру в районі пожежі.

При розрахунку виносу радіонуклідів із зони пожежі використовувалася Гауссова модель. Оскільки лісові масиви України розташовані в європейській частині, то найбільш імовірної є нейтральна стратифікація атмосфери (категорія Б по класифікації Пасквіла). Аналіз сценаріїв минулих лісових пожеж показав, що умови надходження радіонуклідів в атмосферу залежно від типу лісової пожежі (верхова, низова, перехідна та ін.) [5].

Відомо, що ризики радіаційно-індукованих захворювань, що мають стохастичну природу, для злоякісних пухлин становлять $1{,}3 \cdot 10^{-2}$ та $1{,}7 \cdot 10^{-2}$ – для генетичних мутацій на 1 люд.·Зв колективної дози. З даних моніторингу видно, що найбільший ризик одержання вищевказаних захворювань за рахунок опромінення при лісових пожежах має контингент, що проживає на забруднених територіях Київської, Житомирської та Чернігівської областей.

Ця група населення, починаючи з 1986 року, щорічно піддається також опроміненню за рахунок первинного впливу радіонуклідів чорнобильського походження, внесок від якого в даній роботі не враховувався. У зв'язку з актуальністю оцінки комплексного ризику для населення радіаційно-забруднених територій України від впливу двох факторів опромінення передбачається і надалі проводити дослідження в цьому напрямку [6].

Запропонована методика визначення радіаційного ризику забруднення місцевості у зоні впливу військових дій за даними радіаційної розвідки дозволить оцінити і в ряді випадків поліпшити якість прогнозу території дослідження.

Література

1. Загальні вимоги до розвитку і розміщення потенційно небезпечних виробництв з урахуванням ризику надзвичайних ситуацій техногенного походження/ НАН України, Рада по вивченню продуктивних сил України. Наукові керівники: чл.-кор. НАН України С.І. Дорогунцов і генерал-лейтенант В.Ф. Гречанінов. – К., 1995. – 120 с. Кодекс цивільного захисту України від 02.10.2012 № 5403-VI (Редакція від 12.05.2017)

2. Довгий О.С.,Трофимчук О.М., Коржнєв М.М., Яковлєв Є.О., Триснюк В.М. і інші. Моніторинг мінерально-сировинної бази України та екологічного стану територій її гірничодобувних регіонів у контексті забезпечення їх сталого розвитку. /Довгий О.С.,Трофимчук О.М., Коржнєв М.М., Яковлєв Є.О., Триснюк В.М. і інші. – Київ.; Ніка-Центр -2019. -148с.

3. Trysnyuk, V., Trysnyuk, T., Okhariev, V., Shumeiko, V., Nikitin, A. [2018] Cartographic Models of Dniester River Basin Probable Flooding. Centrul Universitar Nord Din Bala Mare - UTPRESS ISSN 1582-0548.

4. Михайлова А.В., Чумаченко С.М. Особливості класифікації джерел небезпеки, що призводять до надзвичайних ситуацій воєнного характеру // Зб. тез доповідей Міжнародної науково-практичної конференції «Проблеми техногенно-

екологічної безпеки: освіта, наука, практика», 21-22 листопада 2019, Харків, НУЦЗУ. – С. 51-53.
5. В.П. Романюк, В.М. Триснюк, Т.Л. Куртсеітов. Постановка задач ліквідації наслідків природних та техногенних катастроф на території України. Системи управління, навігації та зв'язку. Полтавський національний технічний університет імені Юрія Кондратюка. Полтава. Випуск 3 (61) 2020р. – С. 138-143.
6. Азаров С.І. Оцінка радіаційних наслідків лісових пожеж в Україні / С. Азаров // Український географічний журнал. – 2001. – № 2. – С. 52–54.

УДК 681.5.01: 629.52.7

41.ПОВЕРХНЕВІ ВОДНІ ОБ'ЄКТИ УКРАЇНИ У СКЛАДІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗА УМОВИ РОСІЙСЬКОЇ АГРЕСІЇ

Трофимчук О.М.,Триснюк В.М., Шумейко В.О.
Інститут телекомунікацій і глобального інформаційного простору НАН України
trysnyuk@ukr.net

Surface water objects of Ukraine as part of critical infrastructure objects in the event of Russian aggression. An analytical model for assessing the quality of monitoring tasks of surface water bodies of Ukraine as a part of critical infrastructure facilities under conditions of Russian aggression by means of remote sensing of the earth, remotely piloted devices is proposed. on the state of the environment.
The practical significance of the obtained results is that, on the basis of the improved scientific and methodological apparatus for monitoring surface water bodies, new approaches to comprehensive monitoring of the state of critical infrastructure objects have been developed.

Розвиток та вдосконалення ГІС/ДЗЗ-технологій значно розширює можливості отримання просторової інформації, особливо під час надзвичайної ситуації воєнного характеру та нових комплексних порушень екології довкілля. В Україні на першому місці стоять проблеми моніторингу і екологічного контролю за станом поверхневих водних об'єктів у складі критичної інфраструктури (ОКІ) за умови російської агресії, яка почалася 24 лютого 2022 р.та призвела до формування нового науково -технічного напрямку досліджень - геоінформаційного моделювання та управління екологічними викликами воєнного часу, щодо стану критичної інфраструктури (ОКІ) .

Застосування наземних та навколоземних методів дистанційного зондування Землі в оцінці екологічних викликів збройного конфлікту зараз постає як одна із найбільш актуальних сфер використання геоінформаційного моделювання на основі аерокосмічних баз просторових даних. Кінцевою метою якої є ревіталізаційне планування відновлення раціонального ресурсо- та природокористування та управління природними ресурсами на звільнених

територій, моніторинг екологічних злочинів на окупованих природно-територіальних комплексах, вишукування ефективних методів використання, перш за все незахищених від забруднення поверхневих водних обєктів, як джерел питно-господарського водопостачання (ПГВ) для потреб України в умовах глобального світового кризису викликаний російсько-українською війною [11].

Наукові дослідження та програми у галузі оцінки впливу на на об'єкти критичної інфраструктури під час бойових дій, а також визначення територіальних особливостей екологічних викликів воєнного часу картографічними методами дослідження регламентуються Указом Президента України № 64/2022 «Про запровадження військового стану на території України», Законами України та нормативно- правовими актами відповідних галузевих міністерств, а також директивами центральних органів виконавчої влади.

Головний та важливий напрямок досліджень полягає в отриманні точної координатної прив'язки об'єктів в системі «воєнний об'єкт - військова технологія - вплив на водні об'єкти у складі об'єктів критичної інфраструктури ». Геоінформаційне управління та моделювання екологічних викликів воєнного стану виступає інструментом для розв'язання різноманітних завдань за станом поверхневих водніих об'єктів у складі об'єктів критичної інфраструктури.

Ефективним прикладом цього є робота Світлодарської ТЕЦ, яка безпечно працювала, як стратегічний об'єкт критичної інфраструктури під час важких боїв протягом 2014-2015 рр. Базовою інформаційною основою відповідної серії тематичних карт є матеріали безпілотних літальних апаратів (БПЛА)та космічної зйомки. Більшість досліджень в області екологічного контролю за станом (ОКІ) базується на даних ДЗЗ. У системі питно-господарського водопостачання поверхневі водні об'єкти займають -до 70%), в т.ч. водні ресурси р.р.Дніпра,Сіверського Донця,Південного Буга, Тиси,прибережних водозаборів

Одним із перспективних методів проведення моніторингу об'єктів критичної інфраструктури є дистанційний, що базується на основі комплексного використання космічних, повітряних та рухомих наземних комплексів (систем) спостереження. У якості повітряних комплексів розглядаються дистанційно пілотовані літальні апарати (ДПЛА). Постає необхідність процедури допроєктних вишукувань, що передує геоінформаційному моделюванню - розроблення алгоритму управління аерокосмічними базами даних, як основи природно-ресурсної геоінформаційної моделі визначення екологічних ризиків на окупованих та звільнених територіях України. Розробка зосереджувальної когнітивної моделі ДЗЗ-даних включатиме просторово розподілені дані про обсяги отруйних речовин, що потрапляють до геосфер від бойових машин, використанні природних ресурсів окупантом, стан водних, земельних, мінеральних, рослинних та фауністичних ресурсах. Це закладає геоінформаційний базис для аналізу та оцінки сучасного мілітарного та постмілітарного стану природних ресурсів, планування їх перспективного та екологічно_безпечного використання.

Значна частина стоку ПВО України має транскордонний характер, що визначає значні ризики для безпеки експлуатації систем ПГВ за умови їх потенційного забруднення внаслідок військових дій. В окремих районах Донецької та Луганської області, спостерігається патогенний вплив конфлікту на поверхневі водні об’єкти питногоо водопостачання. Збільшення небезпеки руйнування ставків- накопичувачів і полігонів токсичних відходів (42 тис. об’єктів) і ін. потенційно небезпечних об’єктів (ПНО), в т. в гірничо-добувних районах (ГДР) Донбасу, Кривбасу. Карпатського регіону формує екологічно-небезпечні умови для України. [2]

Найбільш ефективно це реалізовується при дешифруванні результатів зйомки об'єктів критичної інфраструктури з відомими розмірами, як правило, за другорядними геотопологічними ознаками, наприклад, природними та техногенними локаціями - балкам, скупченням бойових машин на території атомних електростанцій. В басейні Дніпра зосереджнно 12 блоків АЕС (із 15 діючих), що дає критичні екологічні ризики для для головного джерела (ПГВ).

За своєю структурою система моніторингу (ОКІ0 повинна виконувати такі функції:

- збір інформації про об'єкт критичної інфраструктури;
- обробка, зведення, угруповання і зберігання інформації;
- моделювання (імітація, організація взаємозв'язків, навчання) фізико-хімічних, еколого формуючих процесів різних видів геоекосистем;
- оцінка поточного стану геоекосистем (ОКІ) та прогноз стану геоекосистем; [3].

Важливо відмітити ланцюговий характер потенційних надзвичайних ситуацій (НС) :водно-екологічного походження : “руйнування ПНО; забруднення ВО; вихід з ладу системи ПГВ”.

Науково-дослідницькі сателіти для відповідних цілей є малофункціональними. Військово-розвідувальні супутники є одним з головних джеоел інформації про територію під час бойових дій і застосовуються також для вивчення виснаження природних ресурсів, вирішення безлічі завдань топографічного та еколого- природоохоронного картографування, а також моніторингу навколишнього середовища в контексті оцінки екологічного впливу на довкілля внаслідок бойових дій [4].

Наявні зруйновані потенційно небезпечні техногенні об'єкти та інженерні порушення за матеріалами ДЗЗ виявляються при дешифруванні. В результаті можна отримати еколого-природоохорону геоінформацію про наявність:

- поширення плям нафтового забруднення у Кременчуцькому водосховищі, внаслідок руйнування Кременчуцького нафтопереробного заводу, шляхи міграції забруднених стічних вод при бомбардуванні водогонів та каналізації м. Одеса;
- визначення екологічного стану водних об'єктів: ступені небезпечності забруднення, зміна берегової лінії та русла річок внаслідок руйнування

мостів, знищення флори та фауни;

- інженерна оцінка стану аварійності лінійних та площадних об'єктів, підтоплення залізничних доріг, руйнування терміналів аеропортів та станцій зберігання пального;
- активізації термокарстових процесів на Західному Донбасі, заболочуванні поліської частини Київської, Житомирської та Чернігівських областей;
- виявлення потенційно небезпечних ділянок критичних порушень навколо АЕС, ТЕС, ГЕС.

Застосування сучасних ДЗЗ-ГІС технологій дозволяє оперативно приймати управлінські рішення для зменшення негативних впливів на поверхневі водні об’єкти України у складі об’єктів критичної інфраструктури та забезпечить їх екологічну стійкість. [4]. Під час проведення дослідження були відпрацьовані науково-методичні підходи, на основі яких удосконалено процедуру проведення моніторингу об’єктів критичної інфраструктури з використанням ДПЛА, яка є основою оперативного виявлення пошкоджень та забруднювачів у ході проведення спостереження за заданою територією. Рекомендації (орієнтовно):

1.Удосконалення моніторингу (ДЗЗ, моделі і ін.).

2.Збільшення використання захищених від поверхневого забруднення прісних підземних вод.

3.Районування території України за рівнем уразливості поверхневих систем ПГВ за умови військових дій

4.Визначення гранично припустимих змін екологічного стану поверхневих водних обєктів, як джерел питного господарського використання.

Висновки

Запропоновано аналітичну модель оцінювання якості виконання завдань моніторингу поверхневих водних об’єктів України у складі об’єктів критичної інфраструктури за умови російської агресії засобами дистанційного зондування землі, дистанційно-пілотованими апаратами. на стан довкілля.

Практичне значення отриманих результатів полягає в тому, що на основі вдосконаленого науково-методичного апарату моніторингу поверхневих водних об’єктів розроблено нові підходи комплексного спостереження за станом об’єктів критичної інфраструктури. Запропоновані пропозиції щодо якісної оцінки та контролю параметрів навколишнього середовища при вирішенні завдань моніторингу.

Література

1. Trofymchuk, O., Kaliukh, I., Klymenkov, O. [2017] TXT-tool 2.380-1.1: Monitoring and early warning system of the building constructions of the livadia palace, Ukraine (Book Chapter). *Landslide Dynamics: ISDR-ICL Landslide Interactive Teaching Tools: Volume 1: Fundamentals, Mapping and Monitoring*

2. Довгий О.С.,Трофимчук О.М.,Коржнєв М.М., Яковлєв Є.О., Триснюк В.М. і інші. Моніторинг мінерально-сировинної бази України та екологічного стану територій її гірничодобувних регіонів у контексті забезпечення їх сталого

розвитку. /Довгий О.С., Трофимчук О.М., Коржнєв М.М., Яковлєв Є.О., Триснюк В.М. і інші. – Київ.; Ніка-Центр -2019. -148с.
3. Trysnyuk, V., Trysnyuk, T., Okhariev, V., Shumeiko, V., Nikitin, A. [2018] Cartographic Models of Dniester River Basin Probable Flooding. Centrul Universitar Nord Din Bala Mare - UTPRESS ISSN 1582-0548
4. В.П. Романюк, В.М. Триснюк, Т.Л. Куртсеітов. Постановка задач ліквідації наслідків природних та техногенних катастроф на території України.. Системи управління, навігації та зв'язку. Полтавський національний технічний університет імені Юрія Кондратюка. Полтава. Випуск 3 (61) 2020р. – С. 138-143.

УДК 621.396.4

42.МЕТОД ЗБОРУ ІНФОРМАЦІЇ ПРО СТАН ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ З ВУЗЛІВ БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ

Чумаченко С.М.[1], Лисенко О. І.[2], Тачиніна О. М.[3], Фуртат О.В.[4], Фуртат С.О.[5], Сушин І. О.[6]

[1] Національний університет харчових технологій, Київ, Україна,
[2,6] Навчально-науковий інститут телекомунікаційних систем Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна,
[3] Національний авіаційний університет, Київ, Україна,
[4,5] Таврійський національний університет імені В.І. Вернадського.
E-mail: s_chum@ukr.net, lysenko.a.i.1952@gmail.com, tachinina5@gmail.com, s30041983@meta.ua, furtatsergij@gmail.com, rubin268@ukr.net

Method of collecting information on the condition of critical infrastructure objects from wireless sensor network nodes

The method of collecting information from the nodes of a wireless sensor network using intelligent adaptive flying information and telecommunication robots (IALITR) is presented. The wireless sensor network (WSN) is considered as the network served by IALITR. The key idea in the development of BSM and IALITR algorithms is the flexible clustering of BSM nodes, which provides the opportunity to implement a rational IALITR traffic route.

The implementation of the mentioned ideas is presented in the form of a mathematical statement of the problem, which is characterized by: technical and algorithmic properties of the network, network nodes, IALITR; requirements for the quality of information (data) collection, requirements for the monitoring information (data) collection system. When synthesizing the decision on board IALITR regarding the choice of a rational method of collecting information from BSM nodes, a systematic approach is used, which allowed: to give intelligence and adaptability to the functioning algorithms of flying information and telecommunication robots; to formulate the stages (components) of the method of collecting information from BSM nodes.

Studies of the effectiveness of the improved monitoring data collection method with different initial data are described: the size of the network, the number of clusters, the number of nodes in the cluster, options for building data collection methods, strategies for flying over nodes in the cluster.

В якості мережі, яку обслуговує ІАЛІТР розглядається безпроводова сенсорна мережа (БСМ). Завдання АЛІТР полягає у зборі інформації (даних) з БСМ. Існуючий на сьогодні тривіальний метод збору даних (метод безпосереднього збору даних з кожного сенсорного вузла БСМ окремо [2, 4]) при застосуванні ІАЛІТР не дозволяє використати усі технологічні можливості ІАЛІТР для підвищення ефективності функціонування БМС (збільшити „час життя" та (або) зменшити час збору інформації і, у підсумку, підвищити надійність, функціональну стійкість та живучість БСМ). Основна перевага тривіального методу полягає у спрощених алгоритмах функціонування і взаємодії БСМ та ІАЛІТР, що призводить до здешевлення апаратних засобів БСМ. Але у багатьох критичних ситуаціях економічна перевага поступається своєю важливістю надійності, функціональній стійкості та живучості БСМ[3-6].

Ключова ідея, яка покладена у розробку алгоритмів взаємодії БСМ та ІАЛІТР, полягає у гнучкій (адаптивній) кластеризації вузлів БСМ, яка надає можливість реалізувати раціональний маршрут руху ІАЛІТР. Згідно із цими алгоритмами пропонується об'єднувати вузли в тимчасові кластери, де роль головного вузла кластера покладається на ІАЛІТР. Алгоритм побудови траєкторії руху ІАЛІТР за відомою інформацією про координати положення вузлів БСМ здійснює розрахунок координат точок збору даних та будує траєкторію руху ІАЛІТР („інтелект дії"). У статті, на відміну від існуючих „жорстких" центроїдних алгоритмів кластеризації, пропонується використовувати „адаптивні (гнучкі)" алгоритми кластерного аналізу, які отримали назви відповідно: алгоритм *k*-середніх та алгоритм формального елементу (for.el). Ці алгоритми характеризуються меншою обчислювальною складністю та надають можливість адаптивно змінювати розміри кластера і, тим самим, керувати кількістю кластерів [4-6].

Синтез рішення інтелектуальним адаптивним літаючим інформаційно-телекомунікаційним роботом. При синтезі рішення на борту ІАЛІТР стосовно вибору раціонального способу збору інформації з вузлів БСМ використовується системний підхід, складові якого представлені на рис.1.

Рисунок 1. Структура системного підходу стосовно вибору раціонального способу збору інформації з вузлів БСМ

Системний підхід дозволяє:

1) надати алгоритмам функціонування ЛІТР інтелектуальності та адаптивності;

2) сформулювати етапи (складові) методу збору інформації з вузлів БСМ.

Складові методу збору інформації з вузлів БСМ.

1. Спосіб безпосереднього збору даних з кожного вузла мережі – з обльотом кожного вузла, з обльотом території (де розташована БСМ), з обльотом кластерів БСМ.

2. Спосіб оптимізації операцій стосовно управління – ізольовано (центр управління мережею, система управління ІАЛІТР, система управління вузла БСМ або кооперовано – у взаємодії між ними; при наявності або відсутності інформації про стан вузлів БСМ у ІАЛІТР (ЦУ мережею); централізовано або децентралізовано.

3. Порядок та правила кластеризації БСМ:

а) розрахувати кількість і розміри кластерів (повинна бути проведена оптимізація кількості та розмірів кластерів в залежності від різних цільових функцій управління мережею на етапі збору даних);

б) провести кластеризацію мережі і визначити точки збору даних моніторингу за певними параметрами в залежності від цільових функцій управління мережею і ситуації в мережі;

в) визначити моделі (алгоритми) обміну даними між ІАЛІТР і вузлами кластера;

г) розрахувати стратегії та параметри обльоту ІАЛІТР вузлів в кластерах по заданим цільовим функціям (побудова, оптимізація та корегування шляху обльоту ІАЛІТР вузлів в залежності від цільових функцій управління та наявних ресурсів ІАЛІТР і вузлів БСМ).

При наявності інформації про стан БСМ ці завдання вирішуються централізовано центром управління мережею (ЦУМ). При її відсутності – децентралізовано: ІАЛІТР і вузлами мережі у взаємодії. [1-3]

4. Побудувати маршрути обльоту точок збору даних ІАЛІТР: базового (обльоту всієї мережі БСМ) та маршрутів обльоту кожного з кластерів. Наприклад, базові параметри польоту розраховує ЦУМ, а ІАЛІТР здійснює коригування базового маршруту в кластерах після отримання інформації про стан вузлів кластера при підльоті до нього та наявності відповідних ресурсів.

5. Визначити критерії та їх пріоритет при управлінні процесом збору даних, а саме: мінімізація часу збору даних, максимум часу функціонування БСМ, мінімум ІАЛІТР, мінімізація витрат енергії вузлів в процесі передачі від вузлів до ІАЛІТР, тощо.

6. Визначити модель польоту на основі наявності або відсутності інформації про координати знаходження вузлів БСМ, з постійною або адаптивною швидкістю, з гарантією обслуговування або її відсутністю.

7. Моделі польоту ІАЛІТР при зборі даних моніторингу з БСМ.

Формування та реалізація параметрів польоту ІАЛІТР відбувається в два етапи.

На першому – центр управління мережею будує базовий найкоротший маршрут з обльоту точок збору даних в БСМ одним з відомих алгоритмів вирішення задачі комівояжера [2-6], (наприклад, метод найближчого сусіда) визначає середню швидкість і висоту польоту.

На другому – при підльоті до чергового кластера ІАЛІТР коригує параметри свого обльоту (траєкторію, швидкість, якість обслуговування) в залежності від кількості вузлів в кластері, параметрів вузлів кластера (місцеположення, наявна енергія батарей вузлів та обсяги даних моніторингу), наявних особистих ресурсів (енергії та часу, що залишився на політ) і цільових функцій управління мережею. Так, наприклад, при існуванні „критичних” вузлів в кластері („виснажених”, „перевантажених” тощо) їх обліт (обслуговування) пропонується здійснювати на мінімальній відстані до них з пріоритетом в обслуговуванні. Для забезпечення гарантії часу збору даних розраховується та реалізується необхідна швидкість польоту (зависання ІАЛІТР в певній точці простору на потрібний час).

При цьому доцільно розглядати різні моделі польоту.

1. Базова найпростіша модель.

Політ з однаковою постійною швидкістю в кластері та між кластерами спрощує управління переміщенням ІАЛІТР, не висуває додаткових вимог до БПЛА, може використовуватися як гвинтокрилий так й літаковий тип БПЛА. Збір даних починається при встановленні радіозв’язку з першим вузлом кластера. Час збору дорівнює часу польоту через кластер. Дані, які вузли не встигли передати, зберігаються в вузлах до наступного раунду польоту. При прильоті до зони радіозв’язності з базовою станцією ІАЛІТР передає їй дані та починає новий цикл обльоту. Модель може бути реалізована як роторним так і літаковим типом БПЛА.

2. Політ ІАЛІТР з однаковою постійною швидкістю достатньою для обслуговування кластера та з підвищеною швидкістю (визначається можливостями БПЛА) при переміщенні між кластерами.

Для реалізації моделі необхідні БПЛА зі змінною швидкістю польоту. Ця модель може бути реалізована як роторним так і літаковим типом БПЛА.

3. Політ з адаптивною швидкістю в кластерах.

Для визначених типів додатків може бути необхідна різна швидкість обміну даними, яка визначається зовнішніми факторами такими як надзвичайна ситуація. Наприклад, деякі вузли можуть мати спеціальні можливості збору та передачі аудіо та відео даних, які можуть бути потрібними в певні моменти часу (поява порушника в зоні контролю, висока температура, тиск та вібрація в трубопроводі тощо). Крім цього для гарантованого збору даних необхідно адаптувати швидкість передачі до необхідного часу передачі даних.

Рішення про збільшення або зменшення часу збору інформації приймається ЦУМ або СУ ІАЛІТР разом з вузлом-джерелом цих даних. Можуть бути використані БПЛА гвинтокрилого та літакового типу.

4. Політ з гарантованим обслуговуванням вузлів кластера.

ІАЛІТР розраховує час обслуговування всіх вузлів при постійній швидкості передачі. При браку часу вираховується додатковий час. Необхідно відмітити, що ця модель може бути використана в сценаріях надзвичайних ситуацій або спеціальних місіях, де моніторинг певного географічного району або „гарячої точки ” вимагається за певний період часу.

Модель може бути використана для передачі трафіку реального часу. Використовуються БПЛА роторного типу.

5. Політ з обмеженням максимального часу обслуговування кластера (вузла).

Вузол певного кластера в змозі зібрати досить великий обсяг даних, що вимагає дуже значного часу його обслуговування. Одночасно час інші вузли теж очікують обслуговування в цьому циклі польоту, час затримки в обслуговувані певних додатків може бути перевищений, буфери інших вузлів кластера можуть бути переповнені тощо. Тому для справедливого обслуговування встановлюється граничний час обслуговування для кожного кластера. Якщо кількість даних в кластері не може бути обслужена в період цього циклу обльоту, тоді не обслужена частина даних переноситься на наступний раунд польоту. Використовуються БПЛА гвинтокрилого типу. Ця модель також може бути застосована для забезпечення безпеки системи збору даних в цілому. Вона запобігає захопленню ІАЛІТР вузлом супротивника, який виставив вимогу безмежно великого буферу та організує атаку типу „вимога в обслуговуванні” (DoS-атака).

Вважається, що ІАЛІТР має інформацію про координати вузлів, які можуть бути отримані одним із таких способів:

1. На етапі розгортання наземних мереж при детермінованому розміщенні вузлів фіксуються координати кожного з вузлів при його розміщенні.

2. У разі випадкового розгортання вузлів мережі ІАЛІТР здійснює первинний обліт території, що покривається наземними вузлами БСМ, і збирає дані про координати вузлів в припущенні наявності в вузлах системи позиціонування. В цьому випадку маршрут польоту будується з метою покриття всієї території спостереження. В процесі обльоту ІАЛІТР збирає як інформацію моніторингу, так інформацію про стан вузлів і кластерів для подальшого планування завдань управління.

3. При наявності зв'язної топології вузлів БСМ з наземним шлюзом з'являється можливість збору центром управління інформації про стан і координати розташування сенсорних вузлів.

Розглянемо результати моделювання для наступних основних вихідних даних. Однорідні вузли БСМ розташовані випадковим чином на певної площині. Кількість сенсорних вузлів – $N = 400$. Кількість вузлів в кластері – n_k=10, 20, 50. Початкова енергія вузлів – e_0=0.1 J. Дальність радіозв'язку – $d_{\max} = 250$ м, максимальна висота польоту ІАЛІТР – $h_{\max} = 250$ м, максимальна швидкість польоту – $v_{\max} = 10$ м/с, кількість раундів обльоту – $NR_{зад} = 700$. Протокол доступу до каналу IEEE 802.11g, розмір даних моніторингу вузла – 100 Кб.

Будем розглядати та порівнювати наступні методи збору даних за відповідними класами:

1. Відомий метод безпосереднього збору при центроїдній кластеризації.

2. Вдосконалений (запропонований у статті) метод безпосереднього збору даних з вузлів ІАЛІТР при реалізації різних стратегій (правил обльоту та обміну даними в кластерах):

а) стратегія № 1 – точка збору даних ІАЛІТР тільки в центрі кластера;

б) стратегія № 2 – збір інформації ІАЛІТР з врахуванням правил обльоту „критичних" вузлів;

в) стратегія № 3 – збір інформації ІАЛІТР з врахуванням правил обміну з вузлами, ближчими до траєкторії обльоту кластера;

г) стратегія № 4 – збір інформації ІАЛІТР з вузлів при кооперативній роботі по створенню мінікластерів та побудови енергоефективних маршрутів до вузлів, які знаходяться ближче до маршруту обльоту кластера;

Ефективність функціонування методів будемо порівнювати за критеріями: час збору даних моніторингу $T_{зб}$ та час функціонування БСМ – $T_ф$ (за фізичним змістом - це час від початку роботи БСМ до моменту часу, коли в наслідок інформаційного обміну буде витрачено увесь запас енергії акумуляторної батареї останнього вузла. Якщо $T_ф = 100\%$ – це означає що немає працездатних вузлів для передачі даних, тобто в останньому вузлі залищок енергія споживання $e_{сп}$ стає нулем. Чим вище значення $T_ф$, тим менша кількість працездатних вузлів залишається в мережі). Моделювання та розрахунки здійснено в системі комп'ютерної математики MATLAB.

З результатів моделювання, спостерігається загальна тенденція – зі збільшенням раундів збору даних ІАЛІТР зменшується середня енергія споживання та збільшується кількість непрацездатних вузлів в мережі. Це пояснюється наступним: на початкових раундах обльоту кожний кластер містить

багато працездатних вузлів, але ця кількість зменшується зі зростанням кількості раундів обльоту.

Кращі результати серед трьох стратегій продемонструвала стратегія № 3 (найменше споживання енергії і найменший відсоток непрацездатних вузлів) у порівнянні з результатами у попередніх двох стратегій.

Застосування кооперативної стратегії № 4 (маршрутизація даних з вузлів кластера до вузла, який знаходиться ближче до траєкторії польоту ІАЛІТР з використанням енергоефективних метрик пошуку маршруту) показало помітну перевагу в низькому споживанні енергії та часі функціонування мережі .

Так після 600 раундів, в усіх трьох стратегіях різко знижується кількість працездатних вузлів (стратегії № 1 – 3), але 40% працездатних вузлів залишається при використанні стратегії № 4. Показано, що щільніше розташування вузлів призведе до меншого енергоспоживання і більшої тривалості часу функціонування. Це є результатом використання енергоефективної метрики побудови маршруту для пошуку маршрутизатора з більшою енергією батареї.

Висновки

Наведено порівняльне моделювання вдосконаленого безпосереднього методу збору даних ІАЛІТР з існуючим центроїдним методом збору даних моніторингу, аналіз чотирьох стратегій обльоту кластера (тільки між центрами точок збору; обліт критичних об’єктів).

У запропонованого методу в порівнянні з методом HEED час збору даних менший в середньому на 14% за рахунок використання та пріоритету метрики вибору головного вузла кластера – коротша відстань до траєкторії польоту ІАЛІТР. Виграш збільшується з зростанням частки вузлів, які відмовили. Витрати енергії вузлів при реальній кластеризації в запропонованому методі зменшуються на 10 – 15% внаслідок застосування енергозберігаючих правил побудови топології кластерів, вирівнювання витрат енергії вузлів при побудові маршрутів передачі в кластері (вибираються з множини можливих маршрутів передачі між вузлом та ГВК маршрути, які мають мінімум витрат енергії на передачу та вузли, рівень батарей яких не превищують граничний рівень).

Література

1. Uryvsky L., Lysenko O., Novikov V., Osypchuk S. (2022) Control Methods Research of Indicators for Intelligent Adaptive Flying Information-Telecommunication Platforms in Mobile Wireless Sensor Networks. In: Klymash M., Beshley M., Luntovskyy A. (eds) Future Intent-Based Networking. Lecture Notes in Electrical Engineering, vol 831. P. 444-467. – 2022. Springer, Cham. https://doi.org/10.1007/978-3-030-92435-5_25

2. Oleksandr Lysenko, Valery Romaniuk, Ihor Sushyn, Valery Novikov. The Improvement Direct Method for Collecting Monitoring Data from the Wireless Sensor Network Nodes with their Clustering by Telecommunications Aerial Platforms/ IEEE - International Conference on Information and Telecommunication Technologies and

Radio Electronics . UkrMiCo'2021, Kyiv, Ukraine, November 29 – December 3, 2021. - С. 123-126. ISBN: 978-1-6654-2651-0.
3. Olena Tachinina, Olexandr Lysenko, Iryna Alekseeva, Valeriy Novikov, Ihor Sushyn. Methods for Parametric Adjustment of a Digital System and Precision Automatic Stabilization of an Unmanned Aerial Vehicle. 2021 IEEE 6th International Conference on Actual Problems of Unmanned Aerial Vehicles Development (APUAVD). IEEE Catalog Number: CFP2129V-USB. ISBN: 978-1-6654-3821-6. Oktober 19-21, 2021, Kyev, Ukraine . С. 76-79. http://apuavd.ieee.org.ua/wp-content/uploads/2021/11/53804_CFP2129V-USB.pdf
4. Романюк В.А., Лисенко О.І., Романюк А.В., Новіков В.І., Гуйда О.Г. Метод збору інформації з вузлів безпроводової сенсорної мережі з використанням інтелектуальних адаптивних літаючих інформаційно-телекомунікаційних роботів. Вчені записки таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки. Том 32 (71) № 2 2021. - С. 25-35. Сторінка журналу: www.tech.vernadskyjournals.in.ua. ISSN 2663-5941 (Print). ISSN 2663-595X.
5. Лисенко О.І., Тачиніна О.М., Новіков В.І., Гуйда О.Г., Сушин І.О. Теоретичні основи конструювання керування рухом розподіленого інформаційно-телекомунікаційного робота. Вчені записки таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки**.** Том 32 (71) № 3 2021**.** - С. 55-62. Сторінка журналу: www.tech.vernadskyjournals.in.ua. ISSN 2663-5941 (Print).
6. Лисенко О.І., Тачиніна О.М., Кисельов В.Б., Новіков В.І., Гуйда О.Г., Сушин І.О. Метод розміщення сенсорів літаючими інформаційно-телекомунікаційними роботами динамічними чергами**.** Вчені записки таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки**.** Том 32 (71) № 4 2021**.** - С. 53-59. Сторінка журналу: www.tech.vernadskyjournals.in.ua. ISSN 2663-5941 (Print).

РОЗДІЛ 6

МІЖНАРОДНІ СТАНДАРТИ У ГАЛУЗІ ІНФОРМАЦІЙНИХ І ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ.

УДК 628.472

43.ПОТОЧНИЙ СТАН ПОТЕНЦІАЛУ ПЕРЕТВОРЕННЯ ВІДХОДІВ В ЕНЕРГІЮ: ОГЛЯД СИТУАЦІЇ В ПОЛЬШЕ

Viola Vambol[1*], Alina Kowalczyk-Juśko[1], Sergij Vambol[2], Nadeem Ahmad Khan[3]
1 University of Life Sciences in Lublin, Lublin, Poland
2 National Technical University Kharkiv Polytechnic Institute, Kharkiv, Ukraine
3 Mewat Engineering College, Nuh, Haryana-122107, India
**E-mail: violavambol@gmail.com*

CURRENT STATUS OF WASTE-TO-ENERGY POTENTIAL: AN SITUATION OVERVIEW IN POLAND

To maintain energy security and improve the quality of the natural environment, a transition to a low-carbon economy is necessary. The average level of household waste recycling according to Eurostat in 2017 in Poland was 35.2%. The system of separate collection of municipal waste continues to develop in recent years, however, the annual tonnage of mixed waste is still significant and contains about 60-62% of high-calorie raw materials. It is possible to increase the efficiency of energy recovery from mixed waste using mechanical biological treatment technology.

The immediate threat to the world's largest consumers of raw materials is the shortage of resources, which leads to concern around the world, and contributes to the search for ways to increase the efficiency of their use. Europe is also seriously concerned about finding new solutions to this issue [1], especially against the backdrop of emerging conflicts in the world and a long-term trend associated with an increase in energy consumption. Statistics show that in the period from 1988 to 2018, the volume of mineral fuels (coal, oil, natural gas, oil shale) increased from 9.3 billion tons to 15.2 billion tons, since fuel and energy resources are the basis of the economy of any state [2].

In this regard, the EU countries are focused on resource efficiency, waste, and environmental innovation. Preventing the accumulation of waste by converting it into resources, combined with increased resource efficiency, has a significant impact on the environment, society and the economy. The transition to a low-carbon economy in Poland is very important to maintain energy security and improve the quality of the natural environment. At the same time, minimizing the use of fossil fuels in production processes, creating innovative environmental solutions and using the existing potential in the development of renewable energy sources are important elements in the formation of a low-carbon economy [3].

It has been repeatedly confirmed that the waste contains significant energy potential, and one of the best ways to manage waste is to convert it into energy [4]. The average level of recycling of household waste in all EU countries in 2017 was estimated

by Eurostat at 46.6%. The nationwide assessment of Poland was 35.2%, unfortunately, regional statistics are not available [5].

This work was carried out in accordance with the results of the analysis of reports of official government organizations available through the Internet resources, and scientific studies, the search for which was carried out using ScienceDirect. Conducting scientific research in the field of converting waste into energy every year is more and more intensive, which confirms the relevance of the problem. For the query "potential waste to energy" since 2012, 341534 results have been found in ScienceDirect (24.02.2023) (Fig. 1a). At the same time, after two key words "potential waste to energy Poland, Europe" were added to the query, 7991 results were received for the same period (24.02.2023) (Fig. 1b), which corresponds to 2.1... 2.6% research of the total number of publications on this topic each year.

Fig. 1. The intensity of scientific research in the field of converting waste into energy: a - for the countries of the world; b - for Poland

For the purpose of converting waste into energy, the biological process in sanitary landfills and the thermal process in the form of various technologies can be used. This requires organic, wood, agricultural waste, municipal waste, etc. According to the Environment 2018 - 2022 reports from Statistics Poland (Warsaw), the separate waste collection system in Poland is improving every year (Fig. 2), with the largest share, in recent years, being biodegradable waste 28.1%; 30.1%; 32.4%; 33.9% respectively from 2018 to 2021.

However, mixed municipal waste still makes up a significant share of the total amount of waste generated and, as a rule, is landfilled.

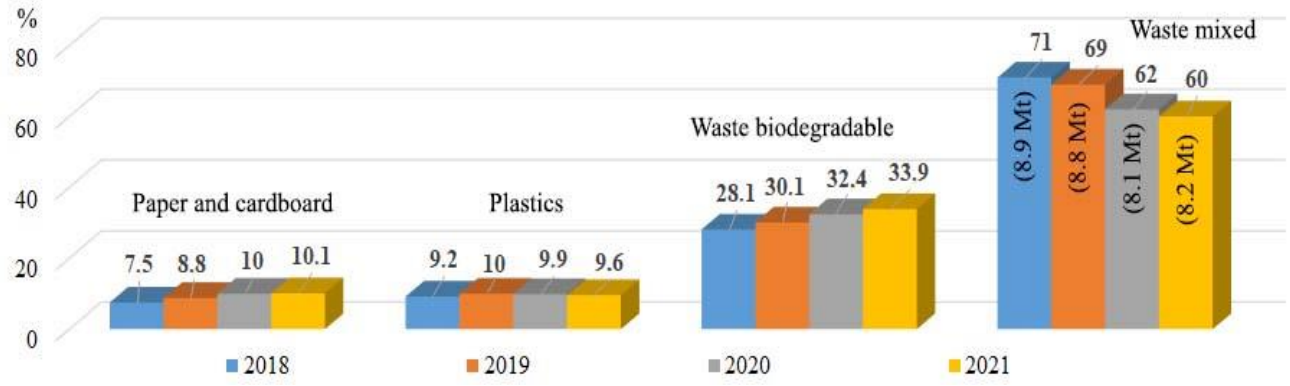


Fig. 2. Percentage of waste potentially suitable for energy production

Waste collected separately is usually converted into resources, while mixed waste is stored in landfills and also has energy and resource potential. And although there is a systematic reduction in the number of operating landfills of 286 pieces at the end of 2018, 278 pieces, 271 pieces and 265 pieces, respectively, at the end of 2019, 2020 and 2021, the tonnage of mixed waste for the year still remains significant and contains about 60-62% mixed package, which is a high-calorie raw material.

According to studies for mixed waste, Mechanical Biological Treatment (MBT) technology is environmentally, economically and socially acceptable, including waste sorting and biological treatment (such as anaerobic digestion and composting). A study [6] showed that the use of MBT technology before disposal in landfills allows the extraction of inorganic materials and reduces the mass by up to 30%, and as a result, the environmental impact is reduced. Researchers recommend this technology for countries with a low level of recycling, since practical testing of this technology with a capacity of 100 tons of waste per day [7] demonstrates the receipt of 33% refuse derived fuel (RDF) and 5% compost, recovery of 12% of recyclable waste; production of 0.435 MWh/day, biogas and methane in the amount of 0.535 and 0.350 m^3/kg VSadded (average), respectively, with 40% volatile solids removal (average total solids 10%); net operating costs of $17 per ton of waste; minimization of greenhouse gas emissions.

Controlled landfills in Poland are equipped with degaussing plants, however, only 27% of these plants operate with energy recovery, which generated 105.4 - 113.1 million kWh of electricity per year from 2018 to 2021, while it is possible to obtain in times more energy if other approaches are used. Since RDF is a secondary raw material from mixed municipal waste, which may include organic waste (domestic origin), rubber, plastic, cardboard, paper, wood, leather, synthetic fabrics, textiles, polymeric materials, its combustion, for example, in thermal power plants, has a higher thermal efficiency than the efficiency of an incineration plant [8].

A positive feature of MBT technology is that it is not a single technology and a complete solution, since it is a set of operations that is selected depending on the composition of the waste.

Therefore, by continuing to develop and improve the system of separate collection of household waste, as well as by introducing efficient technologies for the processing of mixed solid waste, it is possible to reach a high level of energy recovery.

Reference

1. Welfens, P., Bleischwitz, R., & Geng, Y. (2017). Resource efficiency, circular economy and sustainability dynamics in China and OECD countries. International Economics and Economic Policy, 14, 377-382.
2. World Mining Data 2020, World Mining Congresses. Available: https://www.world-mining-data.info/wmd/downloads/PDF/WMD2020.pdf.
3. Dzikuć, M., Gorączkowska, J., Piwowar, A., Dzikuć, M., Smoleński, R., & Kułyk, P. (2021). The analysis of the innovative potential of the energy sector and low-carbon development: A case study for Poland. Energy Strategy Reviews, 38, 100769.
4. Bazregari, M. J., & Norouzi, N. (2022). A parametric exergy and energy analysis of the municipal solid waste dryer system: With a comparative-analytic approach toward recent experimental methods. Cleaner Engineering and Technology, 6, 100389.
5. Zając, P., & Avdiushchenko, A. (2020). The impact of converting waste into resources on the regional economy, evidence from Poland. Ecological Modelling, 437, 109299.
6. Trulli, E., Ferronato, N., Torretta, V., Piscitelli, M., Masi, S., & Mancini, I. (2018). Sustainable mechanical biological treatment of solid waste in urbanized areas with low recycling rates. Waste Management, 71, 556-564. https://doi.org/10.1016/j.wasman.2017.10.018
7. Tyagi, V. K., Kapoor, A., Arora, P., Banu, J. R., Das, S., Pipesh, S., & Kazmi, A. A. (2021). Mechanical-biological treatment of municipal solid waste: Case study of 100 TPD Goa plant, India. Journal of Environmental Management, 292, 112741. https://doi.org/10.1016/j.jenvman.2021.112741.
8. Burnley, S., Phillips, R., Coleman, T., & Rampling, T. (2011). Energy implications of the thermal recovery of biodegradable municipal waste materials in the United Kingdom. Waste Management, 31(9-10), 1949-1959.

44.ENVIRONMENTAL PROTECTION THROUGH INTERNATIONAL CRIMINAL LAW

Aaron Dumont[1]

Why International Criminal Law?

International Criminal Law (ICL) can only be effective in a repressive way, as reactions to violations of international rules and state obligations. The protection of a legal object - in this case, the environment - could be better served if the violation of standards were *prevented* beforehand. The primary regime for this purpose is International Humanitarian Law (IHL) - The jus in bello. IHL defines the 'law of armed conflict'. In fact, IHL also has some rules to protect the environment (directly or indirectly) within the Hague Law[2], Geneva Law[3], the special Convention on the Prohibition of Military or any Other Hostile Use of Environmental Modification Techniques (ENMOD) [4] and Customary International Law.

However, all these regimes have in common that their enforcement mechanisms are deficient - Particularly if a party to the conflict was a UN Security Council (SC) member. Moreover, the actus reus thresholds for the rules mentioned earlier are too high to be effectively applied.[5] In cases of violation of IHL obligations, Article 3 Hague IV, Article V (5) ENMOD, and Article 91 AP I refer to the general Articles of State Responsibility (ASR).[6] According to these, states must immediately cease[7] violating obligations and shall pay reparations[8]. However, enforcement of these secondary obligations is carried out by a decision of the UN Security Council. Russia has a veto right,[9] which means effective enforcement of any environmental IHL violations in the Ukraine-Conflict does not seem realistic. Furthermore, some authors deny deterrent effects of this mechanism altogether. [10] It is assumed that a solely financial 'risk' to pay for reparations is not sufficient for states to refrain from

[1] The author holds a degree in law from Ruhr-University Bochum (RUB) with a specialization in international law.
He is a research associate and PhD student at the Institute for International Law of Peace and Armed Conflict
(IFHV) at RUB. Contact: IFHV, Bochumer Fenster, Room 4.22, Massenbergstr. 9B, 44787 Bochum, Germany.
Email: aaron.dumont@rub.de.

[2] Article 23 Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, 18 October 1907.

[3] Article 35 (1) and 55 (1), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (AP I).

[4] Article I (1), The Convention on the Prohibition of Military or any Other Hostile Use of Environmental Modification Techniques of 18 May 1977.

[5] A. Dienelt, *Armed Conflicts and the Environment* (2022), at 64.

[6] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, November 2001, Supplement No. 10 (A/56/10), chp.IV.E.1.

[7] Article 30 ASR.

[8] Article 31 ASR.

[9] Article 27 (3), United Nations, *Charter of the United Nations*, 24 October 1945, 1 UNTS XVI (UNCh).

[10] Schmitt, 'Green War: An Assessment of the Environmental Law of International Armed Conflict', 22 *Yale Journal of International Law* (1997) 1, at 91.

environmentally harmful acts if these would promise a military advantage in conflicts. UN mechanisms would compensate but not sanction environmental damage.[11]

Hence why IHL enforcement mechanisms are said to be inadequate concerning environmental violations.[12] Therefore, in order to ensure effective deterrence, individual accountability is needed.[13] International Criminal Law seems to be the correct forum for that endeavor.

Environmental Protection under International Criminal Law

The rules of ICL are mainly contianed in the Rome Statute[14] (RS).[15] The RS incorporates the four core crimes of ICL - Genocide, Crimes against Humanity, War Crimes, and the Crime of Aggression. The environment is protected under the Rome Statute through a specific environmental protection rule or 'green criminology'. The specific norm on environmental protection is found in Article 8 (2) (b) (iv) RS and is framed as a War Crime. It prohibits the conduct of: "*intentionally launching an attack in the knowledge that such attack will cause [...] widespread, long-term and severe damage to the natural environment which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated*." The rule is criticized for its high *actus reus* and *mens rea* thresholds.[16] As a result of its high thresholds, no individual has yet been convicted under Article 8 (2) (b) (iv) RS.[17]

Actus Reus

In its actus reus, Article 8 (2) (b) (iv) RS requires widespread, long-term, and severe (w-l-s) damage to the natural environment. The three criteria are formulated based on ENMOD and Articles 35/55 AP I. Unlike Article I (1) ENMOD, however, the requirements of Article 8 (2) (b) (iv) RS are cumulative and not alternative, so a connection to Article 35 AP I can be assumed. The criteria are not defined in the Rome Statute itself. Thus, the International Criminal Law doctrine falls back on the interpretation from AP I.[18] The Travaux préparatoires (TP) of AP I refer to long-term as "damage that last decades".[19] For the remaining criteria, however, the TP are silent. Some Authors define severe as "a serious or significant harm to natural resources"[20]

[11] Dienelt, *supra* note 5, at 37.
[12] *Ibid.*, at 38.
[13] Jessica C. Lawrence and Keven Jon Heller, 'The First Ecocentric Environmental War Crime: The Limits of Article 8(2)(b)(iv) of the Rome Statute', 61 *Georgetown International Environmental Law Review* (2007) 61, at 68.
[14] UN General Assembly, *Rome Statute of the International Criminal Court (last amended 2010)*, 17 July 1998.
[15] There are also international conventions (e.g. *Genocide Convention*) and domestic regimes.
[16] Jessica C. Lawrence and Keven Jon Heller, *supra* note 13, at 75.
[17] Killean, 'From ecocide to eco-sensitivity: 'greening' reparations at the International Criminal Court', 25 *The International Journal of Human Rights* (2021) 323, at 329.
[18] Jessica C. Lawrence and Keven Jon Heller, *supra* note 13, at 73.
[19] Report of Committee III, Second Session (CDDH/215/Rev.1; XV, 263), in H.S. Levie, 2 Protection of War Victims: Protocol I to the 1949 Geneva Conventions 276-77 (1980), at 276 [hereinafter Report of Committee III, Second Session].
[20] Low and Hodgkinson, 'Compensation for Wartime Environmental Damage: Challenges to International Law after the Gulf War', 35 *Virginia Journal of International Law* (1995) 405, at 433; K. Ambos (ed.), *Rome Statute of the International Criminal Court*: *Article-by-article commentary* (2022) mn. 252.

and widespread as an area stretching over "several hundred kilometres".[21] The extent of these thresholds can be seen in particular concerning the burning oil wells in the Gulf War of 1991.[22] Despite the significant environmental damage caused by these events, the UN Security Council did not approve any widespread, long-term and severe environmental damage in the ruling of AP I. [23] This was also due to the fact that the prescribed parameters are difficult to grasp scientifically. A few years after an attack occured, it could turn out that the environmental damage was not as severe as initially assumed.[24] Such an uncertainty of actus reus may even violate the principle of legality.[25] These concerns were raised, among others, in investigating the NATO bombing campaign in Yugoslavia.[26]

However, this does not mean the International Criminal Court (ICC) identifies the same problems in Article 8 RS. Thus, other authors have considered a possible criminal liability in the Iraqi offences.[27] By accepting an investigation, the ICC could finally uniformly define the actus reus of Article 8 (2) (b) (iv) RS. That the ICC sees an opportunity here is based in no small part on the 2016 OTP Policy Paper, in which the Office of the Prosecutor (OTP) set a focus on environmental offenses for future investigations and conducts.[28] However, it can only do so if it finally utilizes its only ecocentric norm and defines its actus reus through case law.

Mens Rea

In its *mens rea* (subjective element), the rule requires that the offender was: "Intentionally launching an attack in the knowledge that such attack will cause [...] damage [...] which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated." The perpetrator must not only be intentionally launching (1), but must also know that the attack will cause w-l-s damage (2) and that the military advantage would be significantly less than the environmental damage. *Knowledge* is defined in the Rome Statute as: "awareness that a circumstance exists or a consequence will occur in the ordinary course of events. "(Article 30 (3) RS). The ICC defined "ordinary course of events" as "virtually certain".[29] Here, the first criticism is that the reference to undefined elements of the offense in the subjective element was a circular argument.[30] A perpetrator can never have known something "virtually

[21] Ambos, *supra* note 20 mn. 252.
[22] *The Guardian,* 11 December 2021.
[23] Low and Hodgkinson, *supra* note 20, at 413.
[24] Weinstein, 'Prosecuting Attacks that Destroy the Environment: Environmental Crimes or Humanitarian Atrocities', 17 *Georgetown International Environmental Law Review* (2005) 697, at 708.
[25] Jessica C. Lawrence and Keven Jon Heller, *supra* note 13, at 75.
[26] Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, 17 (June 8, 2000) 39 I.L.M. 1257 [hereinafter Final Report].
[27] Mistura, 'Is There Space for Environmental Crimes under International Criminal Law: The Impact of the Office of the Prosecutor Policy Paper on Case Selection and Prioritization on the Current Legal Framework', 43 *Columbia Journal of Environmental Law* (2018) 181, at 212; Sharp, 'Prospects for Environmental Liability in the International Criminal Court', 18 *Virginia Environmental Law Journal* (1999) 217, at 242.
[28] Office of the Prosecutor International Criminal Court, Policy Paper on Case Selection and Prioritisation (2016), at 14.
[29] ICC, The Prosecutor v. Jean-Pierre Bemba Gombo, Decisions Pursuant to Article 61(7)(a) and (b) of the Rome Statute on the Charges, 15 June 2009, ICC-01/05–01/08, mn. 362.
[30] Jessica C. Lawrence and Keven Jon Heller, *supra* note 13, at 79.

certain" that was not defined beforehand. Secondly, the available data on forecasting environmental damage by attacks seems to be so poor that it is hardly possible for a perpetrator to anticipate the consequences of an attack *ex-ante,* especially the *long-term* and *widespread* consequences, as can also be seen in the example of the Gulf War.[31]

Green Criminology

Due to the operational problems of Article 8 RS, some authors[32] place their hopes not in the dedicated Article 8 (2) (b) (iv) RS, but in "greening" the remaining rules- especially genocide (Article 6 RS) and crimes against humanity (Article 7 RS). 'Green Criminology' means that the caused environmental damage is used by the perpetratory as a method to substantively fulfil other offenses. An example of this might be the ICC Pre-Trial Chamber decision of 2008.[33] There, a link between genocide and environmental damage was found in the sense that the accused was proven to have, among other things, systematically polluted or poisoned water sources and communal wells to fulfil Article 6 (c) RS. However, it must be considered that Article 6 RS has the highest mens rea requirement[34] in the Rome Statute, which means that this Genocide-Ecocide connection will rarely be establishable.[35] The OTP must prove that a perpetrator intended to use the means of environmental destruction to (physically) exterminate all or part of a group designated in Article 6 RS.

Therefore, another alternative is Crimes Against Humanity described in Article 7 RS. The lower subjective threshold of the offense might make a conviction more likely.[36] Thus, it seems that a conviction via Article 7 could be the most promising scenario in the Rome Statute to convict environmental crimes in conflict.

Reparations via Trust Fund for Victims

A conviction could allow the Trust Fund for Victims to provide physical or physical rehabilitation or to bring material support to victims.[37] However, attention should be paid to eco-sensitivedistribution of money, so as not to negatively impact peace in the region negatively.

[31] Schmitt, *supra* note 10, at 59.
[32] Freeland, 'Human Rights, the Environment and Conflict: Addressing Crimes against the Environment', 2 *Sur - International Journal on Human Rights* (2005) 113, at 133; Killean, *supra* note 17, at 331.
[33] ICC Pre-Trial Chamber, Situation in Darfur, The Sudan, 'Public Redacted Version of Prosecution's Application under Article 58 Filed on 14 July 2008', Case No. ICC-02/05-157, 12 September 2008.
[34] Art. 6 Rome Statute: "[...] intent to destroy, in whole or in part, a national, ethnic, racial or religious group, as such[...]"
[35] Killean, *supra* note 17, at 331.
[36] Mistura, *supra* note 27, at 210; Freeland, *supra* note 32, at 129.
[37] Killean, *supra* note 17, at 333.

УДК 006.3/.8

45.ЗАКОНОДАВСТВО У СФЕРІ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Запорожченко М.М.

Державний університет телекомунікацій
E-mail: zaporozhchenkomm@gmail.com

Legislтaion in the field of cyber protection of critical infrastructure facilities

Ensuring the proper functioning of a country's critical infrastructure is an extremely important process necessary to support its national interests. Modern critical infrastructure threats have become increasingly serious, because with the development of technologies and digitalization, many critical systems have become vulnerable to cyberattacks, hacker attacks and other forms of cybercrime. In addition, critical infrastructure is also prone to natural disasters, terrorist attacks and other emergencies. The report outlines the main requirements of Ukrainian and American legislation to ensure cyber protection of critical infrastructure facilities.

До об'єктів критичної інфраструктури відносяться системи та об'єкти, які мають важливе значення для функціонування держави, її економіки, національної безпеки й оборони. Порушення функціонування об'єктів критичної інфраструктури, зокрема, внаслідок кібератак чи інших загроз, може завдати шкоди життєво важливим національним інтересам. З метою організації більш ефективного забезпечення безпеки і стійкості критичної інфраструктури визначаються сектори критичної інфраструктури, до яких належать, зокрема, енергетика, транспорт, промисловість, фінансовий сектор, медична та соціальна допомога, водопостачання та водовідведення, інформаційні послуги тощо, і визначаються відповідальні за забезпечення безпеки секторальні органи.

Захист критичної інфраструктури України від кібератак та інших загроз є одним з пріоритетних завдань держави. У цьому напрямку працюють державні органи, відповідальні за кібербезпеку, а також приватні компанії, що забезпечують безпеку інформаційних систем критичної інфраструктури. У цілях забезпечення кібербезпеки критичної інфраструктури України використовуються різноманітні технічні та організаційні заходи, такі як кіберсимуляції, аудит безпеки, встановлення захисту від DDoS-атак, моніторинг мереж та систем на виявлення аномалій тощо. Базовим національним документом щодо захисту об'єктів критичної інфраструктури України є затверджені Постановою КМУ Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, які визначають перелік обов'язкових умов, яких повинні дотримуватися підприємства, установи та організації, які були віднесені до об'єктів критичної інфраструктури, серед яких вимоги до [1]:

- формування загальної політики інформаційної безпеки;

- управління доступом користувачів та адміністраторів до об’єктів захисту;
- ідентифікація та автентифікація користувачів та адміністраторів;
- реєстрація подій компонентами об’єкта критичної інформаційної інфраструктури та їх періодичний аудит;
- забезпечення мережевого захисту компонентів та інформаційних ресурсів об’єкта критичної інформаційної інфраструктури;
- забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів об’єкта критичної інформаційної інфраструктури;
- визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації;
- визначення умов використання програмного та апаратного забезпечення;
- визначення умов розміщення компонентів об’єкта критичної інформаційної інфраструктури;

У США кібербезпека та захист критичної інфраструктури від кібератак також добре розвинені і вважаються пріоритетом національної безпеки. Відповідно до американського законодавства критична інфраструктура розділена на 16 секторів: хімічна галузь; зв’язок; виробництво; шлюзи та греблі; військово-промисловий комплекс, екстрені служби, енергетика, фінансовий сектор, харчова промисловість та сільське господарство; державні установи; охорона здоров’я; ядерні реактори та ядерні відходи; транспортна інфраструктура; система водопостачання та водовідведення, а також комерційний сектор [2].

У США функціонують кілька державних установ, відповідальних за кіберзахист критичної інфраструктури, а також організації приватного сектора, які відіграють певну роль у захисті власних систем і мереж.

На федеральному рівні Міністерство внутрішньої безпеки (DHS, U.S. Department of Homeland Security) є головним агентством з координації захисту критичної інфраструктури від кіберзагроз. У рамках DHS Агентство США з кібербезпеки та безпеки інфраструктури (CISA, Cybersecurity & Infrastructure Security Agency) відповідає за надання ряду послуг з кібербезпеки, включаючи оцінку ризиків, реагування на інциденти та технічну допомогу власникам і операторам критичної інфраструктури. Інші федеральні агентства, які відіграють певну роль у кіберзахисті критичної інфраструктури, включають Міністерство оборони (DOD), Федеральне бюро розслідувань (FBI) і Агентство національної безпеки (NSA).

На додаток до цих федеральних агентств, організації приватного сектору, які володіють і керують критично важливою інфраструктурою, відповідають за захист власних систем і мереж від кіберзагроз. Багато з цих організацій створили власні програми кібербезпеки та мають партнерські відносини з урядовими установами для обміну інформацією та координації реагування на кіберінциденти.

Загалом, кіберзахист критичної інфраструктури в США є спільною відповідальністю між державними установами та організаціями приватного сектору, а співпраця та обмін інформацією є ключовими компонентами загального підходу до кібербезпеки.

У США є кілька основних законів щодо кіберзахисту критичної інфраструктури, зокрема:

- Закон щодо обміну інформацією про кібербезпеку (CISA, Cybersecurity Information Sharing Act): цей закон вимагає від федерального уряду ділитися інформацією про кіберзагрози з організаціями приватного сектору, які володіють і керують критичною інфраструктурою. Даний закон також заохочує суб'єктів приватного сектору ділитися інформацією з урядом.
- Федеральний закон про модернізацію інформаційної безпеки (FISMA, Federal Information Security Modernization Act): цей закон вимагає від федеральних відомств розробляти та впроваджувати програми кібербезпеки для захисту своїх інформаційних систем і мереж.
- Фреймворк кібербезпеки Національного інституту стандартів і технологій (NIST Cybersecurity Framework): даний фреймворк містить набір рекомендацій та найкращих практик для організацій критичної інфраструктури.
- Директива Президентської Політики PPD-21 «Захист та стійкість критичної інфраструктури»: ця директива визначає 16 критичних секторів інфраструктури, життєво важливих для функціонування США, і вимагає розробки планів захисту цих секторів від кіберзагроз, а її метою є зменшення факторів вразливостей, своєчасне виявлення та усунення загроз, мінімізація наслідків і вдосконалення заходів реагування та відновлення об'єктів критичної інфраструктури.
- Закон про звітування щодо інцидентів на об'єктах критичної інформаційної інфраструктури (Cyber Incident Reporting for Critical Infrastructure Act, CIRCIA): даний закон встановлює вимоги щодо сповіщення про інциденти, а саме: протягом 24 годин повідомити CISA про будь-які платежі, здійснені внаслідок програм-вимагачів; протягом 72 годин повідомити CISA про будь-який інцидент на об'єктах критичної інформаційної інфраструктури. При звітуванні повинна вказуватися інформація про типи та кількість систем, які піддалися впливу; тип інформації чи даних, які піддалися впливу; детальний опис атаки; дата і час інциденту; масштаб впливу на діяльність об'єкта; вразливості, які були проексплуатовані; тактики та техніки, які використовувалися; контактна інформація [3].

Загалом ці закони та фреймворки спрямовані на вдосконалення стану кібербезпеки критичної інфраструктури в США шляхом сприяння обміну інформацією, встановлення необов'язкових стандартів кібербезпеки та вимагання від федеральних агентств і організацій критичної інфраструктури розробляти та впроваджувати програми кібербезпеки.

Висновки

Було розглянуто та виділено основні вимоги українського та американського законодавства у сфері кіберзахисту об'єктів критичної

інфраструктури. Наразі функцію уповноваженого органу з питань захисту критичної інфраструктури України виконує Державна служба спеціального зв'язку та захисту інформації України. Базові вимоги до забезпечення кіберзахисту критичної інфраструктури визначаються Постановою КМУ «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури». У США відповідальними за координацію кіберзахисту критичної інфраструктури є Міністерство внутрішньої безпеки, Агентство з кібербезпеки та безпеки інфраструктури, а також певну роль відіграють інші урядові установи та приватний сектор. Вимоги до захисту базуються на президентських директивах, рекомендаціях CISA та NIST; законах, які регламентують порядок обміну інформацією, яка стосується кібербезпеки.

Література

18. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Каб. Міністрів України від 19 червня 2019 р. № 518: станом на 7 вересня 2022 р. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 07.03.2023)
19. Critical Infrastructure Security and Resilience. *Cybersecurity & Infrastructure Security Agency*. URL: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience (дата звернення: 07.03.2023)
20. Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). *Cybersecurity & Infrastructure Security Agency*.
URL: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia (дата звернення: 07.03.2023)

УДК 351.71: 65.012.8 (73)

46.БЕЗПЕЧНЕ ВИКОРИСТАННЯ ЗАХИЩЕНОЇ ІНФОРМАЦІЇ ПРО КРИТИЧНУ ІНФРАСТРУКТУРУ: ДОСВІД США

Легомінова С.В., Мужанова Т.М.
Навчально-науковий інститут захисту інформації
Державного університету телекомунікацій, м. Київ, Україна
E:mail: muzanovat@gmail.com

Secure handling protected critical infrastructure information: the US experience

The paper examines the main principles of handling protected critical infrastructure information (PCII), defined in the US regulatory documents. It has been determined that following requirements are met to ensure proper use of PCII in US practice: responsibilities and personal accountability; background checks on persons with access to PCII; following procedures for safe handling and storage, reproduction, transmission and disposal of PCII; protection of automated information systems that contain PCII. The importance of training personnel in the field of PCII protection, backup and preventing unauthorized access to PCII is also noted.

Критична інфраструктура завжди була основною мішенню для кіберзлочинців і зловмисників, яких спонсорують інші держави, з початком військового конфлікту в Україні ситуація ще погіршилася. Звіт Bloomberg за 2022 рік показав, що на початку російського вторгнення 21 американська компанія газової галузі постраждала від масштабних хакерських атак. ФБР також повідомило, що російські хакери сканували системи енергетичних компаній та іншу критичну інфраструктуру США [1]. Майже 80% топ-менеджерів з інформаційної безпеки CISO вважають, що зараз світ перебуває у «постійному стані» кібервійни [2].

З огляду на те, що безпека критичної інфраструктури з кожним роком набуває все більш важливого значення у контексті забезпечення національної безпеки, Департамент внутрішньої безпеки (Department of Homeland Security, DHS) та Агенство кібербезпеки й безпеки інфраструктури (Cybersecurity and Infrastructure Security Agency, CISA) США активно займаються вдосконаленням методів захисту критичної інфраструктури й інформації, що стосується її функціонування та безпеки.

Відповідно до Акту про інформацію про критичну інфраструктуру (Critical Infrastructure Information Act) [3] під інформацією про критичну інфраструктуру (Critical Infrastructure Information, CII) розуміють інформацію, яка зазвичай не є загальнодоступною та пов’язана з безпекою критичної інфраструктури або захищених систем, зокрема щодо:

– фактичного, потенційного або загрозливого втручання, атаки, компрометації або виведення з ладу критичної інфраструктури чи захищених систем шляхом фізичної або комп’ютерної атаки чи іншої подібної поведінки (включно з неправильним використанням чи несанкціонованим доступом до всіх типів систем зв’язку та передачі даних), яка порушує федеральні, державні, чи місцеве закони, загрожує громадському здоров’ю чи безпеці тощо;

– здатності будь-якої критичної інфраструктури або захищеної системи протистояти такому втручанню, компрометації або виведенню з ладу, включаючи будь-яку заплановану або минулу оцінку, прогноз або оцінку вразливості критичної інфраструктури або захищеної системи, включаючи тестування безпеки, оцінку ризиків, планування управління ризиками або аудит ризиків;

– будь-якої запланованої чи минулої операційної проблеми чи рішення стосовно критичної інфраструктури чи захищених систем, включаючи ремонт, відновлення, реконструкцію, страхування чи забезпечення безперервності, якщо це пов’язано з таким втручанням, компрометацією чи непрацездатністю.

У подальших нормативних документах використовують термін «захищена інформація про критичну інфраструктуру» (Protected Critical Infrastructure Information, PCII).

В оновлених Процедурах поводження із захищеною інформацією про критичну інфраструктуру від 2022 року [4] визначено низку вимог щодо належного користування PCII.

Відповідальність та зобов'язання. Усі авторизовані користувачі та розпорядники PCII несуть персональну відповідальність за обробку і зберігання такої інформації відповідно до вимог, а також зобов'язані вживати запобіжних заходів для уникнення доступу до PCII неуповноважених осіб.

Перевірки осіб, які мають доступ до PCII. Усі особи, яким потрібен доступ до PCII, підлягають перевірці з боку уповноважених органів (зокрема, CISA), щоб переконатися, що ці особи не становлять загрози національній безпеці.

Використання та зберігання. Якщо носії PCII перебувають у фізичному розпорядженні уповноважених користувачів, то вони мають вжити належних заходів, щоб мінімізувати ризик доступу до PCII неавторизованих осіб. В іншому випадку PCII має зберігатися в безпечному середовищі.

Розмноження інформації. Згідно з вимогами документи або інші матеріали, що містять PCII, мають бути відтворені в необхідному обсязі та відповідно до потреби у виконанні службових обов'язків за умови, що відтворені документи чи матеріали позначені й захищені таким же чином, як оригінали.

Знищення інформації. Документи й матеріали, що містять PCII, доцільно утилізувати будь-яким способом, який запобігає їх несанкціонованому відновленню та вилученню, наприклад подрібненням або спалюванням.

Передавання інформації. PCII має передаватися лише безпечними засобами доставки відповідно до встановлених керівником вимог і законодавчих норм.

Захист автоматизованих інформаційних систем. Для автоматизованих інформаційних систем, які містять PCII, мають бути встановлені вимоги безпеки, спрямовані на захист інформації в максимально можливому обсязі та згідно із законодавством.

У Посібнику щодо процедур програми захисту інформації про критичну інфраструктуру (Protected Critical Infrastructure Information Program Procedures Manual) [5] наголошено, що основними принципами захисту PCII є, зокрема:

– надання доступу до PCII тільки авторизованих користувачів, які пройшли навчання щодо належного використання PCII та необхідні перевірки;

– дотримання встановлених процедур реєстрації доступу, належного користування та повернення PCII;

– використання засобів фізичного контролю доступу авторизованих осіб до місць фізичного зберігання PCII;

– зберігання PCII в контейнерах або шафах на замку, які розташовані в місцях обмеженого доступу;

– надання доступу до копіювальних апаратів, принтерів шредерів і у місці зберігання лише авторизованим користувачам;

– усунення будь-яких слідів використання та залишків інформації на копіювальних засобах після розмноження матеріалів з PCII;

– налаштування інформаційних систем таким чином, щоб лише авторизовані користувачі мали доступ до електронних баз даних PCII;

– вбудовування засобів запобігання несанкціонованому доступу в електронні бази даних, що зберігають PCII;
– створення резервних копій для електронних баз даних, що зберігають PCII;
– обмін PCII із використанням безпечних і перевірених методів передавання даних.

Отже, як показало дослідження нормативних документів США, основними засадами безпечного користування PCII є: встановлення відповідальності та зобов'язань персоналу щодо захисту PCII, проведення перевірок осіб, які мають доступ до PCII, дотримання процедур безпечного використання та зберігання, розмноження, передавання та знищення PC II, забезпечення захисту автоматизованих інформаційних систем, які містять PCII. Також відзначено велике значення навчання персоналу у сфері захисту PCII, резервного копіювання і запобігання несанкціонованому доступу до PCII.

Література

1. Giulia Moschetta, Filipe Beato, Akshay Joshi. Cybersecurity in this era of polycrisis. Feb 24, 2023. URL: https://www.weforum.org/agenda/2023/02/cybersecurity-in-an-era-of-polycrisis/
2. Stu Sjouwerman. Five Cybersecurity Predictions For 2023. Jan 24, 2023. URL: https://www.forbes.com/sites/forbestechcouncil/2023/01/24/five-cybersecurity-predictions-for-2023/?sh=2666d78df9b7
3. Critical Infrastructure Information Act 2002. URL: https://www.cisa.gov/sites/default/files/2023-01/critical-infrastructure-information-act-of-2002-012014.pdf
4. Protected Critical Infrastructure Information Program Procedures Manual 2009. URL: https://www.cisa.gov/sites/default/files/publications/pcii-program-procedures-manual_508.pdf
5. Procedures for Handling Critical Infrastructure Information. Final Rule - December 2022. URL: https://www.cisa.gov/sites/default/files/2023-01/pcii-program-final-rule-technical-amendments-122022.pdf

УДК 681.7.068.4

47.ОСОБЛИВОСТІ ДИНАМІЧНОГО РОЗШИРЕННЯ СПЕКТРА ОПТИЧНОГО ПЕРЕДАВАЧА

Омецинська Н.В., Кисельов В. Б., Гуйда О. Г.
Таврійський національний університет імені В.І. Вернадського
E-mail ometsynska.nataliia@tnu.edu.ua, kyselov.volodymyr@tnu.edu.ua,, huida.oleksandr@tnu.edu.ua

Features of the dynamic spectrum expansion of the optical transmitter

With the constant increase in the speed of signal transmission over fiber optic communication lines (FOCL), the problem of building an optimal linear path using the limit capabilities of the transmission system is becoming more and more urgent. The use of optical amplifiers eliminates the limitation of the length of the section between the transmitter and the receiver or repeater caused by the attenuation of the optical power. Chromatic dispersion, along with nonlinear effects and polarization mode dispersion, remains the reason for the limitation of the length of the regeneration section of the VOLZ. Under certain conditions, the chromatic dispersion accumulated along the single-mode optical fiber (SFO) can be compensated by the use of passive dispersion compensators.

Розширення імпульсу через хроматичну дисперсію зменшується за зменшення спектральної ширини $\Delta\lambda$ оптичного джерела. Але якщо навіть можна було б використати ідеальне джерело монохроматичного випромінення з нульовою шириною спектральної лінії, після амплітудної модуляції несівної довжини хвилі інформаційним сигналом виникло б спектральне розширення $\Delta\lambda_м$ модульованого сигналу, тим більше за величиною, чим більша швидкість модуляції

$$\Delta\lambda_м = \frac{rB\lambda^2}{2\pi c}, \text{ нм} \qquad (1)$$

де c – швидкість світла у вакуумі;

$B = 1/(2T_0)$ – швидкість модулюючої бітової послідовності;

r – параметр, що визначається формою модулюючих імпульсів: для Гаусового імпульсу $r=\sqrt{2}$, а для імпульсу прямокутної форми у відповідності до [1] $r=\sqrt{3}$ – це відповідає еквівалентному Гаусовому імпульсу із середньоквадратичною тривалістю імпульсу прямокутної форми, що дорівнює значенню $2T_0/\sqrt{12}$ (для Гаусового імпульсу середньоквадратична тривалість σ_t має значення $2T_0/\sqrt{8}$, де T_0 – його напівширина на рівні $1/e$ вниз за інтенсивністю; величина σ_t пов'язана із середньоквадратичною спектральною шириною σ_ω імпульсу співвідношенням $\sigma_t \times \sigma_\omega = 1/2$).

Тому за високих швидкостей передавання застосовують напівпровідникові лазери на одній поздовжній моді (SML-лазери), що мають вузьку ширину спектральної лінії, $\Delta\lambda << \Delta\lambda_м$ в формулі

$$W = \sqrt{\Delta\lambda^2 + \Delta\lambda_м^2}\ . \qquad (2)$$

Для таких лазерів в нормативній документації вказують максимально допустиму ширину спектра на рівні 20 дБ вниз від пікового значення потужності. Ця величина в 6,07 разів більша від середньоквадратичної ширини $\Delta\lambda$ спектра лазера в Гаусовій апроксимації [1]. Лазери на багатьох поздовжніх модах (MML-лазери) та світлодіоди (LED) застосовуються за невисоких бітових швидкостей, переважно в діапазоні довжин хвиль з околу 1310 нм; вони можуть мати велике середньоквадратичне значення $\Delta\lambda$ ширини спектра ($\Delta\lambda >> \Delta\lambda_м$), величина якого безпосередньо вказується в нормативній документації [4].

Ще однією причиною спектрального розширення модульованого сигналу є динамічне розширення його спектра в передавачі, що полягає в зміненні в часі миттєвої частоти передавача при модуляції. Це явище носить назву чірпу (chirp), а сам сигнал – чірпованим.

За використання лазерів з внутрішньою модуляцією, коли імпульсна модуляція застосовується безпосередньо до струму накачування лазера, може відбутися інтенсивне динамічне розширення спектра генерованого імпульсу, що супроводжується зміщенням в цілому короткохвильових (високочастотних) спектральних складових вздовж імпульсу до його переднього фронту, а довгохвильових (низькочастотних) складових – до заднього фронту. При цьому генеровані імпульси називаються імпульсами з додатним чірпом.

Через значне динамічне розширення спектра лазери з внутрішньою модуляцією використовуються за невисоких швидкостей передавання (до 2,5 Гбіт/с). За більш високих бітових швидкостей застосовується зовнішня модуляція випромінення самого лазера. Для лазерів із зовнішньою модуляцією динамічне спектральне розширення модульованого сигналу значно менше за величиною, а знак та величина чірпу можуть бути регульованими. Зовнішні модулятори підвищують складність і вартість системи, вносять додаткові оптичні втрати і ускладнюють керування станом поляризації випромінення. Але вдосконалення процесу виробництва та ріст запиту на передавальні модулі, що об'єднують вузькосмуговий лазер із модулятором для зовнішньої модуляції, змінюють ситуацію на краще.

Кількісно міра чирпування модульованого сигналу описується за допомогою альфа-параметра чірпу передавача, який визначається за формулою [6, 7]

$$\alpha = \frac{\frac{d\varphi}{dt}}{\frac{1}{2P}\frac{dP}{dt}}, \text{ рад}, \qquad (3)$$

де φ – фаза оптичного імпульсу, що змінюється вздовж імпульсу;

$\frac{d\varphi}{dt}$ – відхилення миттєвої частоти вздовж імпульсу від його середньої центральної частоти ω_0 , рад/с;

P – миттєва потужність вздовж імпульсу, Вт.

Відповідно до (3) α-параметр чірпу дорівнює відношенню приросту фази імпульсу до нормованого приросту потужності вздовж імпульсу:

$$\alpha = \frac{\Delta\varphi}{\Delta P / 2P}. \qquad (4)$$

У випадку зовнішньої модуляції лазерного випромінення можливі значення α-параметра чірпу належать діапазону від –1 до 1 радіана [7]. Для лазерів з внутрішньою модуляцією α-параметр може досягати набагато більших додатних значень.

На рис. 1 приведено заміряні вздовж імпульсу розподіли миттєвої потужності P та відхилення миттєвої частоти в Гц від центральної частоти імпульсу, $\frac{1}{2\pi}\frac{d\varphi}{dt}$, [6]. Аналіз цих залежностей з урахуванням (3) показує, що величина α-параметра чірпу може змінюватись вздовж імпульсу.

За протилежних знаків α-параметра чірпу передавача та питомої хроматичної дисперсії ООВ, по якому передається сигнал, можна використати взаємодію цих ефектів для збільшення довжини лінійного тракту між передавачем та приймачем.

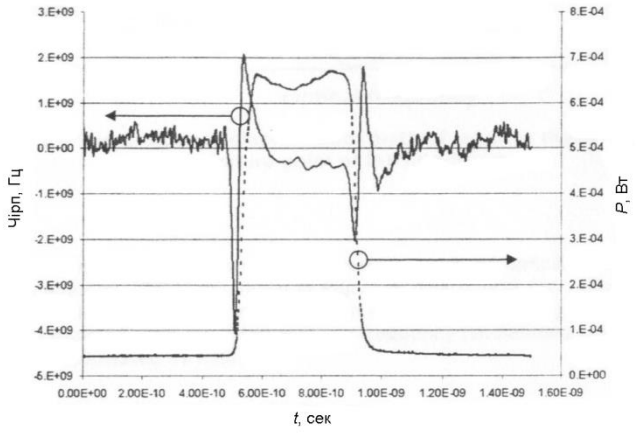


Рис. 1 – Заміряні розподіли миттєвої потужності P та відхилення миттєвої частоти від центральної частоти імпульсу (чірп), в залежності від часу

Висновки

Урахуванням особливостей динамічного розширення в оптичному передавачі спектра модульованого сигналу можна добитися використання граничних можливостей системи передавання для досягнення максимальної

довжини обмеженої за хроматичною дисперсією регенераційної дільниці ВОЛЗ без застосування пасивних пристроїв компенсації дисперсії.

Література

1. IEC/TR 61282-5, Fibre optic communication system – Part 5: Accomodation and compensation of dispersion, 2002.
2. Marcuse D. Pulse distortion in single-mode fibers. 3: Chirped pulses. Applied Optics, 12 October 1981 / Vol.20, No.20.
3. ITU-T Recommendation G.959.1 Optical transport network physical layer interfaces, 2000.
4. Yonggyoo K., Hanlim L., Jaehoon L., Jaeho H., Oh T.W., Jichai J. Chirp characteristics of 10-Gb/s electroabsorbtion modulator integrated DFB lasers, IEEE Journal of Quantum Electronics, Vol.36, No.8, August 2000.
5. IEC 61280-2, Fibre optic communication subsystem test procedures – Part 10: Digital systems – Time-resolved chirp alpha-factor measurement of laser transmitters, 2003.
6. ITU-T Recommendation G.691 Optical interfaces for single channel STM-64, STM-256 systems and other SDH systems with optical amplifiers, 2000.
7. Anderson D., Lisak M. Propagation characteristics of frequency-chirped super-Gaussian optical pulses. Opt.lett., 11, 569 (1986).
8. ITU-T Recommendation G.957 Optical interfaces for equipments and systems relations to the synchronous digital hierarchy.

УДК 004.056.5

48.ПРАВОВІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ ОБЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Щавінський Ю.В., Пальчинська В.Б.
Навчально-науковий захисту інформації
Державного університету телекомунікацій, Київ, Україна
2 Національний університет харчових технологій, Київ, Україна
E-mail: yushchavinsky@ukr.net, val.palchynska@gmail.com

Legal mechanisms for ensuring cyber protection of objects of critical information infrastructure of Ukraine in conditions of hybrid war

The report analyzes regulatory and legal support in the field of cyber security of critical information infrastructure. The importance of information infrastructure in the national security system is determined. It is noted that today in Ukraine, in the context of a hybrid war against Ukraine, it is important to ensure effective protection of the uninterrupted functioning of critical information

infrastructure facilities. It is substantiated that the problem of ensuring cyber security requires improvement of legal, organizational and technical mechanisms. It was determined that one of the ways to solve the problems is to improve regulatory documents and take into account the experience of the countries of the European Union. The responsibility of owners and operators of critical infrastructure objects for the state of protection of critical infrastructure objects and the completion of the formation of their list also needs to be legislated.

Інформаційна складова є важливим елементом критичної інфраструктури будь-якої країни та важливою складовою національної безпеки держави. В сучасних умовах гібридної агресії з боку Російської Федерації є актуальним захист об'єктів критичної інфраструктури, від яких залежить стан забезпечення життєво важливих інтересів людини, суспільства і країни, Тому перед нашою державою виникла нагальна потреба у забезпеченні належного захисту об'єктів критичної інфраструктури.

Основою для організаційних та технічних заходів забезпечення безпеки критичної інфраструктури є нормативно-правові акти, їх розроблення, удосконалення та упорядкування у відповідності з міжнародними договорами та угодами.

Кожна країна при формуванні нормативно-правової бази в галузі захисту критичної інфраструктури враховує географічні та історичні особливості регіону, традиції та політичні і суспільні переконання. При цьому, перелік об'єктів критичної інфраструктури теж має свої особливості. Наприклад, країни Євросоюзу розглядають «Європейську критичну інфраструктуру» як об'єкт критичної інфраструктури, розташований в державах-членах, порушення функціонування або знищення якого буде мати значний вплив, принаймні, на дві держави-члени Євросоюзу [1].

Великобританія до об'єктів критичної інфраструктури відносить активи, послуги та системи, що підтримують економічне, політичне й соціальне життя Великобританії, втрата яких може: 1) викликати масштабну загибель людей; 2) відчутно вплинути на національну економіку; 3) призвести до інших серйозних соціальних наслідків; 4) перетворитись на одне з невідкладних завдань національного уряду [2].

Важливим компонентом критичної інфраструктури є її інформаційна складова – критична інформаційна інфраструктура, Головні причини критичності інформаційної складової інфраструктури випливають зі стрімкого поширення інформаційних технологій у всіх сферах людської діяльності, що призводить до залежності від них громадян, суспільства й держави, а також до посилення вразливостей і потенційних загроз різного характеру.

Але у законодавчих документах більшості країн визначення критичної інформаційної інфраструктури окремо не розглядається, не зважаючи на те, що сьогодні це визначення є центральним компонентом забезпечення безпеки інфраструктури держави. Відсутність поняття «критична інформаційна інфраструктура» у законодавстві багатьох держав пояснюється тим, що інформаційна складова входить до обсягу поняття інфраструктури взагалі та розуміється як «інформаційні системи» (програмне забезпечення, апаратні

засоби й дані) та послуги, які підтримують один чи кілька найважливіших об’єктів інфраструктури, порушення роботи або відімкнення яких завдає серйозної шкоди функціонуванню залежної критичної інфраструктури [3].

Вітчизняне законодавство про критичну інфраструктуру та її захист складають Конституція України, Закон України «Про критичну інфраструктуру» [4], інші закони України, міжнародні договори України, згода на обов’язковість яких надана Верховною Радою України, інші нормативно-правові акти, прийняті на виконання законів для забезпечення безпеки об’єктів критичної інфраструктури.

Об’єктами критичної інфраструктури згідно Закону [4] є підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв.

Аналізуючи Закон України «Про критичну інфраструктуру», який визначає правові та організаційні засади створення та функціювання національної системи захисту критичної інфраструктури і є складовою законодавства у сфері національної безпеки, можна зробити висновок, що, не зважаючи на важливість у сучасних війнах і конфліктах інструментів інформаційної складової, у Законі не приділено достатньої уваги законодавчому закріпленню визначення об’єктів інформаційної інфраструктури. Інформаційна складова розглядається тільки як «інформаційні послуги» та «електронні комунікації», які належать до життєво важливих функцій та/або послуг, порушення яких призводить до негативних наслідків для національної безпеки України.

Існують також деякі неузгодження і в інших нормативно-правових актах. За результатами досліджень [5-9] встановлено, що у Законі України «Про основні засади забезпечення кібербезпеки України» [10] є певні недоліки. Зокрема, у ньому не визначені підстави віднесення організацій (незалежно від форми власності) до суб’єктів критичної інформаційної інфраструктури і, як наслідок, інформаційні системи, інформаційно-телекомунікаційні мережі та автоматизовані системи управління, які належать цим організаціям також не зазначені, виходячи із Порядку формування переліку об’єктів критичної інформаційної інфраструктури, який затверджений Постановою Кабінету Міністрів України від 09 жовтня 2020 р. № 943 «Деякі питання об’єктів критичної інформаційної інфраструктури». Така невизначеність уповільнює ідентифікацію критичних інформаційних систем і знижує рівень ефективності забезпечення безпеки.

Події останніх років в Україні та світі, а також аналіз сучасних кіберзагроз свідчать про нагальну необхідність забезпечення надійного кіберзахисту

інформаційних, комунікаційних систем та систем управління технологічними процесами в секторі енергетики, інформаційних технологій, хімічної і вугільної промисловості та інші. При цьому, основними проблемними питаннями надійного забезпечення кіберзахисту об'єктів інформаційної інфраструктури є незавершеність переліку об'єктів критичної інфраструктури, який повинен бути основою при подальшому формуванні переліку об'єктів критичної інформаційної інфраструктури; низький рівень співпраці з приватним сектором та небажання власників і операторів об'єктів критичної інфраструктури брати на себе додаткові зобов'язання у сфері кіберзахисту.

Як зазначають дослідники [11], не зважаючи на значну кількість відпрацьованих питань нормативно-правового забезпечення кіберзахисту об'єктів критичної інфраструктури, зазначена тематика залишається актуальною, містить велику кількість не вирішених питань і потребує наукових досліджень.

Висновки

Таким чином, існуючі організаційно-правові засади кіберзахисту об'єктів критичної інфраструктури держави потребують негайного удосконалення. Одним із шляхів вирішення проблемних питань удосконалення системи кіберзахисту об'єктів критичної інформаційної інфраструктури є розроблення методик модернізації критичної інформаційної інфраструктури для кожної організації, інформаційної структури, які є об'єктами критичної інформаційної інфраструктури. Сучасний стан співпраці з приватним сектором потребує законодавчого закріплення відповідальності власників і операторів об'єктів критичної інфраструктури за стан захисту.

Література

1. COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. [Електронний ресурс] – Режим доступу до ресурсу: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF.
2. Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards [Електронний ресурс] – Режим доступу до ресурсу: https://www.gov.uk/government/uploads/system/uploads/attachment_
3. data/file/62504/strategic-framework.pdf.
4. Об'єкти критичної інфраструктури та об'єкти критичної інформаційної інфраструктури в європейських країнах. Інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром на запит Апарату Верховної Ради України. [Електронний ресурс] – Режим доступу до ресурсу: https://infocenter.rada.gov.ua/uploads/documents/29297.pdf.
5. Про критичну інфраструктуру. Закон України від 16.11.2021р. - № 1882-IX (редакція 05.12.2022р.). [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1882-IX#Text.

6. Бакалінська О. Правове забезпечення кібербезпеки в Україні. / Бакалінська О., Бакалинський О. // Підприємництво, господарство і право, № 9(2019), с. 100–108. doi:10.32849/2663-5313/2019.9.17
7. Bakalynskyi, Oleksandr & Pakholchenko, Dmytro & Тетяна, Сапожнік. (2021). Аналіз забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури. doi:10.13140/RG.2.2.24986.93122.
8. Малашко, О. Є. Адміністративно-правові засади забезпечення інформаційної безпеки в Україні у контексті європейської інтеграції(Автореферат кандидатської дисертації); Львівський університет бізнесу та права. Львів -2020.
9. Малашко, О. Є. Пріоритетні напрями удосконалення інформаційної безпеки України. / Малашко, О. Є., Скриньковський, Р. М. // Інтернаука. Серія: Юридичні науки, № 6(28). Львів -2020, с. 13–19.
10. М. Ковалів. Правове забезпечення кібербезпеки критичної інформаційної інфраструктури України. / М. Ковалів, Р. Скриньковський, Ю. Назар, С. Єсімов І. Красницький Х. Кайдрович, та інш. // Traektoriâ Nauki= Path of Science. 2021. Vol. 7.No 4. Зз. 2011-2018. https://pathofscience.org/index.php/ps/article/view/888/865
11. Про основні засади забезпечення кібербезпеки України. Верховна Рада України, Закон України від 05.10.2017 р. [Електронний ресурс]. Режим доступу: http://zakon2.rada.gov.ua/laws/show/2163-19.
12. Ткачук Н.А. Організаційно-правові засади формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. //Інформація і право, № 1(24)/2018 с. 133-138. [Електронний ресурс]. Режим доступу: http://ippi.org.ua/sites/default/files/16_4.pdf.

РОЗДІЛ 7

МОДЕЛЮВАННЯ ТА СИМУЛЯЦІЯ СТИХІЙНИХ ЛИХ, НАДЗВИЧАЙНИХ СИТУАЦІЙ І РЕАГУВАННЯ НА НИХ.

UDC 351.861

49.MATHEMATICAL MODELS FOR DETECTING THE HAZARD OF CRITICAL INFRASTRUCTURE OBJECTS BY UNMANNED AIRCRAFT

Miasoyedova[1] A., Divizinyuk[2] M., Shevchenko[3] R.
1 Cherkasy Institute of Fire Safety named after Chernobyl Heroes of the National University of Civil Defense of Ukraine
2 Institute of Environmental Geochemistry of the National Academy of Sciences of Ukraine
3 National University of Civil Defense of Ukraine
E-mail:shevchenko605@i.ua

Математичні моделі виявлення небезпеки об'єктів критичної інфраструктури безпілотними апартанами

Робота присвячена вирішенню актуального наукового завдання в галузі цивільного захисту, а саме формуванню експериментальних методів дослідження для перевірки надійності математичних моделей попередження надзвичайних ситуацій терористичного характеру на об'єктах критичного рівня. інфраструктури України, які захищаються, шляхом своєчасного виявлення та ідентифікації малих безпілотних літальних апаратів активними оптико-електронними засобами [1].

Based on the analysis, it was established that one of the trends in the development of terrorist scenarios at protected critical infrastructure facilities is the use of various small manned and unmanned aerial vehicles to carry out terrorist acts. This work is a continuation of the cycle of previous works on the development of a structural and logical management model of an organizational and technical nature that ensures the safety of the protected object in the event of the appearance of small air targets. The developed method of experimental research to verify the reliability of mathematical models for detecting signals reflected from an emergency situation of a terrorist nature at a protected critical infrastructure object of Ukraine allowed to determine the following - the results of all field experiments performed using a laboratory installation, and theoretically calculated values of expected activities detection of targets as part of numerous experiments are located within the confidence intervals calculated according to the Student's criterion with a reliability of 0.99, which indicates a good convergence of experimental results and theoretical calculations. This, in turn, confirms the reliability of the mathematical model for detecting signals reflected from small unmanned aerial vehicles using active optical systems that use the phenomena of light absorption and scattering in optically transparent media and the mathematical model for detecting and identifying small unmanned aerial vehicles using passive optoelectronic systems.

Literature

1. Miasoiedova A., Divizinyuk M., Shevchenko R. To the issue of detection of small unmanned aerial vehicles using active optical systems // The 8th International scientific and practical conference “Integration of scientific and modern ideas into practice” Stockholm, Sweden. International Science Group. 2022. 768-770.

UDC 351.861

50.INFORMATION METHODS OF PREVENTING EMERGENCY SITUATIONS DUE TO AN EXPLOSION IN TUNNELS

Myroshnychenko A., Shevchenko R.

National University of Civil Defense of Ukraine, Kharkiv, Ukraine
E-mail:shevchenko605@i.ua

The physical field and conditions for the formation of a mathematical apparatus for the prevention of emergency situations of a terrorist nature in railway tunnels have been determined. It has been proven that the formation of individual elements of the mathematical apparatus, namely the mathematical model for the prevention of emergency situations of a terrorist nature in railway tunnels, should take place with the aim of compiling a system of equations for the sequential solution of interconnected separate problems, which collectively allow determining the structural and strength parameters of additional means collective protection of pyrotechnicians. It was determined that the formation of the methodology for the prevention of emergency situations of a terrorist nature in railway tunnels is based on the appropriate control algorithm, which takes into account the multi-level nature of liquidation works and the procedure for calculating the parameters of means of extinguishing excess impulse and determining the minimum possible distance for carrying out explosive works, taking into account the danger of damage to pyrotechnicians by fragments and elements railway tunnel constructions.

The need to eliminate the identified limitations of the mathematical apparatus has been established. In particular, it is necessary to propose options for standards for evaluating operational actions of pyrotechnicians in summer and winter and in the presence of additional complicating factors of danger, such as the possibility of chemical, radiation, or bacteriological damage.

It was determined that the obtained results allow further development of a number of practical recommendations for improving the existing standard operational procedures for the localization of emergency situations of a terrorist nature in railway transport tunnels in order to prevent them from growing to a higher level of danger.

The development of this study will allow further development of a number of practical recommendations for improving current standard operational procedures in the case of using an additional protection device and the methodology of its application

in order to ensure a reduction in the time of work on the localization of emergency situations of a terrorist nature in railway transport tunnels, preventing them from growing to a higher level danger, and ensuring a sufficiently high level of individual and collective protection of the personnel of the State Emergency Service and civilians. However, certain difficulties are expected at the stage of certification of the developed equipment and its wide implementation in the direct activity of pyrotechnic units.

УДК 614.84

51.ПРОБЛЕМИ КЕРУВАННЯ СТВОРЕННЯМ ТА ЗАКУПІВЛЮ ПРОТИПОЖЕЖНОЇ ТЕХНІКИ

Алдошин О.О. [1], Калиновський А.Я. [1]

1 Національний університет цивільної захисту України

E-mail: ugzu.iart @gmail.com

Problems of managing the creation and purchase of fire-fighting equipment

The main task of providing fire-fighting equipment to operational and rescue units of the Civil Protection Service at the modern level is to create and develop scientific foundations for making prospective decisions regarding the management of the design and purchase of fire-fighting equipment, the organization of a more advanced information base for planning the development of the supply system, changes in its structure, adjustment of activities taking into account the dynamics of the fire situation in the state and in specific regions in particular.

In modern conditions, the organization of their mandatory certification at manufacturing plants could be the only means of control on the part of Civil Protection Service over the production of safe and high-quality fire engines. At the moment, the customer's representatives are not able to ensure effective control over the quality of the produced products.

Основне завдання забезпечення протипожежною технікою (ПТ) підрозділів оперативно-рятувальної служби цивільного захисту (ОРС ЦЗ) на сучасному рівні полягає у створенні та розвитку наукових засад для прийняття перспективних рішень щодо управління проектуванням та закупівлею протипожежної техніки, організації більш досконалої інформаційної бази для планування розвитку самої системи постачання, зміни її структури, коригування напрямів діяльності з урахуванням динаміки пожежної обстановки у державі та у конкретних регіонах зокрема.

У проблемі постачання протипожежної техніки, перш за все, виділяються два її основні аспекти: динамічний і територіальний.

Динамічний аспект виявляється у тому, що забезпечення підрозділів ОРС ЦЗ протипожежною технікою не є засобом впливу на пожежну обстановку, а слідує за її змінами.

Екстенсивне нарощування чисельності протипожежної техніки служб пожежогасіння, яким воно було протягом останнього часу, давало все менш відчутний ефект, що виражався у збільшенні кількості пожеж у пропорції значно менших витрат. Саме тому зараз на порядок денний гостро постало питання докорінної зміни якості та методів гасіння пожеж, інтенсифікації діяльності співробітників відповідних служб ОРС ЦЗ, ефективного використання штатної пожежної техніки.

Виходячи з порівняльного аналізу динаміки пожежної обстановки в державі та забезпеченості технікою основних служб ОРС ЦЗ, в цілому розвиток системи постачання ПТ ще не можна охарактеризувати як таку, що має виражену цілеспрямованість, прагнення до оптимальності в штатному забезпеченні, що дозволяє створити випереджальний вплив на пожежну ситуацію.

Пояснення та оцінка динаміки забезпеченості протипожежною технікою підрозділів ОРС ЦЗ повинні припускати виявлення основних факторів, які безпосередньо чи опосередковано впливають на кількісні та, що особливо важливо, на якісні характеристики ПТ.

Домінантою серед комплексів факторів, що детермінують розвиток ПТ, повинні бути, перш за все, негативні явища соціально-економічного характеру, а також недотримання техніки безпеки та технологічних процесів на виробництві. Саме вони створюють умови для формування пожежної ситуації у конкретному регіоні. Від інтенсивності динаміки пожежної обстановки та її зміни залежить реальна технічна політика в системі ДСНС України .

Несвоєчасні оцінки негативного впливу зазначених явищ та прийняття неправильних попереджувальних управлінських рішень у технічній політиці ОРС ЦЗ відіграли негативну роль з погляду впливу їх на пожежну обстановку.

Багато значних особливостей реального розвитку пожежної обстановки внаслідок слабкої організації аналітичної роботи недостатньо враховувалися під час вироблення управлінських рішень, щодо стратегії та пріоритетних напрямів боротьби з пожежами, під час підготовки та прийняття рішень на проектування і закупівлю протипожежної техніки.

Наявність суттєвих відмінностей в інтенсивності, динаміці та структурі пожежної обстановки в регіонах зумовлює необхідність диференційованого підходу до визначення потреби у ПТ територіальних підрозділів ОРС ЦЗ. Її основу мають становити результати аналізу регіональних тенденцій соціальних та економічних процесів, які в кінцевому підсумку визначають реально існуючі відмінності у стані пожежної обстановки.

Реалізація диференційованого підходу до визначення потреби у протипожежній техніці має базуватися на результатах типології регіонів, що враховує тенденції соціальних та економічних процесів та їх зв’язку із станом пожежної обстановки.

Складність сучасних соціально-політичних та економічних процесів у державі та різноманіття їхніх взаємозв’язків із пожежною обстановкою визначають практичну потребу у використанні принципів системного підходу,

сучасних методів математичного моделювання при визначенні потреби у ПТ ОРС ЦЗ ДСНС України.

Територіальний аспект проблеми забезпечення протипожежною технікою пов’язані з тим, що ресурси ПТ різних підрозділів ОРС ЦЗ нерівномірно розподілені територією держави, при цьому переважно технічний потенціал не відповідає реальній пожежній обстановці у тому чи іншому регіоні. Це актуалізує вирішення завдання оптимального забезпечення протипожежною технікою у регіональному аспекті.

Висновки

В даний час розробка та постановка на виробництво транспортних засобів модернізованої або нової конструкції є справою виробника. Держава не виділяє коштів для оновлення продукції (розробки та виготовлення перспективних моделей).

Відповідно за відсутності фінансування підприємства-виробники пожежних автомобілів не зацікавлені у проведенні сертифікаційних випробувань пожежних машин та не проводять їх, зазначаючи що сертифікати ISO 9001 та ISO 14001 не є обов’язковими документами, які вимагаються від виробників спеціальних та спеціалізованих транспортних засобів. Сертифікати ISO 9001 - це система добровільної сертифікації і вона носить рекомендаційний характер.

На сьогоднішній день системи управління якістю, розроблені відповідно до вимог стандарту ISO 9001, є найкращим загальновизнаним у світі запобіжним механізмом, який забезпечує якість продукції на всіх етапах її виробничого (життєвого) циклу і сприяє підвищенню результативності роботи підприємств. Стандарт ISO 9001 застосовується підприємствами й організаціями більш ніж 190 країн світу і користується особливою популярністю на території Європейського Союзу, США, Канади, Японії, тобто в країнах, які є активними учасниками міжнародної торгівлі. Як свідчить міжнародний досвід, впровадження на підприємстві системи управління якістю, розробленої на основі стандарту ISO 9001, сприяє спрощенню системи надання послуг та підвищенню їх якості, встановленню налагодженого зворотного зв'язку зі споживачами, покращенню робочого клімату, забезпеченню стабільної роботи в умовах плинності персоналу, прийняттю раціональних та ефективних рішень на основі фактів. Сертифікація системи управління якістю проводиться з метою засвідчення її відповідності вимогам ДСТУ ISO 9001:2015 і забезпечення упевненості всіх зацікавлених сторін у тому, що:

• організація здатна стабільно випускати якісну продукцію, яка відповідає вимогам нормативних документів і задовольняє запити замовника;

• організація зорієнтована на підвищення задоволеності замовника завдяки результативному застосуванню системи управління якістю, у тому числі процесів, спрямованих на постійне її поліпшення.

Відповідно до ISO 9001 - схема проведення бізнес-процесів, яка забезпечує стабільну якість роботи підприємства і охоплює основні етапи його діяльності: критичний аналіз договорів, проектування, закупівлю сировини і

комплектуючих, контроль якості готової продукції, навчання персоналу, обслуговування клієнтів, роботу з відгуками і рекламаціями і т.п.

Підсумовуючи вищевикладене, можна зробити висновок, що наявність сертифікату на систему управління якістю ISO 9001 це один із механізмів контролю якості виробництва предмета закупівлі на всіх стадіях виробництва та реалізації, відповідно дієвий механізм контролю з боку замовника протипожежної техніки.

В сучасних умовах єдиним засобом контролю з боку ОРС ЦЗ за виробництвом безпечних і якісних пожежних автомобілів могла б стати організація їх обов'язкової сертифікації на заводах-виробниках. На даний момент представники замовника не в змозі забезпечити дієвий контроль за якістю продукції, що випускається.

УДК 351

52.МОДЕЛЮВАННЯ СИСТЕМ ВІДНОВЛЕННЯ БЕЗПЕЧНОЇ ЖИТТЄДІЯЛЬНОСТІ В УМОВАХ РИЗИКУ КАТАСТРОФ

Вихватін М. В.[1]

1 Харківський національний економічний університет імені Семена Кузнеця

E-mail: vykhvatin.maksym.v@hneu.net

Simulation of restoration systems of safe life activities in conditions of disaster risk

The report defines the values of stationary probabilities of each of the system states in emergency situations in order to prevent the occurrence of bottlenecks in the protection system and timely neutralization of such places even before emergency situations occur. A review and analysis of the current state of the problem of "modeling systems of safe life activities under the conditions of the risk of disasters" was carried out; information and efficiency of self-organizing systems are analyzed. Modeling a freelance situation allows you to prevent the occurrence of bottlenecks in the protection system and timely neutralize such places even before emergency situations occur.

В кожній підсистемі «робоче місце» та в цілому в системі «людина-машина-середовище» безпека праці визначається наявністю зв'язків, які обумовлені наявністю небезпек які можуть зустрітися в навколишньому середовищі, а також, зокрема, на робочому місці. Ці зв'язки можна назвати небезпечними та шкідливими. Вони породжують шкідливі та небезпечні виробничі фактори. Розглядається ситуація, коли «людина» може знаходитися в одному із станів, наприклад, «здорова та дієздатна», «хвора, але дієздатна», «недієздатна». Вона переходить з деякими ймовірностями з одного стану в інший, в залежності від підсистем «машина» та «система» та її стану на попередньому кроці.

Велике різноманіття виробничих процесів тісно пов'язані саме з взаємодією комплексу різних шкідливих та небезпечних факторів. Оператор, який знаходиться на робочому місці піддається великій різноманітності зовнішніх факторів, які впливають на його стан, працездатність, продуктивність праці тощо. До цих факторів можна віднести, наприклад, мікроклімат: температура повітря, вологість, шум. Небезпечні та шкідливі фактори так чи інше впливають на оператора протягом роботи. Основною із задач роботодавця – є захист від цих факторів найманого працівника та створення безпечних та нешкідливих умов праці на підприємстві [1].

Кваліметрична модель оцінки вибору алгоритму для вирішення нестаціонарної задачі теплопровідності: властивості якості рішення в вигляді ієрархічної структури при умові, що властивості характеризуються показниками, які кваліметрировані в різних шкалах (від слабких до сильних).

Необхідно оцінити пріоритети методів вирішення досліджуваної задачі за критеріями, які характеризують основні властивості процесу вирішення.

Міра якості визначається за формулою (1):

$$Q = \lambda_T \left(1 - \frac{T_P}{T_H}\right) + \lambda_P \frac{P_P}{P_H} + \lambda_C \left(1 - \frac{C_P}{C_H}\right) + \lambda_F \frac{F_P}{F_H} + \lambda_M \left(1 - \frac{M_P}{M_H}\right), \quad (1)$$

де $\lambda_T,\ \lambda_P,\ \lambda_C,\ \lambda_F,\ \lambda_M$ – коефіцієнти значимості відповідних показників властивостей якості з точки зору дослідження, які визначаються експериментальним шляхом за матрицею парних порівнянь в шкалі Т. Сааті;

$T_P,\ P_P,\ C_P,\ F_P,\ M_P$ – значення відповідних показників властивостей якості вирішення;

$T_H,\ P_H,\ C_H,\ F_H,\ M_H$ – нормативні значення відповідних показників якості вирішення [2].

Враховуючи різноманітні варіанти кваліметрування проблеми слід обрати аналітично-чисельний метод вирішення задачі виходячи з того, що він має високі показники у векторі глобальних пріоритетів та в варіантах, що розглядаються, відрізняється від найкращих в кожному випадку на незначну величину.

«Людина-машина-система» розглядається із введеним кінцевим простором станів s. Переважній більшості таких систем притаманна марківська властивість, що означає вірогідності переходу до нового стану цілком визначаються теперішнім станом та моментом часу. Перехідні вірогідності Марківського ланцюгу визначені шляхом максимізації інформаційної ентропії системи при обмеженнях типу математичного очікування.

Загальною задачею є визначення величин стаціонарних ймовірностей кожного зі станів системи в надзвичайних ситуаціях. З усіх систем ЛМС виділяються системи з підвищеною активністю першої підсистеми – людини, а з другої підсистеми – «машина» виділяється підсистема другого рівня – захист людини та середовища від шкідливих та небезпечних факторів.

Потік подій зі сторони підсистем «машина» та «середовище» є найпростішим з інтенсивністю λ, а час реакція на них зі сторони «людини»

розподіллено з параметром μ. Ці типи подій можуть привести з заданою вірогідністю до зміни станів системи. Величина $P_i(t)$ є вірогідністю стану S_i системи в момент часу t.

Пропонувалося, що параметри p_i порядку можна виміряти за допомогою експерименту. Припустимо, що система, що досліджується, може бути описана вектором стану

$$q = (q_1, q_2, \ldots, q_N), \tag{2}$$

компоненти якого можна виміряти. Індекс і компоненти q_i може означати як номер комірки так і різноманітні фізичні та інші величини. Припускається, що відомі статистичні середні компонент q_i та моменти компонент до четвертого порядку включно. Можна ввести наступні величини в якості обмежень величини f:

$$f_i = \langle q_i \rangle;\ f_i^{(1)} = q_i, \tag{3}$$

$$f_{ij} = \langle q_i q_j \rangle;\ f_{ij}^2 = q_i q_j, \tag{4}$$

$$f_{ijk} = \langle q_i q_j q_k \rangle;\ f_{ijk}^2 = q_i q_j q_k, \tag{5}$$

$$f_{ijk} = \langle q_i q_j q_k \rangle;\ f_{ijk}^{(2)} = q_i q_j q_k q_l. \tag{6}$$

За допомогою множників Лагранжа λ, а також з урахуванням обмежень (3) – (6) можна вирахувати максимум інформаційної ентропії та отримати для інформації величину

$$i = exp\{V(\lambda, q)\}, \tag{7}$$

в якій V розраховується виразом

$$V(\lambda, q) = \lambda + \sum_i \lambda_i\, q_i + \sum_{ij} \lambda_{ij}\, q_i q_j + \sum_{ijk} \lambda_{ijk}\, q_i q_j q_k + \sum_{ijkl} \lambda_{ijkl}\, q_i q_j q_k q_l. \tag{8}$$

Щоб виділити аналогію з нерівноважними фазовими переходами, знаходимо екстремум функції V:

$$\frac{\partial V}{\partial q_i} = 0, i = 1, \ldots, N. \tag{9}$$

В загальному випадку V може мати не один екстремум, а декілька. Їх положення ми позначимо вектором q^0. Продовжуючи дослідження нерівноважних фазових переходів q^0 слід вибрати так, щоб функції $V = (q^0 + w)$ була притаманна найбільша симетрія відносно w. Такий вибір приводить до незміщених оцінок. Це випливає з максимуму інформаційної ентропії. До зміщених оцінок приводить тільки більш низька симетрія, яка виділяє деяку структуру. Для іншого способу визначення q^0 як вектора, який вказує на становище відповідного мінімуму слід простежувати еволюцію q^0 від безструктурного стану шляхом зміни керуючого параметру. Припускаючи, що

$$q = q^0 + w, \tag{10}$$

можна записати V у вигляді

$$V(\lambda, q) = \tilde{V}(\tilde{\lambda}, w), \tag{11}$$

Де

$$\tilde{V}(\tilde{\lambda}, w) = \tilde{\lambda} + O + \sum_{ij} \tilde{\lambda}_{ij} w_i w_j + \sum_{ijk} \tilde{\lambda}_{ijk} w_i w_j w_k + \sum_{ijkl} \tilde{\lambda}_{ijkl} w_i w_j w_k w_l, \tag{12}$$

та, наприклад, коефіцієнти $\tilde{\lambda}_{ij}$ визначаються виразом

$$\tilde{\lambda}_{ij} = \frac{1}{2} \frac{\partial^2}{\partial q_i \partial q_j} | q^0. \tag{13}$$

Минулі обмеження (3) – (6), представимо у вигляді

$$f_i = \left\langle \frac{\partial}{\partial \lambda_i} V \right\rangle, \tag{14}$$

а також

$$f_{ij} = \left\langle \frac{\partial}{\partial \lambda_{ij}} \right\rangle \tag{15}$$

і так далі, одночасно перетворюються в нові обмеження [3]:

$$\bar{f} = \left\langle \frac{\partial \tilde{V,w}}{\partial \tilde{\lambda}_{ij}} \right\rangle. \tag{16}$$

Оскільки (15) та (16) є симетричними обмеженнями за індексами i та j, то множники Лагранжа так само симетричні за цими індексами:

$$\tilde{\lambda}_{ij} = \tilde{\lambda}_{ji}. \tag{17}$$

Виходячи з цього, ми можемо привести матрицю

$$\tilde{\lambda}_{ij} = \tilde{\lambda}_{ji}, \tag{18}$$

до діагонального вигляду з вагомими власними значеннями $\hat{\lambda}_k$.
Діагоналізація виконується за допомогою перетворення:

$$w_i = \sum_k a_{ik} \xi_k, \tag{19}$$

де

$$\tilde{V}(\tilde{\lambda}, w) = \hat{V}(\hat{\lambda}, \hat{\xi}), \quad (20)$$

та матриця коефіцієнтів a_{ik} ортогональна.

Перетворення (19) дозволяє привести розподіл (12) до вигляду, який відповідає (20), в якому перша частина в детальному записі приходить до наступного вигляду:

$$\hat{V}(\hat{\lambda}, \xi) = \tilde{\lambda} + \sum_k \hat{\lambda}_k \xi_k^2 + \sum_{k\lambda\mu} \hat{\lambda}_{k\lambda\mu} \xi_k \xi_\lambda \xi_\mu + \sum_{k\lambda\mu\nu} \hat{\lambda}_{k\lambda\mu} \xi_k \xi_\lambda \xi_\mu \xi_\nu. \quad (21)$$

В загальному випадку V має поблизу $\xi = 0$ сідлову точку. Відповідно, ми розрізняємо додатні та від'ємні λ та записуємо:

$$\hat{\lambda}_k \geq 0, k \to u \text{ (загальне число таких } \lambda \text{ дорівнює } N_u), \quad (22)$$

$$\hat{\lambda}_k > 0, k \to s \text{ (загальне число таких } \lambda \text{ дорівнює } N_s).$$

Порівнюючи з результатами, отриманими в мікроскопічній теорії, ми можемо скористатися термінологією теорії нерівноважних фазових переходів. Ті індекси k, які належать $\hat{\lambda} \geq 0$, ми замінимо на індекси u (від англ. unstable – нестійкі) та позначимо через ξ_u параметри порядку. Якщо подивитися з іншого боку, ті значення k, які відповідні до $\hat{\lambda} < 0$, ми замінимо індексом s (від англ. stable – стійкі) та позначимо через ξ_s амплітуду підпорядкованої моди s [4].

Беручи до уваги це розбиття, запишемо $\hat{V}$ у вигляді:

$$\hat{V}(\hat{\lambda}, \hat{\xi}) = \tilde{\lambda} + \hat{V}_u(\hat{\lambda}_u, \hat{\xi}_u) + \hat{V}_s(\hat{\lambda}_u, \lambda_s; \hat{\xi}_s, \xi_u), \quad (23)$$

де права частина відноситься тільки до параметрів порядку

$$\hat{V}_u = \sum_u \hat{\lambda} \xi_u^2 + \sum_{uu'u''} \hat{\lambda} \xi_u \xi_{u'} \xi_{u''} + \sum_{uu'u''u'''} \hat{\lambda} \xi_u \xi_{u'} \xi_{u''} \xi_{u'''}. \quad (24)$$

Що стосується $\hat{V}_s$, то ця частина має такий вигляд:

$$\hat{V}_u = \sum_s (-|\lambda_s| \xi_s^2) + \sum_{suu'} 3\hat{\lambda}_{suu'} \xi_s \xi_u \xi_{u'} + \sum_{suu'u''} 4\hat{\lambda} \xi_s \xi_u \xi_{u'} \xi_{u''},$$

з додаванням суми добутків

$$\xi_s \xi_{s'} \xi_u, \ \xi_s \xi_{s'} \xi_u \xi_{u'}, \ \xi_s \xi_{s'} \xi_{s''}, \ \xi_s \xi_{s'} \xi_{s''} \xi_u, \ \xi_s \xi_{s'} \xi_{s''} \xi_{s'''}. \quad (25)$$

Інтеграл

$$\int exp\{\hat{V}_s\} d^{N_s} \xi_s = g(\xi_u) > 0, \quad (26)$$

визначає тільки функцію параметрів порядку ξ_u. Додамо функцію h, визначивши її співвідношенням

$$h(\xi_u) + \hat{V}_s = W_s(\xi_s|\xi_u). \quad (27)$$

Та нову функцію W_s, яка задається співвідношенням

$$h(\xi_u) + \hat{V}_s = W_s(\xi_s|\xi_u). \quad (28)$$

Це визначення гарантує, що величина

$$P(\xi_s|\xi_u) = exp\{W_s(\xi_s|\xi_u)\} \quad (29)$$

є нормованою в просторі підпорядкованих мод при будь якому параметрі порядку ξ_u. Потрібно визначити нову функцію Wu, , щоб розподіл (23) залишався незмінним при введені h. Зробимо це за допомогою співвідношення:

$$\tilde{\lambda} + \hat{V}_u(\hat{\lambda}, \xi_u) - h(\xi_u) = W_u(\xi_u). \quad (30)$$

Наприкінці цього розділу запишемо розподіл (23) у вигляді:

$$\hat{V}(\hat{\lambda}, \xi) = W_u(\xi_u) + W_s(\xi_s|\xi_u). \quad (31)$$

Це дозволить нам отримати співвідношення

$$exp\{\hat{V}\} = P(\xi_u)P(\xi_s|\xi_u), \quad (32)$$

де

$$P(\xi_u) = exp\{W_u\}, \quad (33)$$

а множник $P(\xi_s|\xi_u)$ визначається співвідношенням (29).

$P(\xi_s|\xi_u)$ є умовною ймовірністю, в той час як $P(\xi_u)$ – функція розподілу тільки параметрів порядку. До цього моменту наш підхід був тільки загальним. Цей спосіб дозволяє нам визначити функцію розподілу для параметрів порядку, розподіл умовних ймовірностей підпорядкованих мод. В окремому випадку, співвідношення (32), окремий випадком принципу підпорядкованості.

Висновки

Класичні системи масового обслуговування адекватно моделюють систему за умови ординарності вхідного потоку та відсутності наслідків і стаціонарності. При дуже невеликих простота потоку даних є справедливою для потоку аварій. Більш ймовірними будуть короткі інтервали між аваріями. Модель системи масового обслуговування підходить для рятувальних підрозділів, для який ліквідація аварії буде «стаціонарним станом».

За допомогою задач оптимізації для інформаційної ентропії розраховані значення перехідних ймовірностей. Цілком зрозуміло, що аварії чи катастрофи мають релеєвські, степенні чи ерлангови закони розподілу. Моделювання позаштатної ситуації дозволяє попередити виникнення вузьких місць системи захисту та своєчасно знешкоджувати такі місця ще до виникнення аварійних ситуацій.

Література

21. Небезпечні та шкідливі фактори. URL : https://www.sop.com.ua/ article/206-qqq-16-m6-13-06-2016-nebezpechn-tashkdliv-virobnich-faktori .
22. Циба В. Кваліметрія – теорія вимірювання в гуманітарних і природничих науках / В. Циба // Соціальна психологія. – 2005. – № 4. – С. 3–20.
23. Дзюндзюк Б. В., Наумейко І. В., Сердюк Н. Н. Змістовна модель взаємодії декількох шкідливих факторів на людину // Радіоелектроніка та інформатика. 2000. № 3. С. 131-132.
24. Вентцель Е. С., Овчаров Л. А. Теория вероятностей. Москва : Нау-ка, 1969. 366 с.

УДК 614.84

53.ВІЗУАЛІЗАЦІЯ ПОЖЕЖ У ПРОСТОРІ ТА ЧАСІ НА ОСНОВІ МЕТОДУ ПРОСТОРОВОГО РОЗМІЩЕННЯ ПОЖЕЖОНЕБЕЗПЕЧНИХ ДІЛЯНОК

Гаврись А.П., Яковчук Р.С., Пекарська О.О.

Львівський державний університет безпеки життєдіяльності
E-mail: havrys.and@gmail.com, yakovchukrs@ukr.net, pekarska86@gmail.com

Visualization of Fire in Space and Time on the Basis of the Method of Spatial Location of Fire-Dangerous Areas

The subject of the study is the forecasting of fires using the spatial location of fire-hazardous areas. To do this, several approaches were used to visualize data in space and time. A temporary map has been created showing the points of fires using a color scheme linked to the date. A series of small multiple visualizations has been developed. A time series has been created in which the regularity of the brightness of points is distributed depending on the date of origin and animated maps that allow you to view data in space and time. In this case, the geographic information system was used as the main tool when working with maps, as it is one of the best ways to process georeferenced data displayed on the map. A space-time cube is displayed, which displays data in 3D format, or rather, fire points, symbolized by the average temperature of the fire (displayed in different colors) in accordance with the day of the month.

Лісові пожежі є великою проблемою вже не одне десятиліття. Щороку на боротьбу з ними уряди країн та міжнародні організації виділяють тисячі доларів, а служби цивільного захисту постійно організовують проведення гуманітарних місій в країнах, що постраждали від цієї надзвичайної ситуації. Тому необхідним є завчасне попередження та моніторинг виникнення масштабних лісових пожеж, що можна зробити лише за допомогою сучасних інформаційних технологій.

Сьогодні ми можемо здійснювати таку профілактику виникнення пожеж за допомогою сучасних технологій та обмінюючись міжнародним досвідом, отримувати нові корисні знання для запобігання цим надзвичайним ситуаціям.

Для кращого розуміння природи поширення та можливого прогнозування виникнення лісових пожеж, а також для вивчення причин їхнього виникнення авторами було розроблено метод просторового розміщення пожежонебезпечних ділянок на підставі даних дистанційного зондування землі, що дає можливість створити полігони пожежонебезпечних територій та візуалізувати карту просторового розподілення температури на ділянках пожежі.

Оскільки програма ArcGIS орієнтована, в основному, на карти, ніж на час, то почнемо з того, що складемо просту тимчасову карту, відобразивши на ній точки пожеж за допомогою кольорової схеми, прив’язаної до дати.

На карті нижче, де порівнюються дати точок локалізованих пожеж, видно, що більш ранні точки локальних кластерів, розташовані на західному боці, тоді як пізніші точки - на сході.

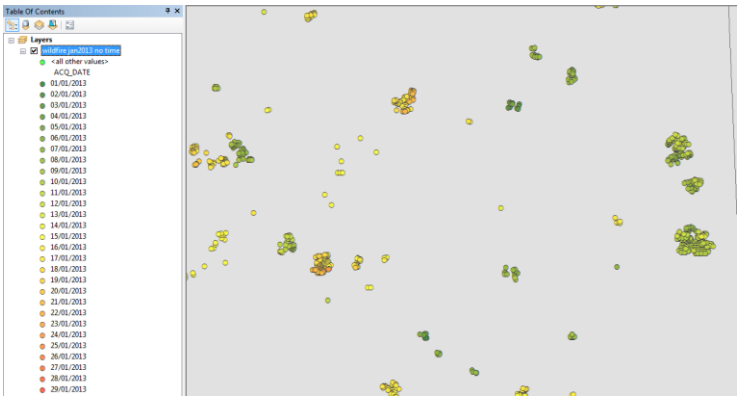


Рис. 1. Карта розташування точок локалізованих пожеж ранжованих за датою виникнення у програмному середовищі ArcGIS

Анімовані карти можуть бути корисним способом перегляду даних в просторі та часі. Повзунок часу в програмі ArcGIS забезпечує швидкий засіб вивчення просторових та часових змін у поширенні лісових пожеж та їх яскравості.

У властивостях шару вмикаємо шар «Час» (Time) на шарі «wildfire», використовуючи «ACQ_DATE» як поле часу (Time Field) (рис. 2).

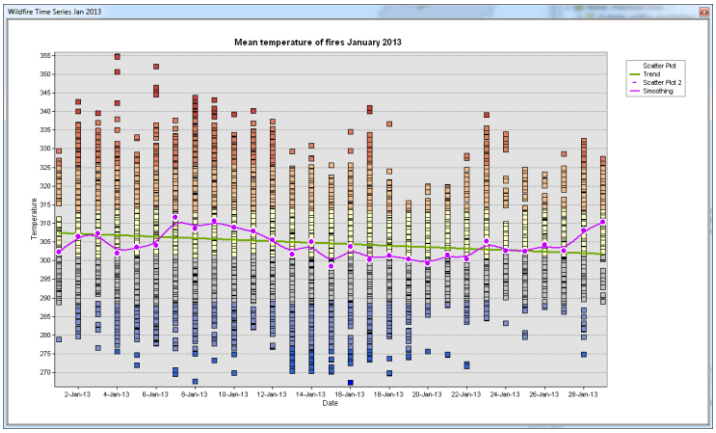


Рис. 2. Графік залежності яскравості точок пожежі (вогневі точки) від часу з нанесеною лінією тренду

Наступним кроком створюємо анімовану карту часу температури лісової пожежі в часі та експортуємо відео у форматі MPEG. Збільшуємо тривалість часу, щоб зрозуміти динаміку змін нашого зразка.

Програмний комплекс ArcGIS підтримує створення кубів в просторі та часі, що зберігаються у форматі NetCDF. Тоді значення вокселів можна експортувати до класу функцій для відображення в програмах ArcMap або ArcScene. Відображення даних у 3D є дорогим в обчисленні, тому ми будемо використовувати невелику підмножину даних.

Для цієї роботи виберемо достатньо великий кластер точок пожежі та експортуємо як новий клас функцій. Далі вибравши інструмент «Create Space Time Cube By Aggregating Points», створюємо куб просторового часу у форматі NetDCF, який зберігає підрахунок кількості точок пожежі та середньої температури пожеж у кожній комірці сітки.

Для того, щоб експортувати значення комірок до класу об’єктів, у якому порядкове значення часового виміру присвоюється значенню z кожного воксельного центроїда, скористаємось інструментом «Visualize Space Time Cube» (Візуалізація куба просторового часу). Наступним кроком потрібно переглянути клас функцій куба даних у 3D в програмі ArcScene, і щоб отримати гарну візуалізацію, необхідно попрацювати із символікою.

На рисунку 3 показано скупчення точок пожежі, що символізуються середньою температурою вогню. Розташування кубу відповідає дню місяця - чим нижче куб, тим, відповідно, раніший день місяця.

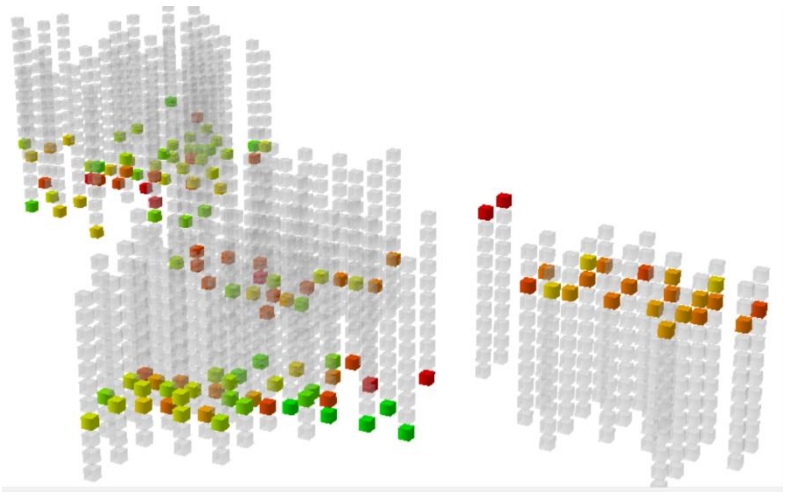


Рис. 3. Візуалізований просторово-часовий куб з позначенням середньої температури вогневих точок

Висновки

Такі явища, як пожежі, виникають як через місцеві причини (наявність палива, джерело займання), так і через регіональні (клімат, землекористування), а, отже, можуть проявляти характер у різних масштабах. Тому необхідно вміти передбачати та виявляти закономірності у певних просторових та часових масштабах. Для даної мети використовується розроблений авторами метод просторового розміщення пожежонебезпечних ділянок на підставі даних дистанційного зондування Землі. Оскільки, окрім прямої задачі - локалізацію вогневих точок (пожеж), даний метод дає можливість дослідити закономірності у просторових та часових масштабах, з можливістю подальшої візуалізації просторово-часового кубу у форматі 3D в програмі ArcScene, що дасть можливість ефективніше спрогнозувати пожежонебезпечні періоди та ділянки на досліджуваній території. Метод просторового розміщення пожежонебезпечних ділянок може бути використаний для будь якої досліджуваної території для якої наявні статистичні та просторові дані, як з метою локалізації пожеж, так і з метою дослідження закономірностей в обраних просторово-часових масштабах.

Література

1. Abdulsahib, G.M., Khalaf, O.I. 2018. An improved algorithm to fire detection in forest by using wireless sensor networks. International Journal of Civil Engineering & Technology (IJCIET)-Scopus Indexed, 9(11), 369–377.
2. ArcGIS Resources. 2012. ArcGIS Help 10.1. [online] Available at: http://resources.arcgis.com/en/help/ main/10.1/index.html#/ [Accessed 19 May 2021].
3. Atwood, E.C., Englhart, S., Lorenz, E., Halle, W., Wiedemann, W., Siegert, F. 2016. Detection and Characterization of Low Temperature Peat Fires during the 2015 Fire Catastrophe in Indonesia Using a New High-Sensitivity Fire Monitoring Satellite Sensor (FireBird). PLoS ONE, 11, e0159410.

4. EARTHDATA. 2020. Active Fire Data | Earthdata. [online] Available at: https://earthdata.nasa. gov/earth-observation-data/near-real-time/firms/ active-fire-data.
5. Havrys, A.P., Moreniuk, R.Y., Harasymiuk, I.M. 2019. Method of spatial location of fire-dangerous sites on the basis of Remote Sensing and Spatial Data. Scientific bulletin of UNFU, 29(8), 36–42. [in Ukrainian] https://doi.org/10.36930/40290804
6. Iizuka, K., Watanabe, K., Kato, T., Putri, N. A., Silsigia, S., Kameoka, T., & Kozan, O. 2018. Visualizing the spatiotemporal trends of thermal characteristics in a peatland plantation forest in Indonesia: Pilot test using unmanned aerial systems (UASs). Remote Sensing, 10(9), 1345.
7. Li, J., Li, X., Chen, C., Zheng, H., Liu, N. 2018. Three-dimensional dynamic simulation system for forest surface fire spreading prediction. International Journal of Pattern Recognition and Artificial Intelligence, 32(8), 1850026.
8. Li, P., Zhao, W. 2020. Image fire detection algorithms based on convolutional neural networks. Case Studies in Thermal Engineering, 19, 100625.
9. Liu, D., Xu, Z., Fan, C. 2019. Generalized analysis of regional fire risk using data visualization of incidents. Fire and materials, 43(4), 413–421.
10. Luo, Y., Zhao, L., Liu, P., Huang, D. 2018. Fire smoke detection algorithm based on motion characteristic and convolutional neural networks. Multimedia Tools and Applications, 77(12), 15075–15092.
11. Muhammad, K., Khan, S., Elhoseny, M., Ahmed, S.H., Baik, S.W. 2019. Efficient fire detection for uncertain surveillance environment. IEEE Transactions on Industrial Informatics, 15(5), 3113–3122.
12. Nikolaevich, K.V., Starodub, Y., Havrys, A. 2021. Computer Modeling in the Application to Geothermal Engineering. Advances in Civil Engineering, 2021.

УДК 621.317; 004.91

54.ПРО НЕОБХІДНІСТЬ СТВОРЕННЯ РЕЄСТРУ МАТЕМАТИЧНИХ МОДЕЛЕЙ ОРГАНІЗМУ ЛЮДИНИ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ДІАГНОСТИКИ В СФЕРІ МЕДИЦИНИ КАТАСТРОФ

Євланов М. В.[1], Антощенков Р.В. [2], Черепньов І.А.[2]
[1] Харківський національний університет радіоелектроніки, [2] Державний біотехнологічний університет
voenpred314@ukr.net

ON THE NEED TO CREATE A REGISTER OF MATHEMATICAL MODELS OF THE HUMAN BODY TO IMPROVE THE EFFECTIVENESS OF DIAGNOSTICS IN THE FIELD OF DISASTER MEDICINE

The reasons for the increased interest in the development of modern equipment for medical diagnostics are investigated. The problem of applying analytical mathematical models in the course of designing and using such equipment is singled out. The features of the manifestation of this problem in the course of designing a system for radiometric contact diagnostics of human body temperature

are considered. The concept of a register of models and variants of their adaptation to the applied features of the tasks being solved for designing medical diagnostic equipment, taking into account the features of disaster medicine, is proposed.

Як відомо, успішність лікування залежить від об'єктивності та своєчасності проведення медичної діагностики. Традиційно, в сфері медицини надзвичайних ситуацій використовуються різні види променевої діагностики, яка дозволяє виявити внутрішні ураження і травми [1]. Враховуючи наявність серйозних недоліків у кількісному та якісному забезпеченні лікувальних закладів України сучасною діагностичною апаратурою, завдання конструювання приладів, що використовують передові технології, є досить актуальним [2]. Одним з обов'язкових етапів створення медичної апаратури, це проведення експериментів на тваринах і за участю людини [3]. Однак, враховуючи вимоги до безпеки, в ряді випадків участь людини або неможлива, або значно обмежена. Крім того, міжнародні норми вимагають мінімізувати використання лабораторних тварин, особливо - теплокровних.

Дані обставини повинні були збільшувати значення математичних та електрофізичних моделей, а також комп'ютерного моделювання [4]. Класичні моделі тіла людини являють собою сукупність циліндричних і сферичних об'єктів, у яких наявний неоднорідний розподіл структури по радіусу [5,6]. Базовим прикладом подібних моделей є модель Столвейка-Харді, наведена на рис.1 [6]. Але такі моделі мають досить значні обмеження у використанні під час вирішення науково-прикладних або чисто прикладних задач, у тому числі – з конструювання та створення методик використання сучасної діагностичної апаратури, неодмінними елементами якої є комп’ютеризовані системи різного призначення. Можна стверджувати, що основною особливістю сучасної обробки результатів діагностичних вимірювань є майже повна відмова від застосування аналітичних моделей.

Ця відмова обумовлена зазначеними в [1]причинами, серед яких, зокрема, визначені надмірна складність і неточність математичного апарату. Саме вони на практиці приводять до значних витрат часу та обчислювальних ресурсів на вирішення задач обробки результатів діагностичних вимірювань у реальному масштабі часу, що, у свою чергу приводить до значного збільшення вартості створення та експлуатації сучасної діагностичної апаратури.

Добрим прикладом обмеження використання аналітичних моделей для вирішення задач діагностики є дослідження з обробки результатів радіометричних вимірювань. Так, у [7] розглянуто результати розробки когерентної моделі радіометричного контактного вимірювання температури тіла людини. Дана модель передбачала застосування рівняння біотепла Пеннеса до шестишарової моделі голови людини з подальшою обробкою результатів моделювання із застосуванням прямої електромагнітної моделі. Однак у [7] зазначалося, що отримана когерентна модель для підвищення точності вимірювань повинна була включати в себе статистику популяційних варіацій населення для широкого діапазону частот.

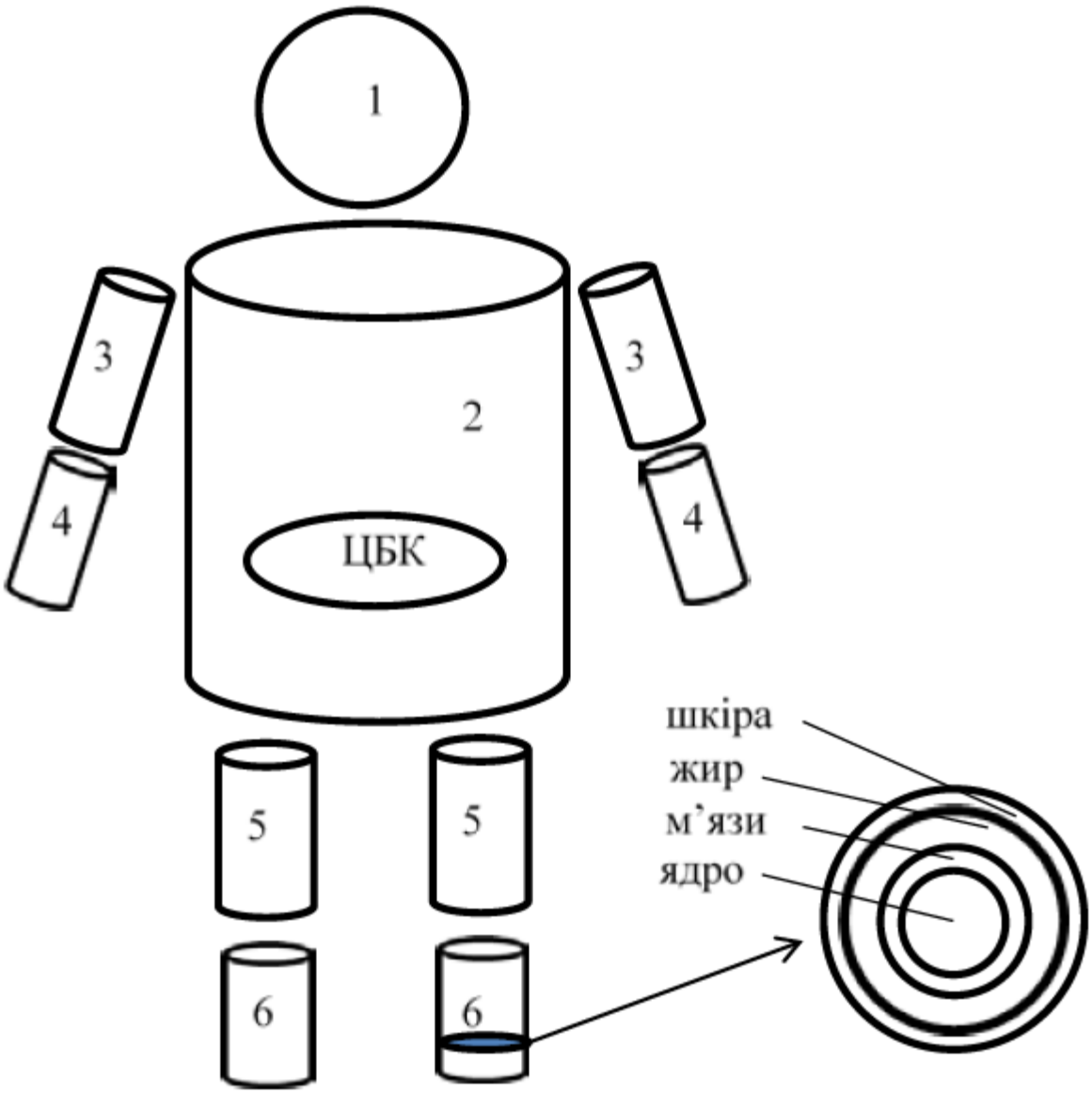


Рисунок 1 – Схема моделі Столвейка-Харді [6]:
ЦКБ – центральний басейн крові, 1 – голова, 2 – тулуб, 3 – плече, 4 – лікоть,
5 – стегно, 6 – гомілка

Тому в ході подальших досліджень [8] автори зосередили свою увагу на внесенні поправок до когерентної моделі за результатами проведених експериментальних вимірювань з урахуванням популяційних варіацій для населення. Отримані уточнення дозволили в [8] скорегувати когерентну модель для окремого регіону США таким чином, щоб результати її застосування знаходилися в межах клінічно прийнятного діапазону помилок. Таким чином, отримана математична модель володіє надмірною точністю, але тільки для конкретного регіону і для осіб які проживають на цій території. Дана обставина ускладнює застосування запропонованої у [7,8] апаратури на практиці в інших регіонах світу, тому що при будь-яких неврахованих варіаціях віку, етнічної

приналежності тощо, ці моделі вже не будуть давати результату з прийнятною точністю.

Для вирішення цієї проблеми пропонується використати досвід управління знаннями при вирішенні задач управління проєктною діяльністю у найрізноманітніших галузях діяльності людства. Цей досвід вказує на необхідність зосередження уваги фахівців, які вирішують задач проектування систем різного призначення (в тому числі – систем програмно-апаратної чи апаратної діагностики) на вирішення таких завдань:

а) здобування нових та вдосконалення вже відомих знань щодо предметної галузі та створюваної системи, які є загальновживаними, тобто не змінюють свою структуру та зміст залежно від конкретних предметної галузі та особливостей створюваної діагностичної апаратури;

б) внесення до цих знань постійно оновлюваних змін і доповнень, які базуються на результатах експериментальних і наукових досліджень різноманітних особливостей – регіональних, етнічних, вікових тощо людей, шкідливих виробничих факторів, діючих на різних підприємствах, а такою особливостей конкретних прояв природних і техногенних катастроф.

Для вирішення цих завдань в напрямі прикладних науково-технічних робіт з проектування та створення медичних діагностичних систем необхідно створення реєстру математичних моделей, актуальних на поточний момент часу з описом їх призначення та їх структури. Цей реєстр повинен складатися ц двох основних розділів:

а) розділ, який описує конкретні математичні моделі, їх базову структуру та зміст;

б) розділ, який описує особливості адаптації базової математичної моделі для вирішення кожної конкретної прикладної задачі (у тому числі додаткові структурні і змістовні елементи як результати коригування базової моделі).

Окрема складова цього реєстру повинна представляти банк експериментальних даних, які підтверджують або спростовують досліджувані математичні моделі.

Як технологічну базу такого реєстру пропонується використовувати комбінацію інформаційних технологій, які базуються на принципах стандартного опису сервісів, що автоматизують різні види бізнесу людини, та на принципах побудови і експлуатації Вікіпедії та інших енциклопедій вільного доступу.

Наявність такого реєстру дозволить підвищити ефективність створення нових поколінь медичної діагностичної апаратури, причому в залежності від специфіки її застосування, можна буде досягти розумного компромісу між точністю і складністю використовуваних математичних моделей. Це значно спростить проектування діагностичної апаратури, зменшить витрати на створення та експлуатацію цієї апаратури.

Література

1. Черепнев И.А. Основные требования к диагностической аппаратуре на основе измерения собственных электромагнитных излучений биологических объектов. *Системи управління навігації та зв'язку.* 2011. Вип.4 (20). С. 124 – 131.
2. Організація променевої діагностики в умовах реформування системи медичної допомоги на регіональному рівні: метод. рекоменд. / Г.О. Слабкий та ін. Київ, 2016. 36 с.
3. Березко Л.О., Соколов С.Є. Алгоритмічний підхід до проєктування нової медичної апаратури. *Комп'ютерні системи та мережі.* 2020. Вип. 2, № 1. С. 6-12. doi.org/ 10.23939/csn2020.01.006.
4. О возрастающей роли математического моделирования в медико-биологических экспериментах в рамках правовых норм биоэтики / И.А. Черепнев та ін. *Вісник ХНТУСГ. Механізація сільського господарського виробництва.* 2012. Вип.124, т.2. С. 490 – 497.
5. Пиротти Е.Л., Черепнев И.А. Методика расчета рассеянных электромагнитных полей на системах организма человека цилиндрической и сферической формы. *Колективна монографія ХВУ.* 2000. Вип.2(28). С.145–148.
6. Стасевич С.П., Руда М.В., Ничай С.Т. Математичні моделі для прогнозування теплового комфорту людини у навколишньому середовищі. *Екологічні науки*. 2021. № 5(38). С. 9-14.
7. Tisdale, K., Bringer, A., Kiourti, A. (2022). Development of a Coherent Model for Radiometric Core Body Temperature Sensing. IEEE Journal of Electromagnetics, RF and Microwaves in Medicine and Biology, 6(3), 355-363. DOI: 10.1109/JERM.2021.3137962.
8. Tisdale, K., Bringer, A., Kiourti, A. (2022). A Core Body Temperature Retrieval Method for Microwave Radiometry When Tissue Permittivity is Unknown. IEEE Journal of Electromagnetics, RF and Microwaves in Medicine and Biology, 6(4), 470-476. DOI: 10.1109/JERM.2022.3171092.

УДК 614.84

55.ОСНОВИ ВИКОРИСТАННЯ ПОЖЕЖНИХ АВТОМОБІЛІВ

Калиновський А.Я.[1], Кравченко І.І.[1]

1 Національний університет цивільної захисту України
E-mail: ugzu.iart@gmail.com

Fundamentals of using fire trucks

Fire engines are operated in different climatic and road conditions. As a rule, the engine and transmission mechanisms warm up already when heading to the place of call. In these conditions, the operation of cars is always accompanied by an increased intensity of wear of the working surfaces of the parts.

The solution to these problems is largely determined by the qualifications of the personnel who operate the cars. Therefore, employees of the State Emergency Service must ensure a high level of readiness of vehicles to act as intended and such training of personnel that would allow them to be used effectively at fires.

На оснащенні пожежно-рятувальних підрозділів ДСНС на кінець 2022 року знаходиться 3 тис. 357 од. основної та спеціальної пожежної техніки, у тому числі 2 тис. 627 пожежних автоцистерн, 376 автомобілів першої пожежної допомоги, 269 пожежних автодрабин, 116 рукавних автомобілів, 111 пожежних насосних станцій, 60 штабних автомобілів, 48 пожежних атопідіймачів [1].

У минулому році до підрозділів ДСНС надійшло 417 пожежних автоцистерн, 45 автодрабини та 19 колінчатих підіймачів, які ДСНС централізовано отримано у вигляді гуманітарної допомоги від європейських партнерів. Територіальні органи ДСНС отримували пожежно-рятувальну техніку через органи місцевої влади, волонтерські та приватні організації.

Разом з тим, незважаючи на значну кількість пожежної техніки, що оставлена в останні роки для переоснащення пожежно-рятувальних підрозділів ДСНС більше половини (64%) пожежних автомобілів на їх оснащенні має термін експлуатації понад 20 років та підлягає списанню, у тому числі через неможливість забезпечити їх ремонт і технічне обслуговування, зважаючи що значна кількість цієї техніки радянського та російського виробництва на шасі ЗІЛ, КаМАЗ, або побудована на шасі білоруського МАЗу.

Використання пожежних автомобілів також носить випадковий характер, як і причини що викликали пожежу та час її виникнення [2].

Збитки від пожежі в самому загальному виді визначаються двома групами факторів.

Першу групу факторів складають: горючість будівельних матеріалів будинків, внутрішньої начинки, планування будинків і споруджень. Ця група факторів багато в чому обумовлює умови розвитку пожеж.

Друга група факторів включає: швидкість виявлення та оповіщення про пожежу, технічну характеристику пожежних машин, дорожні умови, водопостачання та інші подобні фактори. Ці фактори в значній мірі обумовлюють умови гасіння пожеж.

Керуючись факторами другої групи, можна звести до мінімуму тривалість пожеж і, отже, збитки від них. Це обумовлено тим, що з досить високою точністю можна вважати, що збитки від пожежі еквівалентні його тривалості.

Пожежні автомобілі повинні характеризуватися високою готовністю до дій за призначенням і достатньою імовірністю виконання задач по гасінню пожеж у мінімальний час. Таким чином, необхідно оцінювати готовність до дій за призначенням пожежних підрозділів.

Готовність пожежних підрозділів можна характеризувати імовірністю того, що підрозділ готовий виконати задачі, обумовлені статутом дій органів управління та підрозділів Оперативно-рятувальної служби цивільного захисту під час гасіння пожеж.

В даний час більше половини всіх пожеж гасять протягом 1 години. Цим визначається особливість роботи пожежних автомобілів. Вона полягає в тому, що тривалість їх експлуатації відносно невелика. Тому необхідно так обслуговувати автомобілі, щоб протягом цього часу відмови в роботі були практично виключені.

Для того щоб у мінімальний час локалізувати і ліквідувати пожежу, необхідно забезпечити:

- навчання особового складу;
- утримання пожежних автомобілів в технічно справному стані;
- високу готовність автомобілів і пожежних частин до дій за призначенням;
- високу надійність пожежної техніки в експлуатації.

Пожежні автомобілі експлуатуються в різних кліматичних і дорожніх умовах. Як правило, прогрів двигуна і механізмів трансмісії відбувається вже при прямуванні до місця виклику. У цих умовах експлуатація автомобілів завжди супроводжується підвищеною інтенсивністю зношування робочих поверхонь деталей.

Унаслідок цього погіршуються прохідність і динамічні якості автомобіля, подача пожежного насоса і т.п. Для ефективного використання машин протягом міжремонтного пробігу необхідно, щоб ці зміни відбувалися повільніше і машини працювали безвідмовно.

Висновки

Рішення цих задач багато в чому визначається кваліфікацією особового складу, який експлуатує автомобілі. Тому співробітники ДСНС повинні забезпечувати високу готовність автомобілів до дій за призначенням і таку підготовку особового складу, що дозволила б ефективно їх використовувати на пожежах.

Література

25. Огляд за напрямком діяльності державних пожежно-рятувальних підрозділів ДСНС у 2022 році.
26. Пожежні машини : Навч. посібн. / О.М. Ларін, В.Г. Баркалов, С.А. Виноградов та ін. ─ Х. : НУЦЗУ, 2016 . ─ 279 с.

УДК 614.8.086+ 614.89

56.ЗАХОДИ ЗАХИСТУ НАСЕЛЕННЯ ТА ОРГАНІЗАЦІЯ РЕАГУВАННЯ ПІД ЧАС ЛІДКВІДАЦІЇ НАСЛІДКІВ ІЗ ЗАСТОСУВАННЯМ ТАКТИЧНОЇ ЯДЕРНОЇ ЗБРОЇ

Лоїк В.Б., Синельніков О.Д., Гончаренко М.О.
Навчально-науковий інститут цивільного захисту
Львівського державного університету безпеки життєдіяльності, Львів, Україна
E-mail: v.loik1984@gmail.com, o.synelnikov@gmail.com, mariagoncharenco@gmail.com

Measures for the protection of the population and organization of the response during the liquidation of the consequences of the use of tactical nuclear weapons

The greatest danger during a nuclear explosion is not radiation, but heat radiation and shock waves. Immediately after the explosion, a ball of fire is formed in its epicenter, which begins to spread around. The main feature of such an explosion is a super-powerful flash of blinding light, it is visible even on the brightest sunny day. This is the first element of the impressive mechanism of a nuclear explosion - IR radiation, which lasts only a few seconds, but it is so intense that, despite the short duration of its action, it can cause burns to exposed parts of the body facing the direction of the explosion and temporary blindness.

Найбільшу небезпеку під час ядерного вибуху становить не радіація, а теплове випромінювання та ударна хвиля. Одразу після вибуху в його епіцентрі утворюється вогняна куля, яка починає поширюватися навколо. Головна ознака такого вибуху — надпотужний спалах сліпучого світла, він помітний навіть у найяскравіший сонячний день. Це перший елемент вражаючого механізму ядерного вибуху — ІЧ-випромінювання, яке триває всього кілька секунд, але воно настільки інтенсивне, що попри короткочасність своєї дії, може викликати опіки відкритих ділянок тіла, обернених у бік вибуху, і тимчасове засліплення.

Вибух утворює засліплювальний спалах світла та потужну хвилю жару, які миттєво ширитимуться далі від епіцентру. Діаметр цих зон може сягнути понад 10 км, але, знову ж таки, залежатиме від потужності вибуху та способу підриву ядерного боєприпасу. За кількадесят секунд після того від епіцентру вибуху почне поширюватися ударна хвиля, яка просто змітатиме все на своєму шляху. Ураження виникатимуть і від самої хвилі, й від уламків зруйнованих споруд, грудок землі та каміння. Після вибуху підійметься характерний «ядерний гриб», на землю почне випадати радіоактивний осад, в радіусі багатьох кілометрів вируватимуть пожежі [1].

Після спалаху утворюється область, що світиться, у вигляді вогняної кулі у разі наземного і надводного вибуху у вигляді півкулі, яскравість якої в початковій стадії значно перевершує яскравість сонця. Вогняна куля, швидко збільшуючись у розмірах, підіймається, при цьому яскравість її світіння

поступово зменшується. Через кілька секунд після виникнення вогняна куля перетворюється на хмару, що клубиться. Одночасно з вогняною кулею із землі слідом за хмарою підіймається стовп пилу та диму. Ця стадія вибуху зорово нагадує форму гриба — звідси й назва «ядерний гриб».

Удар ядерною ракетою, наприклад, по Львову буде в рази руйнівнішим. Серйозних руйнувань може зазнати майже все місто, а пожежі поширяться далеко за його межі наведено на рис. 1.

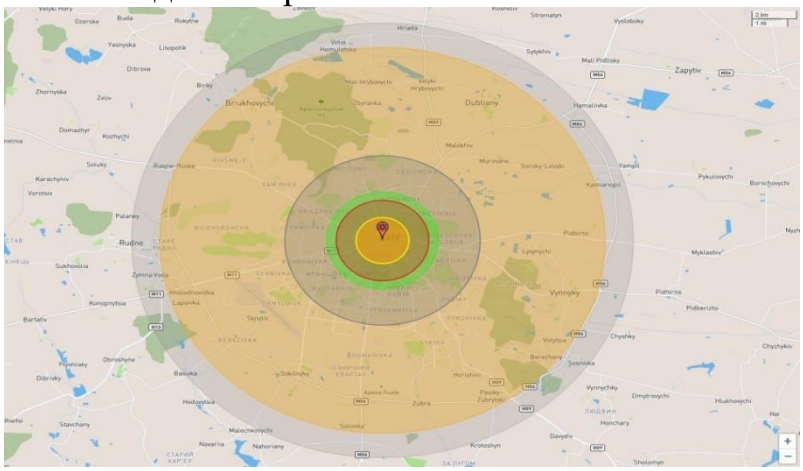


Рис. 1. Прогнозування ***наслідків удару ядерною ракетою***

Жовтим кольором позначений умовний розмір ядерної вогняної кулі, його радіус — 380 метрів, а висота — 350 метрів. Зеленим кольором зображено умовний радіус випромінювання. В цьому випадку він становить 1,11 км. Темно-сірий колір — помірний радіус ураження вибухом, під час вибуху 100-кілотонної бомби радіус становить 3,26 км. Помаранчевим кольором показаний радіус теплового випромінювання — 4,38 км. Усі, хто знаходяться в цьому радіусі поза сховищами, отримають опіки третього ступеня. Світло-сірий колір — це радіус ураження "легким" вибухом, становить 9,18 км [1].

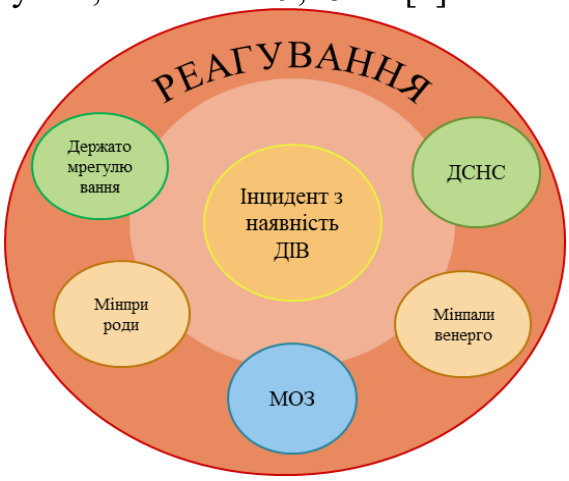


Рис. 2. Реагування центральних органів виконавчої влади

ДСНС: організацію оповіщення населення про загрозу і виникнення радіаційної аварії, контроль за функціонуванням територіальних і локальних систем оповіщення; використання аварійно(пошуково)-рятувальних спеціалізованих формувань для реагування на радіаційну аварію; координацію та контроль за здійсненням заходів щодо захисту населення і територій при

виникненні радіаційної аварії; виконання обов'язків компетентного національного органу, уповноваженого надсилати та одержувати прохання про допомогу і приймати пропозиції про допомогу згідно з Конвенцією про допомогу в разі ядерної аварії або радіаційної аварійної ситуації; забезпечення керівних органів єдиної системи цивільного захисту гідрометеорологічною інформацією та даними про забруднення довкілля за результатами спостережень, що здійснює Державна гідрометеорологічна служба.

Мінпаливенерго: створення системи заходів щодо забезпечення готовності до ліквідації радіаційної аварії на об'єктах категорії радіаційної небезпеки I, включаючи розробку відповідних нормативних актів; координацію дій з ліквідації радіаційної аварії на об'єктах категорії радіаційної небезпеки I та мінімізації її наслідків; надання інформаційно-аналітичної підтримки групі екстреної допомоги АЕС, яка створюється експлуатуючою організацією, відповідно до компетенції.

МОЗ: організацію і координацію робіт з надання термінової медичної допомоги постраждалому населенню в зонах радіаційної аварії, координацію робіт з евакуації постраждалого населення і хворих із цих зон; оцінку і прогноз дозових навантажень населення та надання рекомендацій щодо їх мінімізації, організацію оперативного контролю радіоактивного забруднення у зонах радіаційної аварії; збирання, узагальнення, аналіз і надання органам єдиної системи цивільного захисту відомостей про постраждалих і хворих осіб у зонах радіаційної аварії; створення резервів медичного майна і лікарських засобів та забезпечення термінового постачання їх для локалізації наслідків радіаційної аварії.

Мінприроди: методичне забезпечення управління та контроль за екологічно обґрунтованим проведенням робіт з ліквідації наслідків радіаційної аварії; організацію і проведення спостереження, оцінки і прогнозу стану атмосфери, водних об'єктів і сільськогосподарських культур, радіоактивного забруднення довкілля України; забезпечення керівних органів єдиної системи цивільного захисту гідрометеорологічною інформацією та даними про забруднення довкілля; оперативний контроль за радіоактивним забрудненням у випадку РА згідно з установленим регламентом у місцях проведення постійних спостережень.

Держатомрегулювання: міжнародний інформаційний обмін згідно з Конвенцією про оперативне оповіщення про ядерну аварію та у рамках відповідних двосторонніх договорів з іншими країнами; оперативне повідомлення через засоби масової інформації про радіаційні аварії на території України, а також за її межами у ра зі можливості транскордонного перенесення радіоактивних речовин [3].

Під час ядерного вибуху потрібно діяти максимально швидко. Потрібно заздалегідь подбати про укриття, тривожну валізку, запас води й харчів. Найкращий спосіб пережити ядерний удар у місті — підвал із залізобетонним перекриттям. Він добре захистить від радіації та руйнувань. Бажано, щоб укриття мало щонайменше два виходи, один з яких облаштовано так, щоб його не

завалило уламками. Там має бути запас їжі й води орієнтовно на тиждень. Сховатися можна і в будь-якому іншому приміщенні, але варто триматися якомога далі від стін і подбати, щоб ззовні потрапляло якнайменше повітря. Основна кількість радіації поширюватиметься з пилом від вибухів, який осідатиме на зовнішніх частинах будівель [2].

Звичайний підвал може врятувати, навіть якщо ви перебуваєте в епіцентрі ядерного вибуху. У 1945 році в Хіросімі японець Ейзо Номура, який випадково опинився у звичайному підвалі звичайного будинку, вижив за 170 метрів від епіцентру ядерного удару. Попри це, Номура на своїх ногах і без загрозливих для життя пошкоджень вийшов з будівлі і пішов з епіцентру пішки. Помер він через 37 років, у 84 роки, причому дожив до них досить-таки здоровою людиною. Після того, як опинилися в бомбосховищі або метро, а удари припинилися, не слід чинити, як Номура, і йти пішки. Коли сховище можна буде покинути, повідомлять відповідні служби. Швидше за все це трапиться через 7-10 днів після вибуху, тому важливо мати з собою герметично запечатані запаси води та їжі. Утім, їжа та вода — це наступний крок.

Якщо вибух застав на вулиці, в жодному разі не дивитися в його бік. Якщо помітите спалах, негайно падайте на землю обличчям униз. Спробуйте знайти хоч якесь укриття, щоб залишитися в «тіні» від теплової хвилі. Прикрийте голову руками, а краще капюшоном куртки чи верхнім одягом. Захистіть рот і ніс шарфом чи хустиною. Остерігайтесь уламків та спробуйте дістатися найближчого бомбосховища. Залишайтеся в укритті до того часу, коли покинути уражену зону стане безпечніше. З часом потужність випромінювання слабшає, тож навіть після 24 годин ви зазнаєте меншої дози опромінення, ніж одразу після вибуху [1].

Подбайте про засоби індивідуального захисту. Захищайте очі й органи дихання за допомогою масок, респіраторів та окулярів. Усіляко запобігайте потраплянню радіоактивного пилу на шкіру й усередину тіла. Якщо перебуваєте в укритті, то за змогою обережно зніміть верхній шар одягу й вимийте всі частини тіла, які були відкритими. Перевдягніться в чистий одяг. Споживайте лише герметично запаковану воду та їжу.

Відповідно до викладу матеріалу запропоновано основні заходи захисту населення від застосування тактичної ядерної зброї. Проаналізовано дії центральних органів виконавчої влади щодо організації реагування під час ліквідації наслідків із застосуванням ядерної зброї.

Література

1. Радіаційний, хімічний та біологічний захист Частина 2. Радіаційний захист: / В.Б. Лоїк, Р.Т. Ратушний, О.Д. Синельніков, М.О. Довгановський, Р.С. Яковчук, А.Б. Тарнаський Навчальний посібник – Львів: Львівський державний університет безпеки життєдіяльності, 2022. – 589 с.
2. Зброя масового ураження та захист від неї. Навчальний посібник. /Б. П. Теплоухов. — Київ: Вид. дім «СКІФ», 2023. — 101 с.

3. Наказ Державного комітету ядерного регулювання України, Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 17.05.2004 року № 87/211 «Про затвердження Плану реагування на радіаційні аварії».

УДК 614.84

57.ЩОДО ВИКОРИСТАННЯ ТА КОНСТРУКЦІЇ ШЕСТЕРЕННОГО НАСОСУ ДЛЯ ГАСІННЯ ПОЖЕЖ

Назаренко С.Ю.[1], Мандриченко Д.С.[1]

1 Національний університет цивільного захисту, Україна
E-mail: itaart.nazarenko@gmail.com

Concerning the use and design of a gear pump for fire extinguishing

The work considers the principle of operation, design and characteristic malfunctions of gear pumps

Застосування гідравлічних машин набуло широкого поширення у всіх галузях машинобудування. Рік за роком збільшується число різновидів гідравлічних машин.

Стало абсолютно очевидно, що застаріла вітчизняна база комплектуючих виробів вже не придатна для створення сучасних машин, а вихід на світовий ринок неможливий без застосування нових технології.

У різних галузях машинобудування поряд з іншими типами гідравлічних насосів широко застосовуються шестеренні насоси (НШ). Значною мірою цьому сприяє експлуатаційна надійність НШ, невисока вимогливість щодо догляду за ними, простота реверсування, компактність, мала вага і невелика вартість, що вигідно відрізняє їх від інших типів об'ємних гідронасосу.

Відомо, що НШ є найбільш поширеним видом гідравлічних машин. Вони широко застосовується в різних галузях народного господарства, зокрема технологічному обладнанні гірничодобувної, нафтової та хімічної галузі, в автомобілебудуванні, верстатобудуванні, а також в машинах і обладнанні аграрного та сільського господарства, а також шестеренчасті насоси використовуються для гасіння пожеж (НШН-600).

Можливі причини несправностей насосів НШ:

- насос не нагнітає або нагнітає в недостатній кількості, немає тиску;
- насос НШ не розвиває максимальний тиск;
- перегрів гідравлічного насоса при роботі;
- витік води з приводного валу насоса;
- мимовільне вимикання насоса НШ;

- пошкодження корпусу насоса НШ - здуття, тріщини, пробоїни, протікання

- вібрація, шум при роботі насоса НШ, швидкий знос підшипників насоса, наявність повітря в гідросистемі.

Залежно від типу зачеплення шестеренні насоси можуть бути двох типів - зовнішніми і внутрішніми, що застосовуються у всіх галузях машинобудування. Найпростішим видом шестеренних насосів є пристрій з зовнішнім зачепленням. Воно являє собою конструкцію, що складається з корпусу і двох зубчастих коліс. Ці колеса знаходяться в зачепленні і відрізняються своєю евольвентностю.

Шестеренні насоси та гідромотори завдяки простій конструкції і надійності в роботі широко поширені в гідроприводах дорожніх машин. На рис. 1.2 показано схема шестеренного насоса.

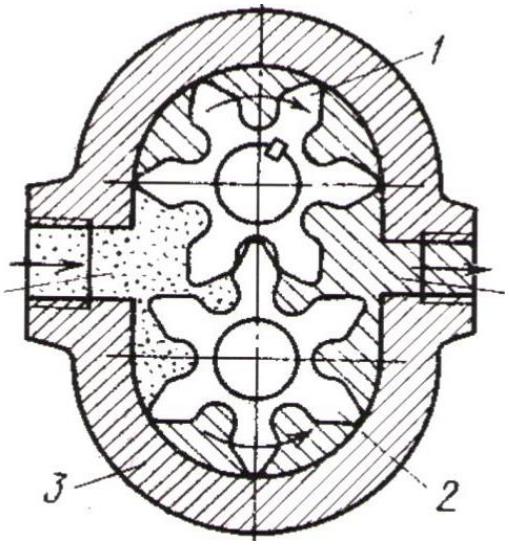


Рис. 1. Схема шестеренного насоса: 1, 2 – шестерні; 3 – корпус

Принцип дії шестеренного насоса полягає в наступному.

Дві шестерні рівної ширини ведуча 1 і ведома 2 знаходяться в зачепленні і розташовані в корпусі 3 з мінімальним радіальним зазором. До торцевих поверхнях шестерень прилягають бічні стінки насоса. При обертанні шестерень рідина, що заповнює западини між зубами, переноситься шестернями по внутрішній поверхні корпусу (показано стрілками) з порожнини всмоктування А в порожнину нагнітання Б.

Об'ємний ККД в основному залежить від витоків робочої рідини через зазори, утворені головками зубів і корпусом насоса, а також між торцевими поверхнями шестерень і бічними стінками корпусу. Крім того, додатково виникають витоку по лінії контакту зубів. Щоб зменшити радіальні витоку, зазор між шестернями і корпусом насоса роблять мінімальним, а для зниження торцевих витоків бічні стінки автоматично притискаються до торцевих поверхонь шестерень рідиною під робочим тиском.

Конструкція насоса шестеренного, що складається з корпусу, двох зубчастих колес і двох опорних втулок. Недоліком конструкції є те, що опорні

втулки в отворах корпусу насоса встановлені у вільному положенні, що призводить до утворення зазорів між корпусом насоса і опорними втулками і до зниження продуктивності, точності, ККД і ресурсу роботи насоса шестеренного. Виконаний аналіз конструкції існуючих насосів шестеренних диктує необхідність підвищення довговічності і ресурсу роботи елементів насоса, а також підвищенні точності роботи насоса, продуктивності і ККД шляхом створення і вдосконалення конструкції і технології виготовлення.

УДК 614.843/083

58.ВИМІРЮВАЛЬНИЙ КОМПЛЕКС ДЛЯ ВИЗНАЧЕННЯ ГІДРАВЛІЧНОГО ОПОРУ В НАПІРНИХ ПОЖЕЖНИХ РУКАВАХ

Назаренко С.Ю.[1], Шаповалов М.М.[1]
1 Національний університет цивільного захисту, Україна
E-mail: itaart.nazarenko@gmail.com

Measuring complex for determining the hydraulic resistance of pressure fire hoses

The problematic issues of determining the hydraulic resistance of pressure fire hoses and its reduction when various additives are introduced into the water flow are considered, and a measuring complex for determining the hydraulic resistance of pressure fire hoses is considered

Вирішення проблеми підвищення ефективності систем подачі води до осередку пожежі та створення науково обґрунтованої методики гідравлічного розрахунку необхідного для підвищення рівня пожежної безпеки, правильного визначення необхідного напору пожежних насосів, оптимальної розробки планів пожежогасіння та загалом для зниження соціальних та економічних наслідків пожеж.

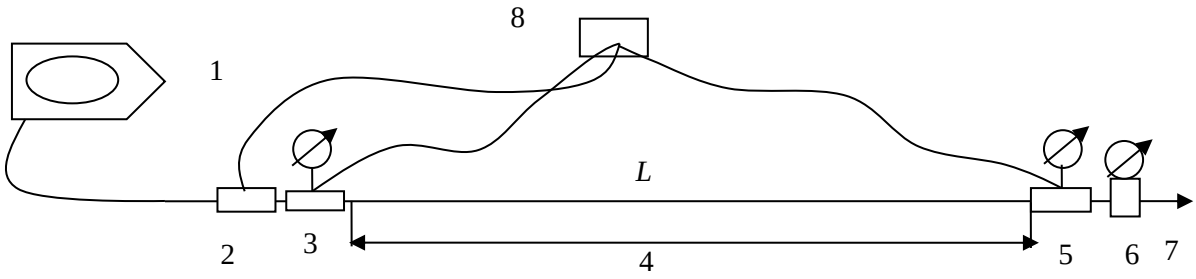
Одним із основних елементів систем пожежогасіння є напірні пожежні рукави (НПР). Гідравлічний розрахунок втрат напору під час руху води в рукавах виконується на підставі довідкових даних [1], які були визначенні в 90-х роках. У наявних довідниках даються постійні значення опору пожежних рукавів, тобто передбачається робота рукавів у квадратичній області у всьому практично значимому діапазоні чисел Рейнольдса. Проте в ранніх роботах є відомості про те, що НПР найчастіше працюють у проміжній області опору.

У кількісному відношенні роботи істотно розходяться, що підтверджує помітну залежність гідравлічного опору рукавів від матеріалів, з якого виготовлений рукав, і технології виготовлення, відхилень розмірів, що допускаються, в першу чергу діаметра рукава. Тому для НПР, що знаходяться в експлуатації потрібно досить точне визначення гідравлічного опору. Так в роботі

пропонується розглянути експериментальну установку для визначення гідравлічного опору в напірних пожежних рукавів, які наведено на рис.1 та 2.

Перша схема розімкнена (рис. 1). Подача здійснювалася автоцистерною. Вода або розчин прокачувалися через вставки з датчиками, пожежний рукав та виливалась у каналізацію. На виході встановлювалися стволи з насадками 9 мм, 12 мм, 16 мм і здійснювався вільний вилив з рукава. Розчин готувався безпосередньо у цистерні шляхом додавання у воду 20 та 25 л піноутворювача.

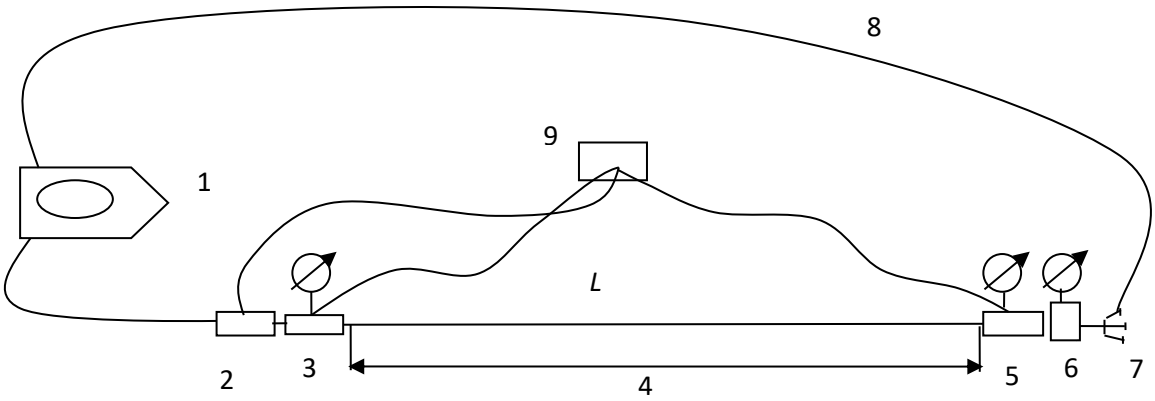
Друга схема замкнута (Рис. 2). Вода або розчин подавалися пожежним насосом з цистерни і після проходження через вимірювальні ділянки та випробуваний рукав по рукавній лінії надходили назад до цистерни.



1 – автоцистерна;
2 – вставка витратоміром;
3, 5 – вставки з датчиками тиску та різниці тиску;
4 – напірний пожежний рукав;
6 – контрольний вимір витрати та тиску;
7 – пожежний ствол;
8 – регістратор РМТ 59

Рис. 1. Розімкнена схема випробувань

Використовувалася дросельне регулювання подачі насоса вентилем на розгалуженні 7 та регулювання шляхом зміни кількості обертів насоса. Робота комплексу контролювалася за витратоміром та манометром 6 (Flowmaster 250), встановленому після вимірювальної вставки 5, показання манометрів на вставках 3 і 4 і показання манометра на пожежному насосі 1.



1 – автоцистерна;
2 – вставка витратоміром;
3, 5 – вставки з датчиками тиску та різниці тиску;
4, 8 – напірний пожежний рукав;
6 – контрольний вимір витрати та тиск
7 – розгалудження;
8 – регістратор РМТ 59

Рис. 2. Зімкнена схема випробувань

Таким чином розроблено експериментальну установку для визначення гідравлічного опору в НПР.

Література

1. Довідник керівника гасіння пожежі [http://repositsc.nuczu.edu.ua/bitstream/123456789/9477/2/Persha_redakciya_dovidnika_KGP_2.pdf] - Затверджено: від 2016 р.

УДК 614.8

59.ЗАСТОСУВАННЯ СВІТЛОПРОЗОРИХ ПЕРЕГОРОДОК ДЛЯ ОБМЕЖЕННЯ РОЗПОВСЮДЖЕННЯ ПОЖЕЖІ БУДІВЛЯМИ ТОРГІВЕЛЬНО-РОЗВАЖАЛЬНИХ ЦЕНТРІВ

Пічугін М.А.[1], Виноградов С.А.[1]

1 Національний університет цивільного захисту України
E-mail: vynogradovs@gmail.com

Use of transparent partitions for fire spread limitations in shopping and entertainment centers

The peculiarity of the structure of the buildings of shopping and entertainment centers and their fire hazard are considered. The possibility of using transparent partitions in the form of fire-resistant or tempered glass to limit the spread of fire in such buildings is discussed. The main problems and perspectives of research was be highlighted.

Торговельно-розважальний центр (ТРЦ) – різновид торговельного центру (ТЦ), який також може розміщуватися у різних будівлях комплексу або в одній багатофункціональній будівлі, до складу якої, крім об’єктів торговельного призначення та додаткового обслуговування, включають об’єкти культурно-видовищного, розважального та фізкультурно-спортивного призначення (кінотеатри, боулінг, фізкультурно-спортивний зал, ковзанка, плавальний басейн, фітнес тощо), а також службові, побутові та допоміжні приміщення персоналу [1].

Аналіз пожеж в таких будівлях показує, що хоча їх і невелика кількість, вони несуть значні матеріальні збитки і загибель людей. Тому велику увагу приділяють поділенню таких приміщень на протипожежні відсіки за для зменшення розповсюдження пожежі. Такі функції можуть виконувати об'ємно-планувальні рішення у вигляді багатосвітового приміщення (атріум), що ділить будинок на частини по всій довжині та висоті будівлі центру (рис. 1). Атріум – частина об’єму будинку у вигляді багатосвітлового простору, розвинутого по вертикалі з галереями на поверхах, на які виходять приміщення різного призначення [2].

Однак слід пам'ятати, що при експлуатації будівель у багатосвітніх приміщеннях (атріуми) не рідко розміщують різне пожежне навантаження, створюючи умови розповсюдження пожежі по всій будівлі. Найчастіше пожежне навантаження у багатосвітніх приміщеннях (атріуми) представлене у вигляді об'єктів острівцевої торгівлі.

Рис. 1. Внутрішній вигляд сучасного торговельно-розважального центру

Одним із способів обмеження розповсюдження пожежі по будівлі з багатосвітніми приміщеннями (атріум) є застосування протипожежних перегородок для відокремлення приміщень різного функціонального призначення від багатосвітового приміщення (атріум). Такі перегородки можуть бути виконані із світлопрозорого матеріалу (скла), що забезпечить максмальну

відкритість (прозорість), візуально збільшує торговельну зону [3]. З метою забезпечення пожежної безпеки такі перегородки повинні бути вогнестійкими.

Основними недоліками використання вогнестійкого скла є його висока ціна, складність монтажних робіт та заміна самого скла через його значну вагу. Вага скла з межею вогнестійкості внаслідок втрати цілісності та теплоізолюючої здатності за температурою (EI) знаходиться в діапазоні 35–50 кг/м2, а в окремих випадках сягає 110 кг/м2. Як альтернатива, у якості заміни вогнестійкому склу можна застосовувати загартоване скло. Популярність цього виду скла полягає в тому, що даний вид скла є дешевшим порівняно з вогнестійким склом, безпечним для людей при його руйнуванні і межа вогнестійкості такого скла вища, ніж у звичайного листового. Проте на сьогоднішній день не встановлені науково-обґрунтовані вимоги до ширини багатосвітового приміщення (атріум) як до протипожежної перешкоди, що обмежує поширення пожежі з використанням загартованого скла.

Література

1. ДБН В.2.2-23:2009 «Будинки і споруди. Підприємства торгівлі». – К.: Мінрегіонбуд, 2009. – 59 с.
2. ДБН В.2.2-9:2018 «Будинки і споруди. Громадські будинки та споруди. Основні положення». - К.: Мінрегіонбуд, 2019. – 43 с.
3. Катріченко, К. О.; Кривуц, С. В.; Скороходова, А. В. Сучасні тенденції використання акрилового скла в рішенні дизайну середовища. Науковий вісник будівництва, 2016, 2: 98-105.

УДК 621.396.4

60.АНАЛІЗ ПРИКЛАДНИХ ПРОГРАМ CFD ТА FEM З ЇХНЬОЮ ХАРАКТЕРИСТИКОЮ ДЛЯ КАБЕЛЬНИХ ТУНЕЛІВ

Самченко Т. В.[1], Нуянзін О.В. [2],

1 Інститут державного управління та наукових досліджень з цивільного захисту, Київ, Україна
2 Черкаський інститут пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного, Черкаси, Україна
E-mail: sam4enkotv@ukr.net, nuianzin_oleksandr@chipb.org.in

Analysis of applied cfd and fem programs with their characteristics for cable tunnels

The report presents the analysis of CFD and FEM applications with their characteristics and the selection of a specific software package depending on the characteristics of the combustion processes in the simulated cable tunnels, the capabilities of the computer and the user.

Розглянемо комп’ютерні програми, що найчастіше використовують дослідники у провідних країнах світу у своїх роботах для гасіння пожеж у кабельних тунелів [1-16].

ANSYS – універсальна програмна система кінцево-елементного аналізу, існує і розвивається протягом останніх 30 років, є досить популярною у фахівців у сфері автоматичних інженерних розрахунків (CAE, Computer-Aided Engineering) рішення лінійних і нелінійних, стаціонарних і нестаціонарних просторових задач механіки деформованого твердого тіла і механіки конструкцій (включаючи нестаціонарні геометрично і фізично нелінійні задачі контактної взаємодії елементів конструкцій), задачі механіки рідини і газу, теплопередачі і теплообміну, електродинаміки, акустики, а також механіки зв'язаних полів. Моделювання і аналіз в деяких областях промисловості дозволяє уникнути дорогих і тривалих циклів розробки типу «проектування – виготовлення – випробування». Система працює на основі геометричного ядра Parasolid, що представлено в [17].

Програмна система кінцево-елементного аналізу ANSYS розробляється американською компанією ANSYS Inc. Компанія також випустила інші системи кінцево-елементного моделювання, в тому числі Design Space, AI Solutions (NASTRAN, ICEM CFD); призначені для використання в більш специфічних галузях виробництва.

Як стратегічний партнер фірма співпрацює з багатьма компаніями, допомагаючи їм провести необхідні зміни. Запропоновані фірмою ANSYS Inc. засоби чисельного моделювання та аналізу сумісні з деякими іншими пакетами, працюють на різних ОС. Програмна система ANSYS сполучається з відомими CAD-системами Unigraphics, CATIA, Pro/ENGINEER, Solid Edge, Solid Works , Autodesk Inventor та деякими іншими [18].

Програмна система ANSYS є досить відомою CAE-системою, яка використовується на таких відомих підприємствах, як ABB, BMW, Boeing, Caterpillar, Daimler-Chrysler, Exxon, FIAT, Ford, БелАЗ, General Electric, Lockheed Martin, MeyerWerft, Mitsubishi, Siemens, Alfa Laval, Shell, Volkswagen - Audi та ін.

ANSYS дозволяє вирішувати завдання в наступних областях:

• міцність

• теплофізика

• електромагнетизм.

ANSYS ICEM CFD - потужний сітковий генератор для побудови як структурованих так і неструктурованих розрахункових сіток. Підтримує імпорт вихідної геометрії з різних CAD-продуктів і, крім того, має широкий набір функцій для її виправлення та доопрацювання. Також має ряд методів для побудови неструктурованих розрахункових сіток (тріангуляція Делоне, метод Octree, метод просування фронту). У поєднанні з інструментами локального змінення розмірів осередків, вони дозволяють домогтися високої якості розрахункової сітки практично для будь-якої форми досліджуваного об'єкта.

ANSYS ICEM CFD дозволяє будувати блочно-структуровані розрахункові сітки, які, як відомо, краще неструктурованих для деяких типів розрахунків (надзвукові і гіперзвукові течії). Процес побудови структурованих сіток заснований на технології трансфінітної інтерполяції і полягає в створенні блокової структури, асоціації блокової структури з вихідної геометрією і завдання згущення [19, 20].

Перша версія FDS офіційно була випущена в лютому 2000 року. На сьогоднішній день приблизно половина додатків моделі служить для проектування систем управління димом і вивчення активації спринклерів і детекторів. інша половина служить для відновлення картини пожежі в житлових і промислових приміщеннях.

Основною метою FDS протягом свого розвитку було рішення прикладних задач пожежної безпеки та в той же час забезпечення інструментом для вивчення фундаментальних процесів при пожежі.

Програма FDS (Fire Dynamics Simulator) реалізує обчислювальну гідродинамічну модель (CFD) тепломасопереносу при горінні. FDS чисельно вирішує рівняння Нав'є-Стокса для низькошвидкісних температурно-залежних потоків, особлива увага приділяється поширенню диму і теплопередачі при пожежі.

Smokeview (SMV) - програма для візуалізації результатів розрахунків FDS.

Програми Fire Dynamics Simulator і Smokeview розроблені Національним інститутом стандартів і технології (НІСТ) міністерством торгівлі США за сприяння Технічного науково-дослідного центру VTT (Фінляндія).

FDS і Smokeview - безкоштовне програмне забезпечення. Відповідно до Кодексу США Глава 17 Частина 105 авторські права розробників не захищені, програма є загальнодоступним ПО. НІСТ не несе ніякої відповідальності за використання будь-яких версій вихідних кодів програми, документації або виконуваних файлів і не дає явних або непрямих гарантій на її якість, надійність або інші властивості.

FDS - не проста комп'ютерна програма, що працює за принципом "вказівки і клацання". FDS необхідно запускати з командного рядка, а вхідні параметри повинні бути записані в текстовий файл [21].

FLOW-3D – це CFD пакет загального призначення здатний моделювати різноманітні потоки рідини. Хоча спеціалізацією вищезазначеного даного програмного комплексу є моделювання течій з вільною поверхнею, але FLOW-3D є програмою для моделювання обмежених внутрішніх течій [22].

У даній програмі FLOW-3D є пакет «все включено», який не вимагає жодних додаткових програм. Графічний інтерфейс користувача поєднує постановку завдання (включаючи створення/імпорт геометрії і генерацію сітки), рішення і обробку результатів, пропонуючи також кілька корисних утиліт, як: переглядач STL файлів, розрахунків і засоби контролю над ходом розрахунку.

Відмінні риси FLOW-3D.

По-перше, FLOW-3D – це програмний комплекс для створення сітки, який використовує підхід та віддає переваги простій прямокутній сітці з гнучкістю

деформованих сіток. Такий підхід називається “вільне формування сітки” оскільки сітка і геометрія може бути вільно змінені незалежно одна від одної. FLOW-3D використовує фіксовану сітку з ортогональних елементів, що спрощує генерацію і забезпечує багато корисних властивостей (наприклад, регулярність покращує точність, зменшує вимоги до пам'яті, полегшує чисельну апроксимацію).

По-друге, FLOW-3D включає в себе спеціальну техніку, яка включає в себе FAVOR™ (Fractional Area Volume Obstacle Representation) метод, що використовується для опису прямокутної геометричної сітки в довільній формі. Філософія FAVOR™ полягає в тому, що чисельні алгоритми в методі кінцевих обсягів базуються на інформації, що включає лише одне значення тиску, швидкості і температури кожного з елементів, тому було б нелогічно використовувати докладнішу інформацію для опису геометрії.

По-третє, основною особливістю що відрізняє FLOW-3D, від інших CFD програм у його методі обробки поверхні поточної рідини. Ця програма використовує спеціальні чисельні методи для відстежування становища поверхонь й у правильному застосуванні ними граничних умов. У FLOW-3D, вільні поверхні моделюються за допомогою методу кінцевих обсягів Volume of Fluid (VOF). Деякі з конкурентних CFD програм наголошують на впровадженні VOF методу, хоча реально вони використовують тільки одну чи дві із трьох фундаментальних складових VOF методу [22].

Висновки

Запропоновано програму більш прийнятною для побудови математичної моделі кабельного тунелю є «Fire Dynamic Simulator 6.2». По-перше, базовими в ній є рівняння Нав’є – Стокса, що описують рух рідин і газів у широкому діапазоні чисел Рейнольдса. По-друге, система дає змогу побудувати геометрію об’єкта без використання спеціальних CAD-програм. По-третє, система «FDS» уможливлює легке корегування параметрів тунелю та граничних умов. По-четверте, система «FDS» має розвинений апарат візуалізації отриманих результатів.

Проаналізовано можливість використання математичних моделей, що дають змогу ефективно змоделювати процес тепломасопереносу у кабельному тунелі.

Література

1. ГБН В. 2.2-34620942-002:2015. Лінійно-кабельні споруди телекомунікацій. Проектування.
2. Постанова Верховної ради України «Про Основні напрями державної політики України у галузі охорони довкілля, використання природних ресурсів та забезпечення екологічної безпеки» (Відомості Верховної Ради України (ВВР), 1998, N 38-39, ст.248.
3. Мала гірнича енциклопедія : у 3 т. / за ред. В. С. Білецького. — Д. : Східний видавничий дім, 2004 –2013.
4. ДНАОП 0.00-1.32-01 Правила будови електроустановок. Електрообладнання

спеціальних установок.
5. СНиП 3.05.06-85 Электротехнические устройства.
6. Hsu W. S. et al. Analysis of the Hsuehshan Tunnel Fire in Taiwan //Tunnelling and Underground Space Technology. – 2017. – Т. 69. – С. 108-115.
7. Ji J. et al. Influence of aspect ratio of tunnel on smoke temperature distribution under ceiling in near field of fire source //Applied Thermal Engineering. – 2016. – Т. 106. – С. 1094-1102.
8. Niu Y., Li W. Simulation Study on Value of Cable Fire in the Cable Tunnel //Procedia Engineering. – 2012. – Т. 43. – С. 569-573.
9. Zhao Y., Zhu G., Gao Y. Experimental Study on Smoke Temperature Distribution under Different Power Conditions in Utility Tunnel //Case Studies in Thermal Engineering. – 2018.
10. Tian X. et al. Full-scale tunnel fire experimental study of fire-induced smoke temperature profiles with methanol-gasoline blends //Applied Thermal Engineering. – 2017. – Т. 116. – С. 233-243.
11. Modic J. Fire simulation in road tunnels //Tunnelling and underground space technology. – 2003. – Т. 18. – №. 5. – С. 525-530.
12. Vaari J. et al. Numerical simulations on the performance of water-based fire suppression systems //VTT Technol. – 2012. – Т. 54.
13. Brahim K. et al. Control of Smoke Flow in a Tunnel //Journal of Applied Fluid Mechanics. – 2013. – Т. 6. – №. 1.
14. Zhong W. et al. A study of bifurcation flow of fire smoke in tunnel with longitudinal ventilation //International Journal of Heat and Mass Transfer. – 2013. – Т. 67. – С. 829-835.
15. Sun J. et al. Experimental study of the effectiveness of a water system in blocking fire-induced smoke and heat in reduced-scale tunnel tests //Tunnelling and Underground Space Technology. – 2016. – Т. 56. – С. 34-44.
16. Zhang P. et al. Experimental study on the interaction between fire and water mist in long and narrow spaces //Applied Thermal Engineering. – 2016.. – С. 706 - 714.
17. Басов К. А. ANSYS и LMS Virtual Lab. Геометрическое моделирование. ДМК Пресс, 2006. – С. 240.
18. Методи математичного моделювання теплових процесів при випробуваннях на вогнестійкість залізобетонних будівельних конструкцій / Нуянзін О. М., Некора О. В., Поздєєв С. В. [та ін.] // Монографія. Черкаси: ЧІПБ ім. Героїв Чорнобиля НУЦЗ України, - 120 с.
19. Ansys Release 10, inc. Theory Reference.
20. Milarcik E. L An Analysis of the Performance of Residential Smoke Detection Technologies Utilizing the Concept of Relative Time / E. L. Milarcik, S. M. Olenick, R. J. Roby // The National Fire Protection Research Foundation Suppression and Detection Research and Applications Symposium (SUPDET), March, 2007. (2007 Carey award).
21. Ellen Eberhardt. "PNW - Fire and Environmental Research Applications Team (FERA) Research/Studies.
22. Anthony J. Lockwood, «Editors Pick: Flow Science Release FLOW-3D Version 10.0», Desktop Engineering, August 9, 2011.

УДК 614.84

61.СИСТЕМНИЙ ПІДХІД ДО ОЦІНКИ РІВНЯ ГОТОВНОСТІ ПІДРОЗДІЛІВ ОРС ЦЗ

Калиновський А.Я. [1], Свєрчков О.В. [1]

1 Національний університет цивільної захисту України
E-mail: ugzu.iart@gmail.com

A systematic approach to assessing the level of readiness of units of the operational rescue service of civil protection

The theoretical and practical significance of problematic issues related to the improvement of the assessment of the level of preparedness of operational and rescue units of the civil protection service for extinguishing fires, as the most important direction of increasing the efficiency of its activities, ensuring comprehensive protection of life and health of people, property, society and the state from fires

In order to find regularities in the process of functioning of the operational rescue service of civil protection, it is necessary to have reliable initial information about this process. First of all, the official documents of the fire protection of cities, settlements and objects can serve as an information base here.

The obtained information should be processed using appropriate scientific methods. It is important not only to find the value of the values that interest us, but also to find out the nature of their change over time, their dynamics, as this will allow us to build fairly reliable forecasts of changes in the operational situation and the corresponding development of the operational and rescue service of civil protection.

Теоретична та практична значимість проблемних питань, пов’язаних із удосконаленням оцінки рівня готовності підрозділів оперативно-рятувальної служби цивільного захисту (ОРС ЦЗ) до гасіння пожеж, як найважливішого напряму підвищення ефективності її діяльності, забезпечення всебічного захисту життя та здоров’я людей, майна, суспільства та держави від пожеж.

Під оперативною обстановкою у місті розуміється комплекс умов, що склався у ньому в той чи інший період часу, які сприяють чи перешкоджають виникненню, розвитку та ліквідації пожеж та інших надзвичайних ситуацій і таких, що визначають можливі масштаби їх соціально-економічних наслідків.

Останнім часом концепція поняття оперативної обстановки із пожежами, питання її аналізу та моделювання докладно вивчалися з позицій системного підходу. Сутність цієї концепції полягає у тому, що ОРС ЦЗ можна представити як складну динамічну систему, покликану виконувати цілком певні функції, пов’язані з попередженням і гасінням пожеж. Для виконання цих функцій підрозділи ОРС ЦЗ мають у своєму розпорядженні відповідні матеріальні та трудові ресурси (сили та засоби).

ОРС ЦЗ функціонує в деякому навколишньому середовищі, де виникають ті чи інші пожежонебезпечні ситуації. Ліквідуючи ці ситуації, пожежно-рятувальні підрозділи вступають у взаємодію з відповідними елементами навколишнього середовищ. Вона може бути більш менш успішним залежно від ряду факторів як випадкового, так і невипадкового характеру (керованих або некерованих). Звідси, зокрема, випливає важлива можливість оцінки ефективності функціонування підрозділів ОРС ЦЗ, тобто ступеня її пристосованості до виконання, поставлених перед нею завдань.

Запропонована концепція дозволяє виділити основні елементи поняття оперативної обстановки, визначити фактори, що належать до кожного елемента, намітити параметри, що характеризують оперативну обстановку в цілому та її елементи, а також знайти шляхи їхньої кількісної оцінки.

Так, основними елементами та факторами, що характеризують поняття оперативної пожежної обстановки, є:

1. Можливості ОРС ЦЗ міста (характеристики системи):

• чисельність особового складу (пожежно-рятувального та профілактичного);
• професійна підготовка особового складу;
• умови роботи профілактичного складу;
• готовність до дій за призначенням оперативних підрозділів;
• кількість оперативних відділень на пожежних автомобілях;
• якість та стан пожежної техніки;
• загальна технічна оснащеність підрозділів ДСНС міста;
• дислокація пожежно-рятувальних підрозділів;
• розклад виїздів підрозділів ОРС ЦЗ;

2. Рівень пожежної небезпеки міста (характеристики середовища):

• чисельність та щільність населення;
• площа територій міста;
• загальний економічний потенціал, його складові;
• характер міської забудови;
• ступінь вогнестійкості будівель;
• ступінь благоустрою міста (водопостачання, опалення, дороги та ін.);
• загальна кількість об’єктів економіки;
• наявність об’єктів підвищеної небезпеки;
• кліматичні та погодні умови.

3. Динаміка оперативного реагування підрозділів ОРС ЦЗ на пожежонебезпечні ситуації (взаємодія системи та середовища):

• обсяг та рівень виконання пожежно-профілактичної роботи;
• час прибуття першого та наступних підрозділів до місця виклику;
• рівень використання різноманітних методів, способів та засобів гасіння пожеж;
• рівень взаємодії з іншими службами міста;
• характеристика ефективності діяльності ОРС ЦЗ (величини матеріальних збитків від пожеж та врятованих матеріальних цінностей та ін.).

Поняття оперативної обстановки, таким чином, є складним та багатогранним, що залежить від великої кількості різних за характером факторів. Всі ці численні чинники впливають на загальну оцінку оперативної обстановки в місті, рівень його пожежної небезпеки та на розробку планових заходів щодо подальшого вдосконалення системи забезпечення пожежної безпеки міста.

У цьому вся сукупність чинників знаходить досить об'єктивне свій відбиток у кількох параметрах, які піддаються кількісної оцінці і дозволяють знайти кількісні закономірності оперативної діяльності підрозділів ОРС ЦЗ. Такими параметрами є:

- частота виїздів, для виконання дій за призначенням, підрозділів ОРС ЦЗ;
- тривалість виїздів;
- кількість оперативних пожежно-рятувальних підрозділів (відділень), які виїжджають на виклик.

Ці параметри є основними. До них можна додати багато інших, наприклад кількість пожежних рукавів, використаних, при гасінні пожежі, витрати різних вогнегасних засобів і т.д.

Вочевидь, що чим більше значення кожного перерахованого параметра, тим більше напружена оперативна обстановка в місті, і навпаки. На значення вищевказаних параметрів безпосередній вплив має більшість факторів, що становлять елементи оперативної обстановки. Наприклад, на частоту виїздів підрозділів на пожежі серед інших факторів значний вплив може чинити рівень пожежно-профілактичної роботи у місті. Тому до переліку параметрів оперативної обстановки цілком доречно включити, наприклад, кількість пожежно-технічних обстежень об'єктів, проведених за певний проміжок часу, та виявлені порушення вимог пожежної безпеки.

Сукупність параметрів оперативної обстановки дозволяє досить повно та точно оцінити обсяг оперативної та профілактичної роботи, яку доводиться виконувати підрозділам ДСНС. Чим частіше доводиться, наприклад, виїжджати оперативним підрозділам, чим довше і більшими силами ліквідуються пожежі, аварії та інші надзвичайні ситуації, що виникли, тим складніше оперативна обстановка, тим більший обсяг роботи виконують підрозділи пожежної охорони. Ці об'єктивні показники необхідно враховувати під час обґрунтування штатної чисельності та технічної оснащеності підрозділів ОРС ЦЗ.

Вивчення та аналіз елементів, факторів і параметрів оперативної обстановки допомагають визначити конкретні шляхи впливу на неї з метою розрядки та зменшення ступеня її напруженості. Наприклад, вивчення структури потоку виїздів пожежно-рятувальних підрозділів (на житлові будинки, на промислові підприємства, за хибними викликами тощо) і причин, що їх викликали, може вказати напрямок посилення профілактичної роботи, що дозволить зменшити загальну кількість викликів, зменшити кількість пожеж, підвищити пожежну безпеку міста чи населеного пункту. Підвищення рівня готовності до дій за призначенням підрозділів ОРС ЦЗ, більш якісна розробка оперативних планів можуть зменшити тривалість процесу гасіння пожеж,

знизити збитки від них. Великі значення часу прибуття першого підрозділу ОРС ЦЗ до місця виклику можуть призвести до зміни дислокації підрозділів, меж районів обслуговування, обґрунтованого збільшення числа пожежно-рятувальнх частин та окремих пожежних постів тощо.

Висновки

Результати дослідження оперативної обстановки, її параметрів дають ті вихідні закономірності, на основі яких можна розробляти математичні моделі процесу функціонування ОРС ЦЗ, причому параметри оперативної обстановки для цих моделей є вхідними параметрами. Такі моделі дозволяють розробити науково обґрунтовані нормативи та сформулювати рекомендації щодо вдосконалення організації оперативної діяльності пожежної охорони міст та населених пунктів.

Для пошуку закономірностей процесу функціонування ОРС ЦЗ необхідно мати достовірну вихідну інформацію про цей процес. Інформаційною базою тут можуть служити передусім офіційні документи пожежної охорони міст, населених пунктів та об’єктів (наприклад, диспетчерські журнали виїздів пожежно-рятувальних підрозділів). На жаль, далеко не завжди вдається отримати з цих документів досить повну та надійну інформацію, тому у ряді випадків доводиться проводити спеціальні спостереження та експерименти для збирання необхідної інформації.

Отриману інформацію слід обробити за допомогою відповідних наукових методів. В даному випадку найбільш підходящими є методи математичної статистики. Важливо не тільки знайти значення величин, що нас цікавлять (параметрів), а і з’ясувати характер їх зміни в часі, їх динаміку, оскільки це дозволить будувати досить надійні прогнози зміни оперативної обстановки та відповідного розвитку оперативно-рятувальної служби цивільного захисту.

УДК 621.391:004.94

62.ІМІТАЦІЙНА МОДЕЛЬ ПЕРЕДАВАННЯ ТЕКСТОВИХ І АУДІО ПОВІДОМЛЕНЬ З ВИКОРИСТАННЯМ НЕРОЗДІЛЬНОГО ФАКТОРІАЛЬНОГО КОДУВАННЯ В СЕРЕДОВИЩІ SIMULINK

Фауре Е. В., Скуцький А. Б., Лавданський А. О.
Черкаський державний технологічний університет
E-mail: a.b.skutskyi.asp21@chdtu.edu.ua

Simulation model for text and audio messages transmission in the Simulink environment using non-separable factorial coding

The work is devoted to the development of a model for text and audio messages transmission using non-separable factorial coding. The creation of a simulation model using Matlab and Simulink software products and the process of setting their parameters are considered. The algorithm for

encoding text messages and the algorithm for encoding samples of an audio signal are given. The resulting model makes it possible to investigate probabilistic indicators of the information exchange process as well as assess the impact of communication channel error on the quality of various types of messages (text or audio) reproduction. The use of the developed model is also necessary to create mock-up samples of secure information exchange devices based on non-separable factorial data coding.

Розвиток технічних можливостей, соціально-політичне становище, передові технології в сучасному житті людини диктують нові правила щодо парадигми безпеки в сферах людської діяльності. Використання нероздільного факторіального кодування (НФКД) як нової перспективної моделі криптозахисту відкриває новий етап розвитку сучасних програмних систем. Узагальнення моделей і методів НФКД викладено в [1].

Метою роботи є розробка та дослідження імітаційної моделі передавання даних на основі НФКД. Дані представлено у вигляді тексту та вибірок аудіо сигналу. Основою для роботи є імітаційна модель системи зв'язку, результати дослідження якої викладено в праці [2]. Канал зв'язку має ненульову ймовірність виникнення бітової помилки під час передавання текстової та аудіо інформації. Середовищем моделювання використано програмні продукти Simulink і Matlab [3], [4].

Складові компоненти розробленої моделі: підсистема *coder* – виконує відкриття та завантаження файлу до середовища моделювання, підготовку даних для кодування, кодування даних за заданим алгоритмом; підсистема каналу передавання даних – містить двійковий симетричний канал зв'язку; підсистема *decoder* – приймає дані з каналу зв'язку, декодує, форматує та приводить дані до початкового вигляду та зберігає їх до файлу.

Модель передавання текстових даних за допомогою НФКД створено адаптивною. Таким чином, загальний час симуляції інформаційного обміну базується на кількості даних, що необхідно передати, та мінімального значення часу симуляції. У моделі використано частоту передавання $F_{TX} = 100 МГц$, звідки мінімальне значення часу симуляції дорівнює $1/F_{TX} = 10^{-8} c$. Розв'язувач (*Solver*) обрано типу *Fixed-step: discrete (no continuous states*). Стоп симуляції процесу передавання текстових даних виконується тільки після того, як усі дані у вхідному файлі оброблено, передано, прийнято, декодовано та збережено в зовнішній файл.

Для моделювання процесу передавання аудіо даних використано розв'язувач типу *Variable-step.* Вхідні дані – вибірки аудіо сигналу – отримуються від периферії комп'ютера через мікрофоний/лінійний вхід та функціональні блоки Simulink Audio Toolbox (*Audio Device reader*). У режимі реального часу відбувається кодування та передавання цих даних каналом зв'язку, декодування та, за аналогією з моделлю обробки текстових даних, збереження до зовнішнього файлу (*To Multimedia file*).

У середовищі Matlab для реалізації необхідного алгоритму кодування створено додаткові сценарії для обробки даних: *coder.m, decoder.m, int2factStr.m,*

fact2int.m. Принципи обробки текстових повідомлень для їх факторіального кодування представлено в [5].

Розроблена імітаційна модель опрацьовує текстові дані за наступним алгоритмом:

1) зчитування ASCII символів з текстового документу;
2) конкатенація по два символи вхідного тексту (опрацювання тексту виконується зліва направо) та перетворення їх у перестановку довжини $M = 8$;
3) передавання даних каналом зв'язку з бітовими помилками;
4) зворотне перетворення перестановки в двійкові дані;
5) зберігання даних у зовнішній файл.

У випадку передавання аудіо повідомлення зазначений алгоритм опрацьовує вибірки аудіо сигналу в форматі Waveform Audio File Format (WAV) у моно режимі з розрядністю 16 біт на семпл.

Модель виконує збереження даних на кожному етапі обробки для подальшої статистичної оцінки вбудованими модулями *To File*. Вбудованими інструментами Simulink проведено аналіз впливу бітової помилки на якість отриманого повідомлення. Отримані модельні результати перевірено на відповідність теоретичним.

Висновки

Таким чином, у результаті проведеного дослідження розроблено та досліджено імітаційну модель, яка: опрацьовує текстову та аудіо інформацію, виконує кодування та передавання даних відкритим каналом зв'язку з незалежними бітовими помилками. Модель буде використано для аналізу показників передавання інформації, а також для розробки та дослідження макетних зразків приймально-передавальних пристроїв системи захищеного інформаційного обміну на основі НФКД.

Література

1. Основи теорії нероздільного факторіального кодування даних : монографія / Фауре Е.В. та ін. Харків : СГ НМТ Новий курс, 2021. 167 С.
2. Фауре Е.В., Скуцький А.Б., Лавданський А.О. Імітаційна модель системи передавання інформації з нероздільним факторіальним кодуванням даних у середовищі Simulink // Вісник Черкаського державного технологічного університету. Черкаси, 2022. № 4. С. 31-47.
3. Desmond J. H., Nicholas J. H. Matlab Guide. Third Edition. SIAM, 2017. 476 p.
4. Devendra. K. C. Modeling and simulation of systems using Matlab and Simulink. CRC press, 2017. 734 p.
5. Лавданський А.О., Фауре Е.В., Тинимбаєв С.Т., Скуцький А.Б. Система захищеного інформаційного обміну текстовими даними через радіоканал ISM-діапазону // Вісник Черкаського державного технологічного університету. Черкаси, 2022. № 3. С. 41-48.

УДК 664.7:621.3.

63.ТЕХНІЧНІ ЗАХОДИ ЩОДО ЗМЕНШЕННЯ ВТРАТ ЗЕРНА НА ЕТАПІ ЗБЕРІГАННЯ ВІД БІОТИЧНИХ ФАКТОРІВ

[1*]Черепньов І.А., [2]Вамболь С.О., [3]Барбара Савицька, [4,5]Париса Зіараті, [6]Барбара Крохмаль-Марчак

[1]Державний біотехнологічний університет, м. Харків, Україна
[2]Національний технічний університет «ХПІ», м. Харків, Україна
[3] Університет природничих наук у Любліні, Люблін, Польща
[4] ELIDAN genome SAS, 1 авеню дю Лісі, 77130 Монтеро Фулт-Йонн; Франція
[5] Кафедра медичної хімії, Тегеранські медичні науки, Університет Азад, Тегеран, Іран
[6] Прикарпатський державний коледж у Кросно, Кросно, Польща
*E-mail: *voenpred314@ukr.net*

Technical measures to reduce grain losses at the storage stage from biotic factors

The abstracts consider the main tasks that food stocks play in state reserves. Given that a significant part is grain, based on the analysis of literary sources, the main factors of storage losses, which include biotic and, above all, insect pests, are identified. Both traditional and alternative methods of their destruction have been studied. It is recognized that the most promising and environmentally safe are microwave technologies for processing grain before storage. Based on our own research, options are proposed to eliminate the existing shortcomings of electromagnetic disinfection of grain.

Проблема забезпечення населення продовольством в масштабах держави виникла практично одночасно з появою держав як таких. Як зазначено в роботі [1]:зберігання резервних запасів основних продуктів харчування так само стара, як цивілізація, і продовольчі запаси завжди були інструментом, використовуваним урядами. Стратегічні запаси продовольства зберігалися в Стародавньому Єгипті з 1750 р. до н. е.), Китай (використовується безперервно, з 498 р. н. е.) та за часів Римської імперії.

В даний час переважна більшість держав в структурі державного резерву мають значні запаси продовольства які виконують два основні завдання:

- стабілізація цін та / або ціновий контроль;
- продовольчі резерви для реагування на надзвичайні ситуації на всіх рівнях можуть використовуватися для вирішення надзвичайних ситуацій з поставками продовольства;

Крім того, запаси продовольчого зерна можуть сприяти довгостроковій продовольчій безпеці за рахунок стимулювання сільськогосподарського виробництва [2].

Як відомо, в загальному обсязі виробництва продуктів харчування зернові культури займають близько 50%, крім того, значна частина зерна використовується в тваринництві для відгодівлі сільськогосподарських тварин. Отже, постійне збільшення обсягів виробництва зерна та продуктів його переробки є важливим завданням, що стоїть перед науковими фахівцями та

практичними працівниками аграрного сектору виробництва не лише в Україні, а й за кордоном, тим більше, що саме зерно становить основу продовольчих резервів [3].

У всіх великих розвинених країнах провідною галуззю у виробництві сільгосппродукції є зернове господарство. Показово, що термін "продовольча безпека" був офіційно введений в міжнародну практику в 70-х роках після глибокої зернової кризи 1972-1973 рр. [4]. На рис.1 представлена структура валових зборів зерна в світі. Виходячи з початкових прогнозів ФАО світового виробництва зернових у 2022 році та їх використання в 2022/2023 році, запаси скоротяться на 0,4% відносно початкового рівня, тобто до 847 млн. т. При нинішніх рівнях застосування і прогнозах співвідношення світових запасів до споживання знизиться з 30,5% у 2021/2022 році до 29,6% у 2022/2023 році, що є найнижчим показником з сезону 2013/2014. Серед основних зернових культур зменшення запасів кукурудзи, як очікується, буде найзначнішим. Запаси ячменю і рису також скоротяться, в той час як обсяги щодо пшениці і сорго, ймовірно, збільшяться [5].

Як зазначено в роботі [6], зернові є основою основних продуктів харчування в більшості країн, що розвиваються, і на їх частку припадають максимальні післязбиральні втрати по калорійності серед усіх сільськогосподарських товарів. На етапі зберігання може бути втрачено до 50-60% зерна.

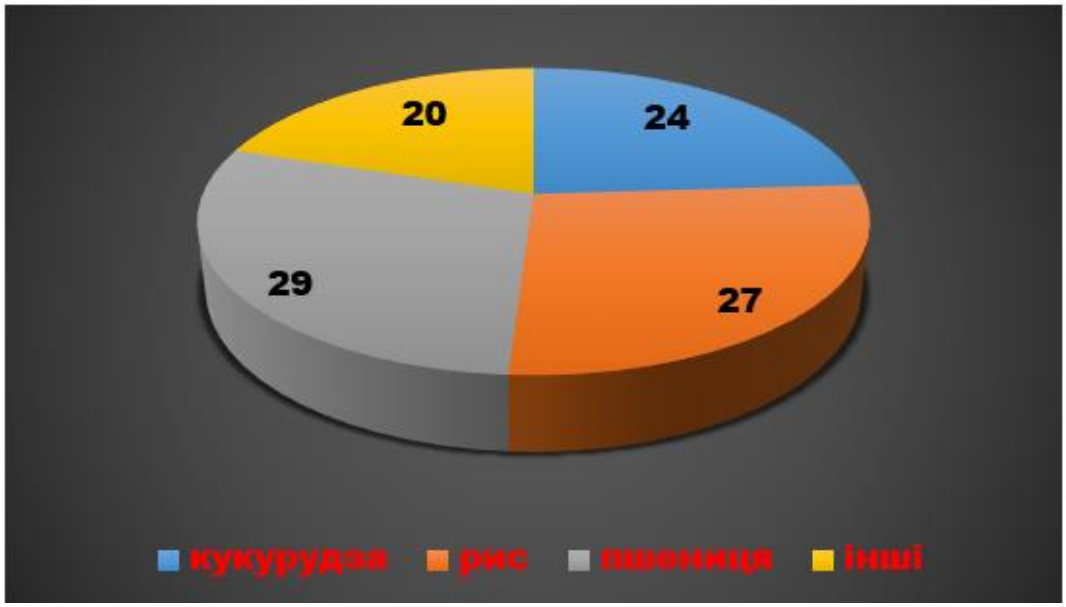


Рис.1 - Структура валових зборів зерна в світі:
кукурудза (24%), рис (27%) , пшениця (29%), інші (20%) [3].

На рис.2 представлені усереднені загальносвітові дані, що показують процентне співвідношення втрати зерна на різних циклах його виробництва [3]. За даними більшості фахівців серед всіх біотичних факторів комахи-шкідники

вважаються найбільш важливими і викликають величезні втрати зерна (30% - 40%) [6,7].

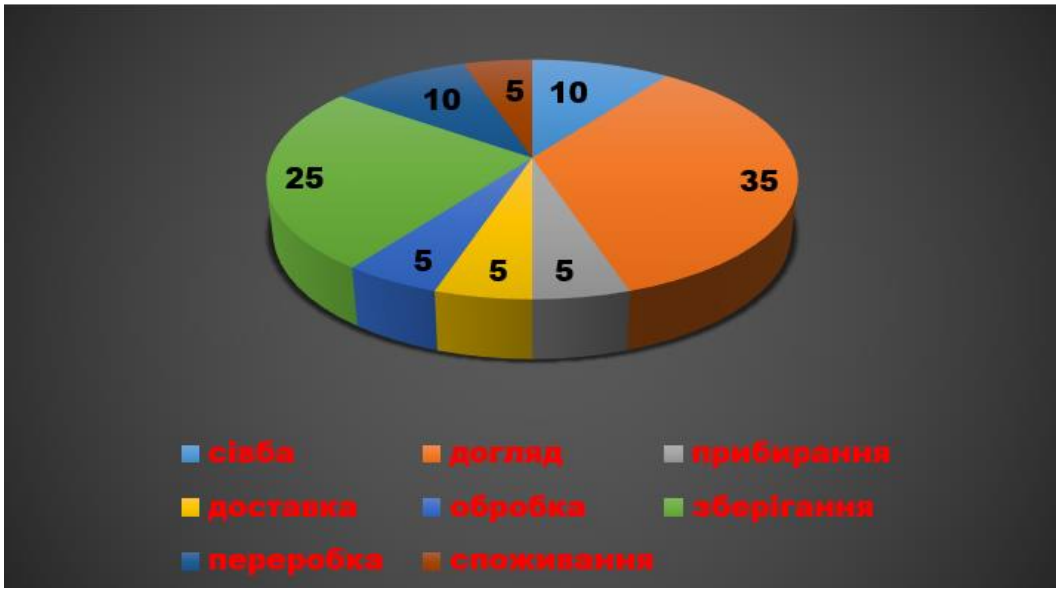


Рис.2- Процентне співвідношення втрати зерна на різних циклах його виробництва

Серед найбільш поширених методів знищення так званих комірних шкідників є хімічний. Зазвичай для боротьби зі шкідниками використовуються хімічні фуміганти, контактні інсектициди. Підвищення обізнаності про проблеми зі здоров'ям, пов'язані з органічними залишками в продовольчому зерні, призвело до обмеження використання хімічних пестицидів через несприятливий вплив залишків пестицидів на зерно та навколишнє середовище. Це призвело до суворих обмежень щодо реєстрації пестицидів регулюючими органами. Крім того, у багатьох країнах, зокрема, у комах розвивається стійкість до контактних інсектицидів і до традиційно використовуваного газоподібного фосфіну [8].

Починаючи з 80-х років XX століття і до теперішнього часу неодноразово проводилися дослідження по застосуванню мікрохвильовій обробці зерна перед закладкою його на зберігання. Дослідження, проведене на різних харчових продуктах, заражених великими комахами, показує, що повна смертність, тобто 100%, може бути досягнута за допомогою мікрохвильової енергії. Однак, поряд з позитивними результатами проявилися і недоліки даного методу, а саме [9]:

- мікрохвилі не підходять для сушіння пшениці, яка буде використовуватися в якості насіння, навіть при використанні низьких рівнів потужності;
- низька проникаюча здатність мікрохвиль при обробці сипучих зерен - не глибше 4 дюймів.

На думку авторів даних тез, ці недоліки цілком переборні. У роботі [11] запропоновано застосовувати імпульсні електромагнітні випромінювання, в результаті чого для знищення шкідників достатньо всього 2 секунд, протягом

яких зернова суміш не встигає розігрітися до неприпустимої температури. Крім того, як випливає з результатів досліджень наведених у роботі [12] тороїдальні антенні системи унікальні за своїми властивостями і гнучкості управління властивостями випромінювання і, завдяки цьому, знаходять широке застосування в різних галузях техніки. Вони дозволять здійснити генерацію хвиль поздовжньої поляризації і забезпечити проникнення електромагнітних випромінювань на значно більшу глибину. Безумовно потрібне проведення додаткових теоретичних та експериментальних досліджень для оптимізації мікрохвильової технології обробки зернової суміші.

Література

1. No More Food Crises: The Indispensable Role of Food Reserves. Alex Wijeratna. Food Reserves as Key to Preventing Food Crises. June 2011. 17 p. DOI:10.13140/RG.2.2.15358.43845.

2. W. Würdemann, Gerdien W. Meijerink, Marianne van Dorp Strategic food grain reserves. Desk review. J. Project Report. January 2011. Project code 8140006800 Wageningen UR Centre for Development Innovation. 34p.

3.Некоторые организационно-технические аспекты повышения продовольственной безопасности Украины / И.А. Черепнев та ін. *Вісник ХНТУСГ. Механізація с.-г. вир-ва та перероб. с.-г. продукції.* 2010. Вип. 103. С. 284-299.

4. Мостова А.Д. Стратегічне забезпечення продовольчої безпеки України: монографія. Харків: ХНТУСГ, 2019. 311 с.

5. Food Outlook – Biannual Report on Global Food Markets. *Food and Agriculture Organization* веб-сайт. URL: https://www.fao.org/publications/card/ru/c/CB9427EN/ (дата звернення 02.02 2023).

6. Reducing Postharvest Losses during Storage of Grain Crops to Strengthen Food Security in Developing Countries. Deepak Kumar, Prasanta Kalita. Foods 2017, 6(1).22 p. DOI:10.3390/foods6010008

7. Postharvest losses in food grains – A Review. Nura Abdullahi, Miner Abba Dandago. Turkish Journal of Food and Agriculture Sciences, 2021, № 3 (2): p. 25-36. Doi:10.53663/turjfas.958473

8. Food Grain Storage Practices-A Review. Prashant Said, Rama Pradhan. Journal of Grain Processing and Storage January-June, 2014.Vol. 1 Issue 1. P.01-05

9. Chandrasekaran S., Ramanathan S., Basak T. Microwave food processing. A review. Food Research International, 2013, V. 52, no. 1, pp. 243–261
doi.org/10.1155/2013/926468

10. Rasha Ahmed Zinhoum, Nilly A. H. Abdelfattah. Microwave energy as an alternative control method for stored grain pests. International Journal of Food Science. (2019), № 2 (4). P.612 - 621 doi.org/10.1155/2013/926468

11. Черепнев А.С., Черепнев И.А., Ляшенко Г.А. Использование импульсного электромагнитного излучения для обеззараживания зерновой смеси. Збірник наукових праць ХУПС ім. І. Кожедуба. 2008, Вип. 2(17). С. 53-55

12. Черепнев И. А., Ляшенко Г. А. Возможности тороидальных антенн для повышения эффективности терапевтического воздействия миллиметрового излучения. *Вісник ХНТУСГ.* 2014. Вип. 153. С. 153-155

УДК 621.317

64.РЕЗУЛЬТАТИ ЕКСПЕРИМЕНТАЛЬНИХ ДОСЛІДЖЕНЬ ЕФЕКТИВНОСТІ ДИСТАНЦІЙНОЇ РАДІОТЕРМОМЕТРІЇ У СФЕРІ МЕДИЦИНИ НАДЗВИЧАЙНИХ СИТУАЦІЙ

[1*]Черепньов І.А., [2]Вамболь С.О., [3]Niloofar Mozaffari, [3]Nastaran Mozaffari
[1]Державний біотехнологічний університет, м. Харків, Україна;
[2]Національний технічний університет «ХПІ», м. Харків, Україна;
[3]Université Laval, Quebec, Canada.
*E-mail: *voenpred314@ukr.net*

The results of experimental studies of the effectiveness of remote radiothermometry in the field of medicine of emergency situations

The data examines the main types of injuries that victims of railway accidents receive and shows an alarming trend in the increase in the number of these events on the territory of Ukraine. The main objective shortcomings of radiography, which is the most common method of medical control, as well as the state of radiology in Ukraine as a whole, are shown. The results of our own theoretical and experimental studies are presented, which prove the expediency of using the method of remote radiothermometry in the field of emergency medicine.

Як зазначено в роботі [1] аналіз медичних наслідків найбільш поширених катастроф (транспортні пригоди, катастрофи на вугільних шахтах та рудниках, землетруси, потужні вибухи та ін.) дозволяє зробити висновок про виникнення у постраждалих різних травм і патологій. Зокрема при залізничних катастрофах найчастіше зустрічаються механічні травми — 90,0% та механічні травми у комбінації з термічними опіками — 10,0%. В деяких випадках можливі гострі отруєння, хімічні опіки, радіаційні ураження та комбіновані та поєднанні ураження. Проблема аварій на залізничному транспорті вельми актуальна для України. За даними інформаційного агентства УНІАН в Україні зросла кількість аварій на залізниці: тільки за минулий рік зареєстровано 813 транспортних подій. В результаті 212 осіб загинули та 140 осіб отримали травми, з них: 479 аварій, з яких 126 аварій внаслідок зіткнення, сходження з рейок рухомого складу залізничного транспорту [2].

Отже для успішного лікування таких важких уражень, як переломи і опіки необхідно застосовувати ефективні методи діагностики і перш за все променевої. Як відомо, рентгенографія, історія застосування якої в медицині, в тому числі і військової налічує більш ніж сто років, довела свою дієвість і до недавнього часу її частка в світової медичної практиці складала 60–70%, а в Україні ця цифра сягає 90% [3,4]. Але тим не менш, вона не позбавлена істотних недоліків, які особливо чітко проявилися коли з'явилися інші методи променевої діагностики, зокрема наявність обмеження частоти проведення сеансів діагностики відповідно до індивідуальної дозою, яку отримає пацієнт, віком, статтю і

конкретним видом захворювання. Крім того, одяг, прикраси, гіпсові пов'язки, також впливають на на якість знімка, а отже і на об'єктивність діагностики [5]. В результаті при рентгенографії об'єкта в гіпсовій пов'язці треба підвищувати напругу на рентгенівській трубці на 10-15 Кв або збільшувати експозицію в три рази, що небажано, а в деяких випадках несе реальну небезпеку для пацієнта. В умовах України ці об'єктивні недоліки рентгенографії поглиблюються наступними обставинами[6]:

- вкрай недостатнім рівнем забезпеченості закладів охорони здоров’я вторинного рівня сучасним обладнанням для проведення обстеження пацієнтів з використанням променевих методів обстеження;
- низьким рівнем використання сучасних технологій з забезпечення променевої діагностики.

У роботі [7] показані переваги використання діагностичної апаратури на основі вимірювання власних електромагнітних випромінювань біологічних об'єктів і перш за все її абсолютну безпеку. Наведемо результати медичного експерименту з проведення діагностики травмованої людини, який частково був описаний в роботі [8] з використанням дослідного зразка медичної діагностичної системи радіотеплового картування, що вміщує в собі два функціонально завершені пристрої: кореляційний радіометр та модуляційний радіометр (рис.1).

Потерпілий мав множинні опіки кистей, сідниць, зовнішніх статевих органів та нижніх кінцівок, на 40% поверхні тіла, з пошкодженням дихальних шляхів, у стані шоку. В ході радіометрії, яка проводилася при накладених на тканини пов'язках, виявлена термоампутація гомілок і стоп (рис. 2 кадр 1). Була застосована гангліонарна блокада і скоректований обсяг і склад проведеної терапії (рис.1, кадр 2).

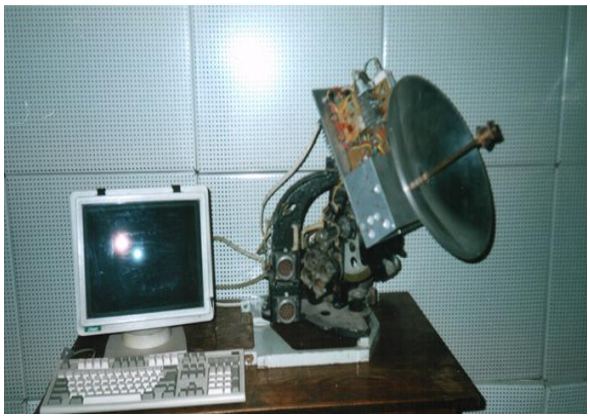


Рис.1. Дослідний зразок медичної діагностичної системи радіотеплового Картування

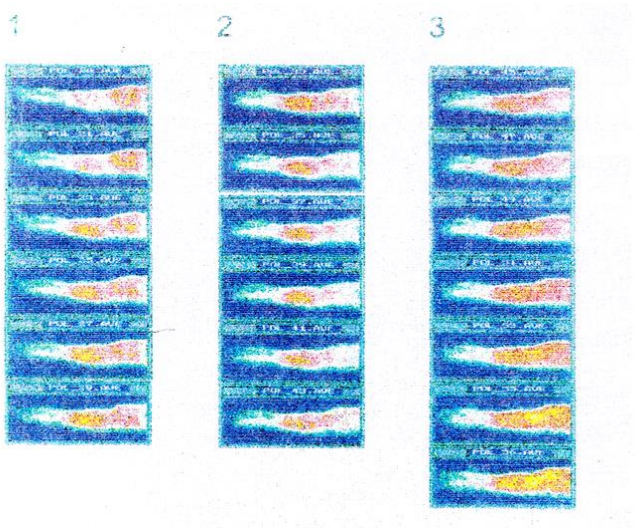


Рис.2. Радіометрія стану пошкоджень і реакція організму на процес лікування

Яскравість радіозображень тканин збільшилася, термо амплітуда зникла, що свідчило про поліпшення кровообігу в нижніх кінцівках (рис.1, кадр3). По завершенні цього процесу відзначено поліпшення показників: артеріальний тиск 120/70 мм рт. ст., зменшилася набряклість тканин. Термоампутація кінцівок була відсутня на радіотермограмах в останні дні.

В ході клінічних спостережень відзначено, що дистанційна радіотермометрія забезпечує отримання безпосередніх і безінерціальних даних про температуру тканин в їх глибині, причому самі дані слабо схильні до термоэкранирующему і термостабилизирующему впливу верхніх шарів шкіри, нанесених на поверхню тканин лікарських препаратів, медичних пов'язок та інших покриттів, що доводить доцільність використання цього методу діагностики в медицині надзвичайних ситуацій.

Література

1. Халмурадов Б. Д. Медицина надзвичайних ситуацій: підручник. Київ: Центр учбової літератури, 2016. 208 с.

2. ЗМІ назвали причини великої кількості аварій на українській залізниці. *УНІАН:* веб-сайт. URL: https://www.unian.ua/society/zmi-nazvali-prichini-velikoji-kilkosti-avariy-na-ukrajinskiy-zaliznici-novini-ukrajini-11501047.html (дата звернення 30.01. 2023).

3. Медична апаратура спеціального призначення: навч. посіб. / С. М. Злепко та ін. Вінниця : ВНТУ, 2010. 159 с.

4. Васько Л.М. Іноваційний метод цифрової рентгенологічної візуалізації – малодозовий томосинтез. *Актуальні проблеми сучасної медицини: Вісник Української медичної стоматологічної академії.* 2018. № 1 (61). т 18. С. 292-296.

5. Pizzutiello R. J., Jr., Cullinan J. E. Introduction to medical radiographic imaging. Rochester, NY: Health Sciences Division, Eastman Kodak Co., 1993. 237 p.

6. Організація променевої діагностики в умовах реформування системи медичної допомоги на регіональному рівні: метод. рекоменд. / Г.О. Слабкий та ін. Київ, 2016. 36 с.

7. Черепнёв И.А., Лупиков В.С., Ляшенко Г.А. Основные требования к диагностической аппаратуре на основе измерения собственных электромагнитных излучений биологических объектов. *Системи управління навігації та зв'язку.* 2011. Вип.4 (20). С. 124 – 131.

8. Экспериментальное обоснование медико-технических требований к аппаратуре радиотеплового картирования биологических объектов / И.А. Черепнев та ін. *Збірник наукових праць ХВУ*. 2002. Вип.1(39). С. 126–130.

УДК 614.84

65. РОЗРОБКА АВТОНОМНОЇ СИСТЕМИ ДЛЯ ГЕНЕРУВАННЯ КОМПРЕСІЙНОЇ ПІНИ

Шахов С.М.[1], Гречаник О.С.[1]
1 Національний університет цивільного захисту, Україна
E-mail: lophennss@gmail.com

Development of an autonomous compressed air foam system

A modern means of fire extinguishing with compression foam is proposed. The developed sample corresponds to the technical characteristics of foreign systems for generating and supplying compression foam. The implementation of the developed system will allow to increase the efficiency of the emergency and rescue units of the State Emergency Service of Ukraine in the performance of assigned tasks.

Пожежі класів А та В серед інших класів пожеж завдають значної матеріальної та екологічної шкоди. Найбільш поширеною вогнегасною речовиною, що застосовується для гасіння пожеж класу А є вода, так як вона має високі показники теплоти пароутворення, теплоємності і низьку теплопровідність. Основним механізмом вогнегасної дії води є охолодження зони горіння. Вода при потраплянні в осередок пожежі охолоджує горючу речовину нижче температури займання. Крім цього, при поглинанні водою тепла утворюється пара, яка перешкоджає надходженню кисню повітря до зони горіння.

Традиційно у переважній більшості в Україні застосовуються водяні пожежні стволи. Протягом багатьох років технології пожежогасіння із застосуванням води розвивалися в основному в напрямку збільшення номінальної витрати води і дальності її подавання. Ефективність такого методу виправдана лише при гасінні великомасштабних пожеж. Але у випадках пожеж у спорудах житлового сектору, частка яких складає 76 % від загальної кількості пожеж по Україні, використання такої техніки не є ефективним, адже надлишок води (до 90 %), що застосовується для цілей пожежогасіння, не бере участі у гасінні пожежі, заливає нижні поверхи та приводить до суттєвих побічних збитків. Для підвищення ефективності гасіння у розвинутих країнах використовують нову технологію (система CAF) з застосуванням компресійної піни (КП), яка практично немає у своєму складі незв'язаної води, що надає їй нові, непритаманні як воді так і повітряно-механічній піні, властивості.

Компресійна піна (англійською Compressed Air Foam) – високодисперсна гомогенна піна низької кратності, яка генерується у спеціальних системах [1-9] - Compressed air foam systems (рис. 1), шляхом змішування води піноутворювача, та повітря під тиском [10,11]. У літературі зустрічається також як: «газонаповнена», «пневматична піна», «легка піна».

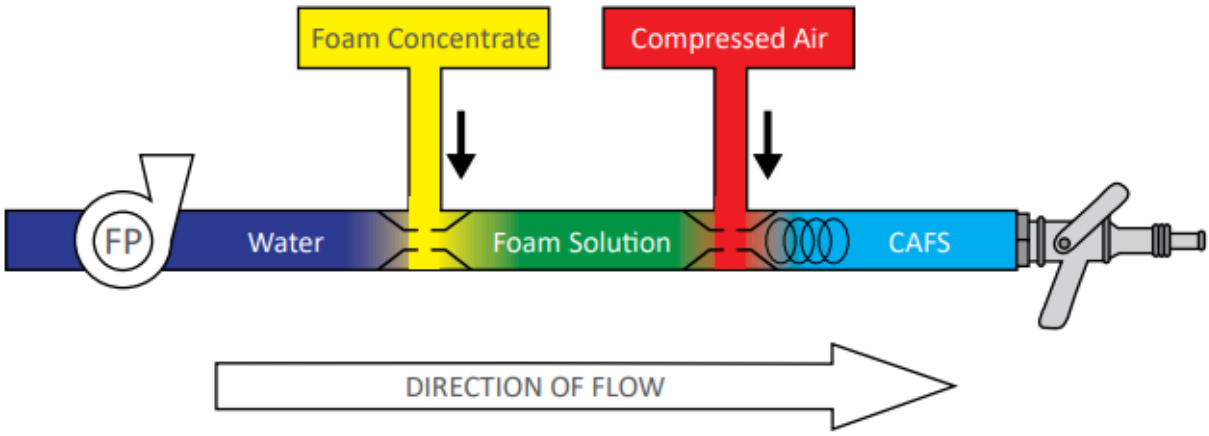


Рис. 1. Процес генерування компресійної піни у системах CAFS

Серед світових виробників систем флагманом є технологія ONE SEVEN , яка являє собою високоефективний засіб пожежогасіння для використання якого необхідно лише незначна кількість води. ONE SEVEN широко використовується в багатьох країнах світу, зокрема, в Німеччині, Австрії, Франції, США, Великій Британії, Росії. Аналіз досвіду застосування компресійної піні в США, Австрії, Німеччині та Росії доводять, що піногенеруючі системи мають ряд переваг в порівнянні з традиційними технологіями пожежогасіння, а саме: - більш висока ефективність гасіння (зменшення часу гасіння); - зменшені витрати води (2-5 рази) і піни (6-10 разів); - швидке зниження температури в зоні горіння; - невеликі пошкодження майна в результаті зменшення промокання водою; - можливість подачі піни по сухотрубах на велику висоту; - збільшення дальності подачі піни.

Окрім системи ONE SEVEN є також не менш ефективні переносні технічні засоби пожежогасіння, які знаходяться на оснащенні у пожежно-рятувальних підрозділах багатьох країн світу, це такі як: засіб пожежогасіння «HDL 70» (Німеччина), установки протипожежні високого тиску УПВТ «REIN» та «HIPRESS» MSA AUER (Німеччина), HLG «HYDROJET» та HLG «POWERJET» (Франція), установка протипожежна високого тиску УПВТ «ЕРМАК» (Російська Федерація), портативна система «CAFS 60-P» (США), мобільна система «CAFS Mobile» (Австрія) тощо.

Окремо треба зазначити значну вартість закордонного обладнання та компонентів для виготовлення компресійної піни. Тому значний інтерес викликає вивчення можливостей отримання компресійної піни із використанням вітчизняних компонентів та обладнання, що знаходиться на оснащенні підрозділів ДСНС, що робить роботу актуальною. Результати виконаної роботи дозволять започаткувати впровадження в практику нових інноваційних методів гасіння пожеж з підвищеною ефективністю.

У роботі пропонується дослідний зразок системи генерування компресійної піни, який може працювати в автономному та стаціонарному

режимах. На рис. 2 наведена 3D модель дослідного зразка для отримання компресійної піни.

Рис. 2

Співвідношення вода - повітря та загальні витрати вогнегасної речовини, тиск у системі регулюються за допомогою розробленого пульта керування, рис. 3.

Рис. 3. Загальний вигляд багатофункціонального пульта керування прототипу дослідного зразку системи з генерування компресійної піни.

Виготовлена система генерування компресійної піни забезпечує зміну тиску в інтервалі від 1 до 10 бар, витрати води до 3,5 л/с. Максимальний тиск у компресорі 14 бар , він може регулюватися через редуктор від 1 до10 бар з похибкою 0.2 бара. Ємність для води 20 л.

В якості основи для установки був використаний вогнегасник ОП-20. Подача повітря передбачено як від компресору мод. К-22 УХЛ4.2 (робочий тиск 16 МПа, об'ємом ресиверу 220 м3), так і від балонів зі стисненим повіт-рям (робочий тиск 250 МПа, об'єм 19 л.). У лінію після компресору вмонто-ваний редуктор для регулювання тиску та витрат повітря до робочої камери. Для змішування розчину піноутворювач + вода з повітрям в використо-вувався оригінальний реактор. Витрати розчину та повітря регулювалися окремо за

допомогою кранів. Максимальний тиск повітря, що використовувалось -10 МПа. Витрати води передбачені до 80 л/хв. Розчин піноутворювача готуємо окремо, а потім заливаємо до ємності ОП - 20.

Висновки

1. Запропоновано сучасний засіб пожежогасіння компресійною піною. Розроблений зразок відповідає технічним характеристикам закордонних систем генерування та подавання компресійної піни. Впровадження розробленої системи дозволить підвищити ефективність аварійно-рятувальних підрозділів ДСНС України при виконанні завдань за призначенням.

Література

1. Compressed Air Foam System: веб-сайт. URL: http://compressedairfoamsystem.com
2. Oneseven: веб-сайт. URL: http://www.oneseven.com
3. Systeme: einfach, sicher und okonomisch: веб-сайт. URL: http://www.oneseven.com/de/stationaerbrandschutz/systeme/standardsystem/beschreibung.php (дата звернення: 30.12.2018).
4. Leistungsstark. Einfach. Sicher : веб-сайт. URL: http://www.rosenbauer.com
5. CAFS–Systems : веб-сайт. URL: http://www.waterousco.com/cafs–systems
6. Firefighting Vehicles : веб-сайт. URL: http://www.gimaex.com. (дата звернення:
7. Products: веб-сайт. URL: http://kssieler.de/hale/cafs (дата звернення: 27.11.2018).
8. Описание технологии NATISK : веб-сайт. URL: http://www.specialauto.ru/catalog/524.html
9. Оборудование пенного пожаротушения : веб-сайт. URL: http://www.stalt.ru/en/products/sistema–pennogopojarotusheniya.html (дата звернення: 27.11.2018).
10. Ларін О.М., Виноградов С.А., Баркалов В.Г. Пожежні машини. К.: МПБП «Гордон», 2016. 279 с.
11. Kovalyshyn, V., Velykyi, N., Kovalyshyn, V., Voitovych, T., & Sorochych, M. (2021). Засоби отримання та перспективи застосування компресійної піни. Пожежна безпека, 39, 94-104. https://doi.org/https://doi.org/10.32447/20786662.39.2021.11

УДК 614.84

66. ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ГЕНЕРУВАННЯ КОМПРЕСІЙНОЇ ПІНИ З ВІТЧИЗНЯНИМИ ПІНОУТВОРЮВАЧАМИ

Шахов С.М.[1], Зінченко О.О.[1]
1 Національний університет цивільного захисту, Україна
E-mail: lophennss@gmail.com

STUDY OF THE EFFICIENCY OF COMPRESSED AIR FOAM GENERATION WITH DOMESTIC FOAM FORMERS

A study was conducted on the possibility of generating compression foam using domestic foaming agents. Based on the results of research, it was established that with an increased concentration of the foaming agent "Bars - S1" from 3% to 5%, the multiplicity of the foam increases significantly. When the concentration was further increased from 5% to 6%, no significant changes were observed for the multiplicity of the generated foam. When using the foaming agent "Pirena,1" there is a significant increase in the multiplicity when the concentration of the foaming agent is increased from 4% to 5%.

Водо-пінні вогнегасні речовини постійно використовують під час боротьби з пожежами. Для гасіння пожеж легкозаймистих горючих рідин застосовують повітряно-механічна піну. Вода є найбільш поширеною вогнегасною речовиною для гасіння пожеж твердих горючих матеріалів. За кордоном для гасіння пожеж класу А та Б застосовують компресійну піну [1-5], яка є більш ефективною порівняно з традиційними вогнегасними речовинами.

Компресійна піна – це піна низької кратності, що утворюється за рахунок одночасного введення до камери змішування повітря, води та піноутворювача. З результатів аналізу [] встановлено, що для генерування компресійної піни застосовуються спеціальні піноутворювачі класу А. Сьогодні на території України відсутні потужності, необхідні для виробництва таких піноутворювачів, а їх закупівля є дуже невигідною, що зумовлено великою вартістю.

Тому актуальним завданням є можливість дослідження генерування компресійної піни за допомогою вітчизняних піноутворювачів.

На теперішній час в Україні виробляються піноутворювачі різних класів. Найбільше підрозділами ДСНС використовуються:

- загального призначення - синтетичний піноутворювач підвищеною вогнегасною здатністю «Пірена-1»; та синтетичні піноутворювачі «Пегас» - (який за своїми характеристиками не поступається російському аналогу «ПО-3НП»), «АЛЬПЕН - М», Барс S-1.

- спеціального призначення – «ППЛВ-(Універсал)» марок 103, 103М,

Піноутворювач 106, 106М, є альтернативою закордонним плівкоутворювальним піноутворювачам, плівко утворюючий піноутворювач «СОФИР» (AFFF, AFFF AR), та «Барс AFFF-1» – фторсинтетичний плівкоутворювальний для отримання пін як низької так і середньої кратності.

За допомогою дослідного зразку автономної системи генерування компресійної піни (рис. 1) проведено дослідження з можливості генерування компресійної піни із вітчизняними піноутворювачами.

Рис. 1. Загальний вигляд системи

На першому етапі використано синтетичний піноутворювач загального призначення: «Барс-S1», згідно з ТУ У 20.41.20-20.00-36918251-001:2015. На рис. 2, подано отримані результати.

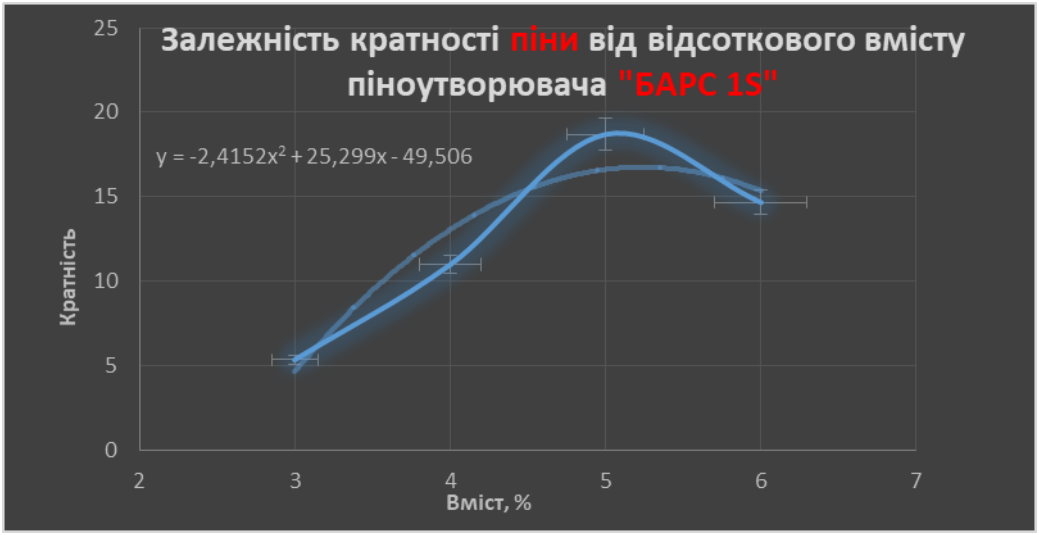


Рис. 2. Залежність кратності піни від концентрації ПУ «Барс – S1»

Далі було застосовано такі піноутворювачі, як «Пірена-1» згідно з ТУ У 24.6-20166240-002:2010 та експериментальний модифікований

плівкоутворювальний піноутворювач “Ефект”, виробництва ТОВ НВП «Укрпожстандарт». На рис. 3. подано зведені результати досліджень.

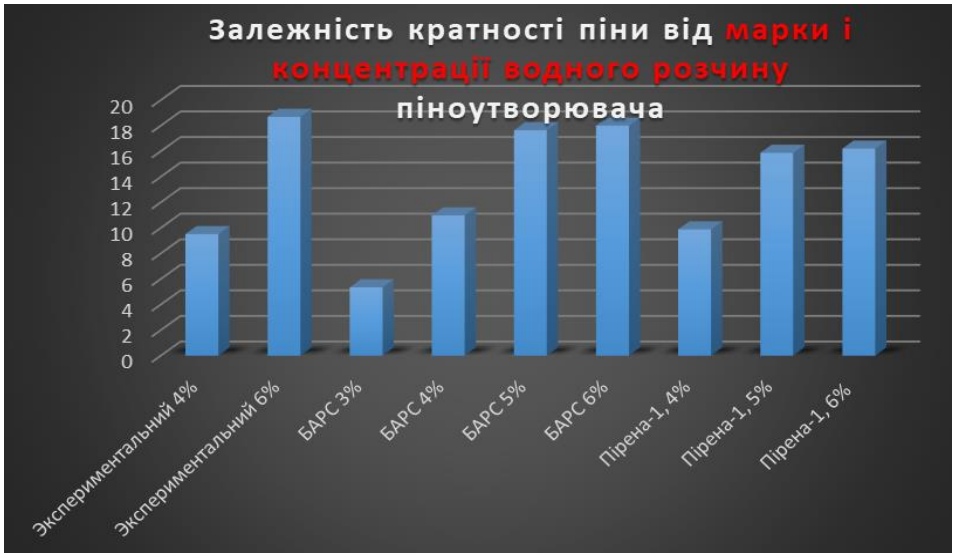


Рис. 3. Залежність кратності піни від марки та концентрації ПУ.

Висновки

1. Проведено дослідження з можливості генерування компресійної піни із використанням вітчизняних піноутворювачів. За результатами досліджень встановлено, що при підвищені концентрації піноутворювача «Барс - S1» від 3 % до 5 % суттєво збільшується кратність піни, що підвищує її вогнегасні властивості. При подальшому збільшенні концентрації від 5 % до 6 % значних змін для кратності генерованої піни не спостерігалось. При використанні піноутворювача «Пірена,1» має місце значне збільшення кратності при підвищенні концентрації піноутворювача від 4 % до 5 %. При підвищенні кратності до 6 % зміна кратності не спостерігалась. Під час генерування піни за допомогою «експериментального» піноутворювача найбільшу кратність піни отримано з робочою концентраціє 6 %. У разі генерування піни з 4 % концентрацією «експериментального» піноутворювача, отримана піна кратністю 10, яка є нестійкою.

Література

1. Шахов С.М. Визначення вогнегасної ефективності компресійної піни під час гасіння нею твердих горючих речовин. / С.М. Шахов, С.А. Виноградов, А.І. Кодрик, О.М. Тітенко // Проблеми пожежної безпеки. - Вип. 46. – 2019. - С. 199–205. Режим доступу : http://repositsc.nuczu.edu.ua/handle/123456789/12273

2. Tao Chen, Xue-cheng Fu, Zhi-ming Bao, Jian-jun Xia, Rong-ji Wang. (2018). Experimental Study on the Extinguishing Efficiency of Compressed Air Foam

Sprinkler System on Oil Pool Fire. Procedia Engineering. Volume 211. P. 94-103. doi: https://doi.org/10.1016/j.proeng.2017.12.142.

3. Шахов С.М., Виноградов С.А., Ларін О.М. Аналіз світових зразків систем пожежогасіння газонаповненою піною. *Надзвичайні ситуації. Попередження та ліквідація*. 2017. Вип 1. С. 50–58.

УДК 614.8

67. ДО ПИТАННЯ ЗАХИСТУ ОСОБОВОГО СКЛАДУ В КАБІНІ ПОЖЕЖНО-РЯТУВАЛЬНОГО АВТОМОБІЛЯ ВІД НЕБЕЗПЕЧНИХ ЧИННИКІВ ПОЖЕЖІ

Яценко В.О.[1], Виноградов С.А.[1]
1 Національний університет цивільного захисту України
E-mail: vynogradovs@gmail.com

On the issue of protection of personnel in the cab of a fire rescue vehicle from dangerous factors of fire

The report draws attention to the problems of protecting firefighters and rescuers in the cabin of the personnel of the fire-rescue vehicle from dangerous factors of fire. It is necessary to decide what conditions should be provided in the car cabin for the work of rescuers and how to provide them. In fire-rescue vehicles manufactured in Ukraine, the issue of protecting personnel in the vehicle cabin from dangerous fire factors is not taken into account in any way.

При створенні пожежно-рятувальних автомобілів (ПРА) конструкція кабіни вантажного автомобіля, на базі якого створюється пожежний автомобіль, значних змін не піддається. При цьому захист від впливу зовнішнього середовища зводиться до запобігання водію та членам оперативного розрахунку від перегріву, переохолодження, впливу сонячної радіації та атмосферних опадів.

Водночас умови роботи ПРА суттєво відрізняються від умов роботи автомобілів народногосподарського призначення. Ця відмінність обумовлена можливим впливом на кабіну та салон оперативного розрахунку небезпечних чинників пожежі. Це вплив неминуче призводить до зміни мікрокліматичних умов у ній.

Зміна умов роботи рятувальників у кабіні пожежного автомобіля під час роботи поблизу фронту полум'я вперше було розглянуто ще у 70-х роках XX століття, але досі досить повно ніким не досліджено. Однак нагрівання кабіни від впливу відкритої пожежі може призвести до найсерйозніших наслідків, аж до загрози здоров'ю та життю рятувальників та виходу автомобіля з ладу.

Таким чином, при розробці теплового захисту пожежного автомобіля необхідно вирішити питання які умови мають бути забезпечені в кабіні

автомобіля для роботи рятувальників та яким чином їх забезпечити. Очевидно, що в цьому випадку безпечні мікрокліматичні умови будуть визначатися гранично допустимими для людини температурами повітря та поверхонь огорож, загазованістю повітря, інтенсивністю теплового випромінювання всередині кабіни тощо.

У пожежно-рятувальних автомобілях, що виготовляються в Україні, питання захисту особового складу в кабіні автомобіля від небезпечних чинників пожежі не враховуються. Тому розвиток цього питання є актуальним.

РОЗДІЛ 8

ДОСВІД ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ, БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ І РОБОТІВ ДЛЯ МОНІТОРИНГУ ДОВКІЛЛЯ, ЗАПОБІГАННЯ Й ЛІКВІДАЦІЇ ЗАГРОЗ ПРИРОДНОГО І ТЕХНОГЕННОГО ПОХОДЖЕННЯ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ.

УДК 004.932.75, 004.4'236, 004.942, 621.317.3

68. ВИКОРИСТАННЯ БПЛА ТА СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ МОНІТОРИНГУ ПОЛІВ ПРИ ТОЧНОМУ ЗЕМЛЕРОБСТВІ

Бобков Ю. В.[1], Шевчук А. А.[1,]

1 Навчально-науковий інститут аерокосмічних технологій Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
E-mail: bobkov_yuriy@ukr.net

Use of UAVs and Modern Information Technologies to Monitor Fields in Precision Agriculture

In this work, ways of building a monitoring system to solve the problems of precision agriculture and environmental problems are analyzed. The expediency of using a UAV with a technical vision system to obtain high-resolution images of the studied land plot is shown. Necessary equipment and software were developed for the monitoring system. The proposed algorithm is based on the use of high-quality images from camera of the quadcopter, low-resolution satellite images and the results of agrochemical analyzes. The identified zones of plant fertility make it possible to build a differentiated fertilizer application map and a map of the agro-operations task plan for precision farming equipment.

Вступ. Сучасний стан розвитку сільськогосподарського виробництва характеризується потребами в застосуванні найсучасніших технологій для підвищення його еколого-економічної ефективності, зокрема шляхом всебічного моніторингу стану полів.

Особливістю сільського господарства в Україні є відсутність зонування родючості землі, що не дозволяє мати ефективне з точки зору економіки землеробство та веде до виснаження ґрунтів та падіння врожайності. З іншої сторони, надмірне застосування добрив та засобів боротьби з сільськогосподарськими шкідниками та бур’янами може призвести до виникнення різнопланових екологічних загроз довкіллю.

Вирішення вказаних проблем можливо за рахунок точного землеробства, яке передбачає просторово диференційований підхід до застосування технологій вирощування сільгоспкультур залежно від властивостей ґрунту, забезпеченості рослин поживними речовинами та вологою, стану рослин на певному етапі їх розвитку.

Постановка задачі. Необхідною умовою ведення точного землеробства є детальна та динамічна оцінка просторової неоднорідності стану ґрунтів та сільськогосподарської рослинності, що забезпечує своєчасне застосування адекватних агрозаходів саме в тих місцях, що цього потребують. [1,2,3]

В класичному варіанті для точного землеробства використовують комплекс супутникових та комп'ютерних технологій, що включає в себе технології глобального позиціонування (GPS), географічні інформаційні системи (GIS), технології оцінки врожайності (Yield Monitor Technologies), технологію змінного нормування (Variable Rate Technology) і технології дистанційного зондування землі. Нажаль ці сучасні технологічні рішення потребують дуже значних вкладень як в апаратне, так і програмне забезпечення, а також на їх супровід. В сьогоденних умовах України затрати на супутникові інформаційні системи не можуть собі дозволити навіть крупні агрохолдинги, не кажучи вже про середні, дрібні та фермерські господарства.

Існує альтернативний, більш економічний варіант, при якому для ведення землеробства застосовуються дані моніторингових спостережень, отримані від безпілотних літальних апаратів (БПЛА), оснащених системами технічного зору (СТЗ). [4,5]

В останньому випадку доводиться вирішувати ряд складних задач, пов’язаних з вибором або розробкою необхідного обладнання та програмного забезпечення системи моніторингу, просторовою прив’язкою отриманих даних та їх обробкою, застосуванням результатів для пооперацийного ведення агротехнічних робіт. Саме на вирішення цих задач була спрямована робота.

Розробка та вибір обладнання системи моніторингу. В більшості випадків для мінімізації витрат для системи моніторингу доцільно застосовувати серійні фото- відео-камери (далі просто камери).

Практичний досвід показує, що навіть знімання звичайною фотокамерою з високої роздільною здатністю дозволяє отримати гарні результати щодо оцінки стану посівів, прогнозу врожаїв та можливих ризиків. Це обумовлено особливістю даних, отриманих за допомогою фотозйомки з БПЛА, особливо квадрокоптера, а саме:

- висока та навіть надвисока просторова роздільна здатність, що обумовлена кількома факторами, зокрема: вибором камери з високою роздільною здатністю, відносно низькою висотою та швидкістю польоту, що дозволяє досягти високої деталізації даних (знімків);
- можливість планувати та виконувати зйомку у найбільш зручний для досягнення заданої мети час.

Тому було прийнято рішення щодо застосування для поставлених задач точного землеробства промислового квадрактоптера, оснастивши його СТЗ із застосуванням серійної камери.

Відповідно був обраний квадракоптер типу DJI Mavic 2 Pro з наступними основними характеристиками: максимальна швидкість польоту - 72 км/год; максимальна висота - 6000 м; час польоту - 31 хв.

За отриманими в роботі результатами були розраховані необхідні за роздільною здатністю характеристики камери, а саме: роздільна здатність не

менше 18 Мп, апертура на рівні f/3 – f/10. За цими характеристиками була обрана камера Mavic 2 Pro, що повністю відповідає за конструктивними кріпленнями обраному квадракоптеру та має роздільну здатність 20 Мп, і апертуру f/2,8 – f/11.

Розробка інформаційного забезпечення системи моніторингу. Кінцевою метою обробки агротехнічної інформації є отримання карти завдань для техніки точного землеробства, що дозволяє забезпечити високу ефективність та мінімізувати екологічні ризики для довкілля.

Для вирішення цієї задачі було запропоновано використати наступні джерела інформації:

1. Зображення поверхні землі отримане з супутників Sentinel–2 програми Copernicus. Знімки Sentinel-2 добре підходять для звичайних потреб сільського господарства, оскільки оновлюються кожні 3–5 днів та є у вільному доступі. На основі цих знімків розраховується індекс вегетації NDVI, що є показником стану розвитку рослини, та створюється відповідна карта ділянки. Але їх роздільної здатності в 10 метрів недостатньо для техніки точного землеробства.

2. Знімки досліджуваної земельної ділянки (поля), отримані за допомогою СТЗ квадрокоптера. Оскільки площа досліджуваної ділянка може бути достатньо великою та досягати десятків і навіть сотень гектарів, то для її охоплення квадрокоптер повинен робити знімки з великої висоти. Але при цьому знижується просторова точність вирішення задачі за рахунок втрати дрібних деталей (окремих рослин), які є суттєвими. Альтернативним шляхом, що застосовувався в цій роботі, є отримання серії знімків земельної ділянки з невеликої висоти (близько 120 метрів) і наступне об’єднання (зшивання) зображень в одне ціле за допомогою розробленого програмного забезпечення. Значну роль при цьому має точна координатна прив’язка знімків до географічних координат ділянки. Процес є достатньо складним, але дозволяє запобігти втраті даних та отримати необхідну роздільну здатність.

3. Результати агрохімічного обстеження ґрунту в спеціальній сертифікованій лабораторії за відібраними зразками. Ґрунти досліджують більш ніж по 30 параметрам, основними з яких є кислотність, вміст фосфору, калію і гумусу. За його результатами складають у GIS (Geographic Information System) програмах цифрові карти властивостей полів.

Виходячи із послідовності обробки знімків для отримання карти завдань для сільськогосподарської техніки точного землеробства був розроблений програмно-алгоритмічний комплекс системи моніторингу.

Практичні результати. Наведемо деякі практичні результати, що були отримані із застосуванням розробленої системи моніторингу та програмно-алгоритмічного комплексу. Дослідження проводились у 2020-2021 рр. на тестовій ділянці поля площею 57,4 га, що була розташована в Чаплинському районі Херсонської області.

За допомогою обраного обладнання була отримана серія знімків ділянки та сформований єдиний ортофотоплан з зонами однорідності сходу рослин (рис. 1). На основі супутникових знімків Sentinel-2 побудовано зображення ділянки у форматі NDVI низької роздільної здатності (рис.2, а). За результатами агрохімічного аналізу побудовано карти ділянки за окремими мікроелементами ґрунту. Для прикладу на рис. 2 наведені карти з результатами аналізів за вмістом рухомого фосфору (рис. 2, б) та рухомих форм сірки (рис. 2, в.)

Проведена обробка інформації по ділянці та побудований ортофотоплан (рис. 1) з надвисокою просторовою роздільною здатністю та заданою допустимою похибкою геоприв'язки, дозволяють розробляти карти завдань агроопераций для техніки точного землеробства. В якості прикладу на рис. 3 наведена карта для диференційованого внесення добрива Амофос розкидачем Suzuki Sulky, обладнаного системами для точного землеробства.

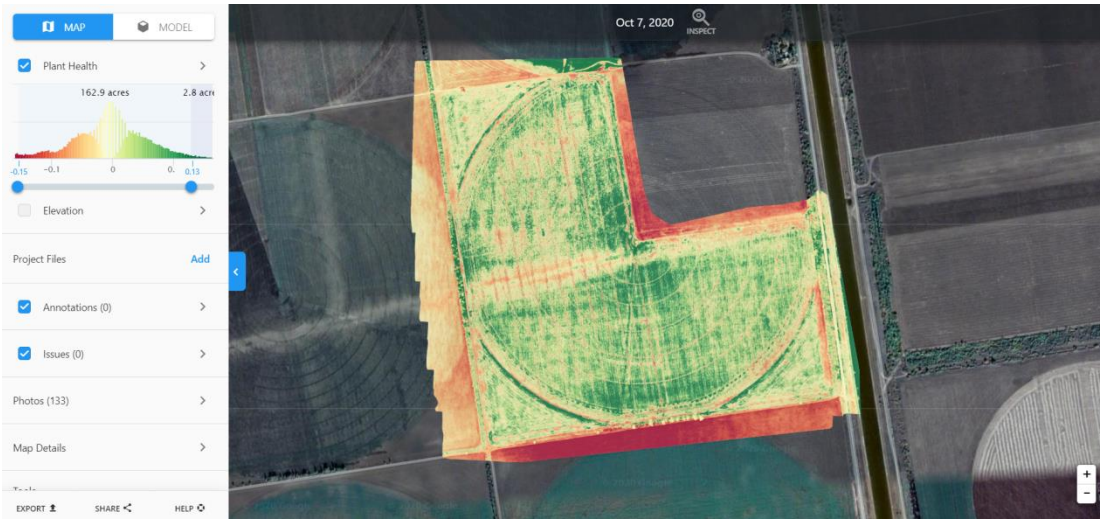
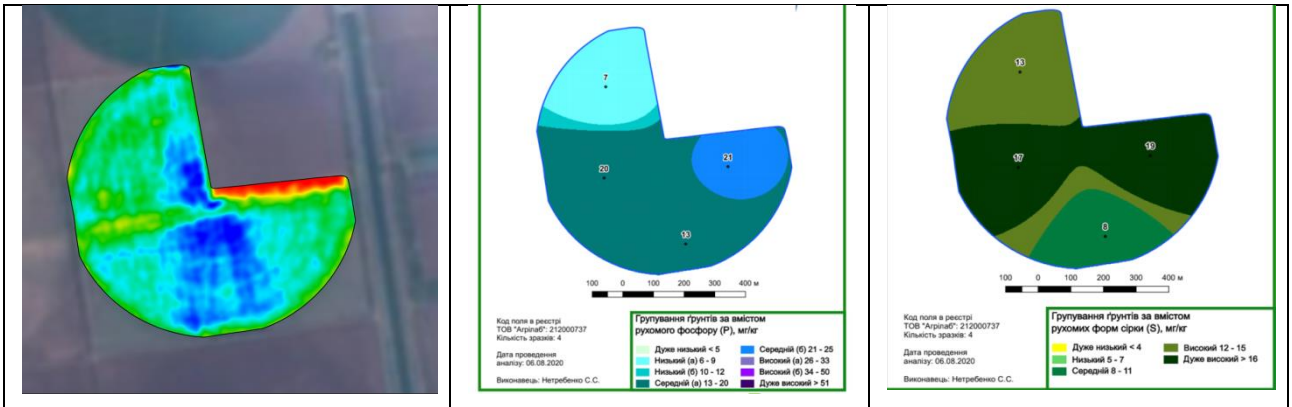


Рис. 1 - Ортофотоплан з зонами однорідності сходу рослин



а	б	в

Рис. 2 - Супутниковий знімок NDVI та результати агрохімічного аналізу

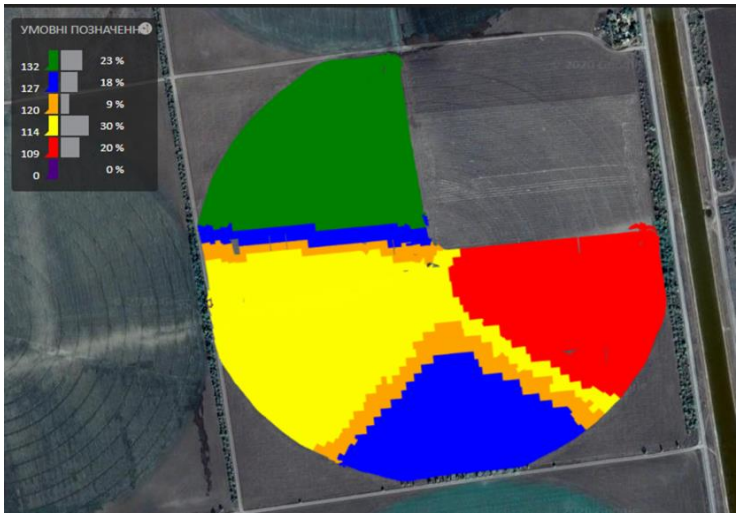


Рис. 3 - Карта завдання для диференційованого внесення добрива Амофос

Висновки

1. Запропоновано використовувати БПЛА, оснащені СТЗ, для моніторингу стану полів та вирішення задач точного землеробства. Для отримання необхідної роздільної здатності, з урахуванням простоти та доступності доцільно в якості БПЛА обирати квадракоптери.

2. Обґрунтовано розробку або вибір необхідного обладнання системи моніторингу на основі розрахунку необхідних технічних характеристик, в першу чергу потрібної просторової роздільної здатності.

3. Запропоновано інформаційне забезпечення системи моніторингу, що базується на застосуванні високоякісних знімків від системи технічного зору квадрокоптера, супутникових знімків низької роздільної здатності та результатів агрохімічних аналізів ґрунтів. При обробці даних окремі знімки, отримані за допомогою камери квадрокоптера, об'єднуються в єдиний ортофотоплан. Ідентифіковані зони родючості рослин та карти поточного стану ґрунтів використовуються для побудови диференційованої карти завдань агроопераций для техніки точного землеробства.

Проведені польові дослідження повністю підтвердили правильність обраних рішень та роботоздатність запропонованих алгоритмів.

Отримані в роботі результати можуть бути також застосовані для оцінки техногенного впливу на довкілля на основі аналізу стану рослинного покриву.

Література

1. Victor Alchanatis, et al. Thermal Imaging for Precise Irrigation Guidance. Optimizing irrigation by using thermal images to map the variability of water potential in the field. [Israel

Agricultural Portal]. – 2014. – November 3. - URL: http://www.israelagri.com/?CategoryID=396&ArticleID=645
2. Rocío Calderón .Early Detection and Quantification of Verticillium Wilt in Olive Using Hyperspectral and Thermal Imagery over Large Areas [Електронний ресурс] /Rocío Calderón, Juan A. Navas-Cortés and Pablo J. Zarco-Tejada // Remote Sensing/ - 2015. – 7(5)/ - URL: http://www.mdpi.com/2072-4292/7/5/5584/htm
3. Lu Xu Retrieval of Soil Water Content in Saline Soils from Emitted Thermal Infrared Spectra Using Partial Linear Squares Regression [Електронний ресурс] / Lu Xu, Quan Wang. Academic Editors: Nicolas Baghdadi and Prasad S. Thenkabail //Remote Sensing – 2015. - 7(11). - 14646-14662. - URL: http://www.mdpi.com/2072-4292/7/11/14646/htm
4. Ачасов А. Б. (2015) Щодо використання БПЛА для оцінки стану посівів / А. Б. Ачасов., А. О. Ачасов., Г. В. Тітенко, О. Ю. Селіверстов, А. О. Сєдов // Вісник Харківського національного університету імені В. Н. Каразіна, Серія «Екологія», вип. 13. С. 13-18.
5. Ачасова А. Ефективне використання дронів в сільському господарстві: що необхідно? [Електронний ресурс] 50 North. – URL: http://www.50northspatial.org/ua/drones-agriculture-issues

УДК 614.8

69. ПРОБЛЕМИ ГАСІННЯ ПОЖЕЖ НА ОБ'ЄКТАХ ЕНЕРГЕТИКИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

Стаматі В.Г.[1], Виноградов С.А.[1]
1 Національний університет цивільного захисту України
E-mail: vynogradovs@gmail.com

Problems of fire extinguishing at energy facilities and ways to solve them

The report examines the consequences of missile strikes on energy facilities in Ukraine, the main problems in extinguishing such fires, including repeated missile attacks during fire suppression. The technical characteristics of the Magirus Wolf R1 tactical robot were reviewed and it was noted that the use of robotics is the main direction of reducing possible losses of firefighters when extinguishing fires at energy facilities.

У 2022 році в Україні зареєстровано більше 80 000 пожеж [1]. Серед причин їх виникнення у зв'язку з повномасштабним вторгненням російської федерації в Україну додалась ще одна – обстріли ворожої армії. З цієї причини сталося більше 10 000 пожеж.

Найбільш потужних ракетних ударів зазнала критична інфраструктура України, серед якої – об'єкти електро-енергетики. За рік війни у енергетичні об'єкти України влучило 255 ракет [2] (рис. 1). Україна тимчасово втратила 44% атомної генерації, 75%

потужності ТЕС та 33% блочних ТЕЦ [3].

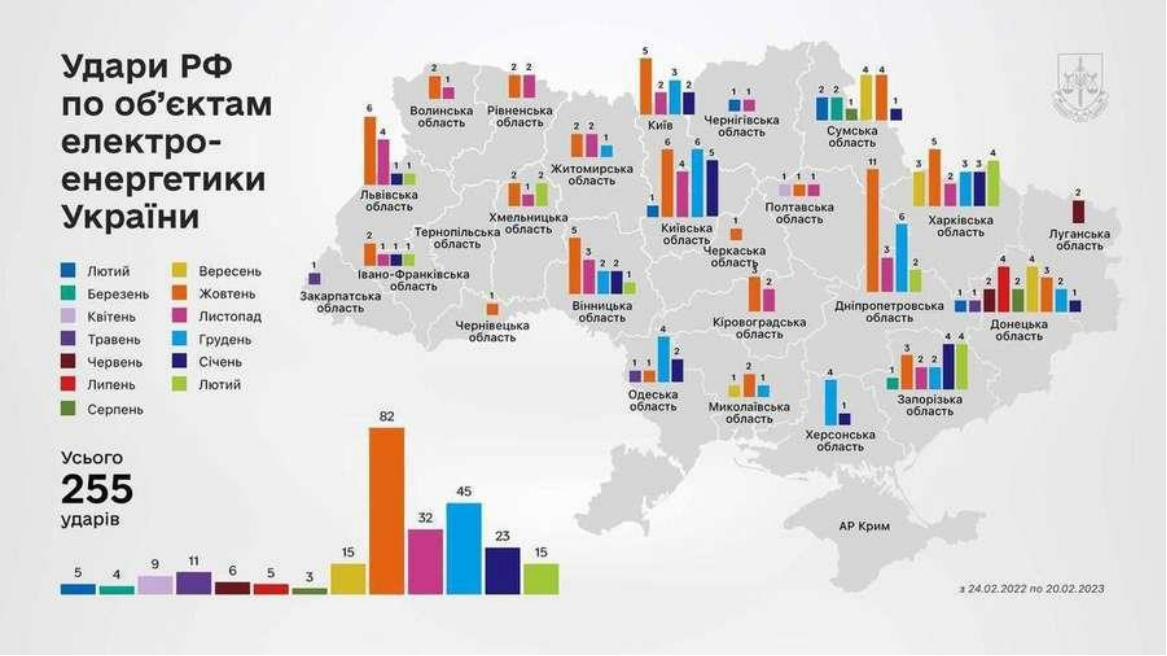


Рис. 1. Удари рф по об'єктам електро-енергетики України

Кожен з ударів спричинив великі пожежі, на гасіння яких було задіяно десятки одиниць спеціальної техніки ДСНС України та сотні осіб особового складу.

До основних чинників, що ускладнюють гасіння пожеж на об'єктах енергетики відносяться [4]:

- наявність електрообладнання під напругою;
- наявність великою кількості горючої речовини;
- наявність шляхів поширення полум'я з ускладнених до них доступом (кабельні тунелі);
- наявність великої кількості небезпечних чинників пожежі.

Під час воєнних дій до них додається ще один – ймовірність повторної ракетної атаки під час ліквідації пожежі.

У таких умовах пріоритетним завданням є забезпечення безпеки особового складу, що задіяний на гасіння пожежі. Одним з найбільш сучасних способів уникнення впливу небезпечних чинників пожежі на пожежних-рятувальників та невілювання втрат особового складу від ворожих обстрілів є застосування робототехніки під час гасіння пожежі.

У 2022 році підрозділи ОРС ЦЗ вже почали отримувати пожежних роботів, призначених для дистанційного гасіння пожежі [5]. Так, сучаний тактичний робот Magirus Wolf R1 дає можливість гасити складні пожежі у важкодоступних місцях з мінімальним ризиком для особового складу. Ві змонтований на гусеничному шасі з силою тяги до 4т, має акумулятор ємністю 8,8 кВт/год, 4 статично та 2 динамічно спрямовані камери для нормальної та теплової передачі зображення, 6 світлодіодних прожекторів по 1800 люмен кожен, систему дистанційного керування з радіусом дії до 150 м, ствол з можливістю подачі води або піни з витратою до 2000 л/хв при тиску 10 бар на відстань до 65 метрів.

Ураховуючи обставини, що виникають при пожежах на енергооб'єктах, саме постачання робототехніки з заявленими характеристиками є найбільш доцільним напрямком розвитку технічного оснащення підрозділів ОРС ЦЗ ДСНС України.

Література

27. Аналітична довідка про пожежі та їх наслідки в Україні за 12 місяців 2022 року. – К.: ІДУ ЦЗ, 2023. – 39 с.

28. За час великої війни рф завдала 255 ударів по об'єктах електроенергетики України. – Конкурент. Інформаційне агенство. – Режим доступу: https://konkurent.ua/publication/112861/za-chas-velikoi-viyni-rf-zavdala-255-udariv-po-obektah-elektroenergetiki-ukraini/

29. Шмигаль оцінив масштаби втрат енергетики за рік війни. – Kosatka.media. – Режим доступу: https://kosatka.media/category/elektroenergiya/news/shmigal-ociniv-masshtabi-vtrat-energetiki-za-rik-viyni

30. Основи тактики гасіння пожеж: навч. посіб. / В.В Сировой, Ю.М. Сенчихін, А.А. Лісняк, І.Г. Дерев'янко. – Х.: НУЦЗУ, 2015. – 216 с.

31. Озброїлися роботом: на Рівненщині рятувальники навчаються гасити пожежі тактичною технікою. – Суспільне новини. – Режим доступу: https://suspilne.media/357276-ozbroilisa-robotom-na-rivnensini-ratuvalniki-navcautsa-gasiti-pozezi-takticnou-tehnikou/

УДК 351.861

70. ГЕОІНФОРМАЦІЙНА СИСТЕМА АКУСТИЧНОГО МОНІТОРИНГУ ДЖЕРЕЛ РІЗНОГО РОДУ ЗАГРОЗ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКРУРИ МІСТА

Тютюник В. В.[1], Тютюник О. О.[2], Усачов Д. В. [1]

1 Національний університет цивільного захситу України, Харків, Україна

2 Харківський національний економічний університет імені Семена Кузнеця, Харків, Україна

E-mail: tutunik.vadim.72@gmail.com, tutunik.o@ukr.net, usachovrabotadsns21@gmail.com

Geoinformation system for acoustic monitoring of different sources of threats for objects of critical infrastructure of the city

In the article, continuous and long-term real-time operational monitoring of hazard sources for the normal functioning of critical infrastructure facilities of the city is supposed to be carried out by combining ground-based automated devices for controlling acoustic space and passive location of hazard sources into a monitoring system, as well as receiving and processing information from ground-based acoustic devices control by the situational center, the functioning of which is connected

with the system for the implementation of anti-crisis decisions to prevent, localize and eliminate the consequences of emergency situations.

Сучасні міста, як елементи державної системи управління, є складними та розгалуженими системами з розподілом у просторі та часі параметрів життєдіяльності, які за чисельністю населення поділяються на невеликі, малі, середні, великі тощо, а також за характером спеціальних функцій на промислові, транспортні, наукові, історичні, багатогалузеві.

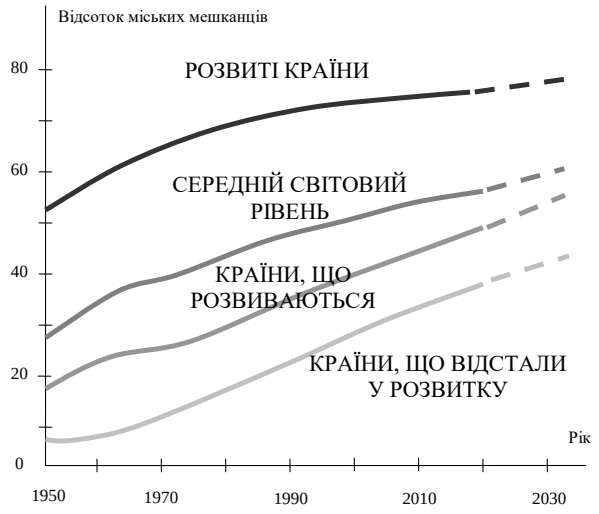


Рис. 1. Динаміка кількості міських мешканців на Земній кулі

Розвиток інфраструктури, будівництво доріг і систем комунікацій істотно впливає на рівень розвитку міст. За прогнозами експертів ООН (рис. 1), в найближчих 15 років зростання міського населення продовжуватиметься і може досягти понад 60% від населення Земної кулі.

Крім того, місто – це не просто скупчення матеріальних об'єктів (житлових і виробничих будівель, комунікацій і так далі), а цілісна, складна, динамічна система, в якій взаємодіють люди, природа, економіка і суспільство.

Зворотнім боком даного процесу є те, що міста у процесі свого функціонування та розвитку створюють передумови для виникнення небезпек, що негативно впливають на стан природно-екологічного, економіко-технічного та соціально-політичного балансу як на території міста так і в регіоні, а також можуть завдати шкоди життєво важливим національним інтересам [1].

Одним із шляхів підвищення ефективності безпеки в містах є необхідність створення ситуаційних центрів, з ефективною геоінформаційною системою моніторингу території міста з метою виявлення та ідентифікації джерел небезпек різної природи.

Тому, авторами безперервний та тривалий у реальному масштабі часу оперативний моніторинг за зоною надзвичайних ситуацій (НС) пропонується здійснювати шляхом об’єднання у систему моніторингу наземних автоматизованих пристроїв контролю акустичного простору та пасивної локації джерел небезпек, а також отримання й обробки інформації від наземних пристроїв акустичного контролю ситуаційним центром, функціонування якого пов’язано з системою виконання антикризових рішень щодо запобігання, локалізації та ліквідації наслідків НС [2, 3].

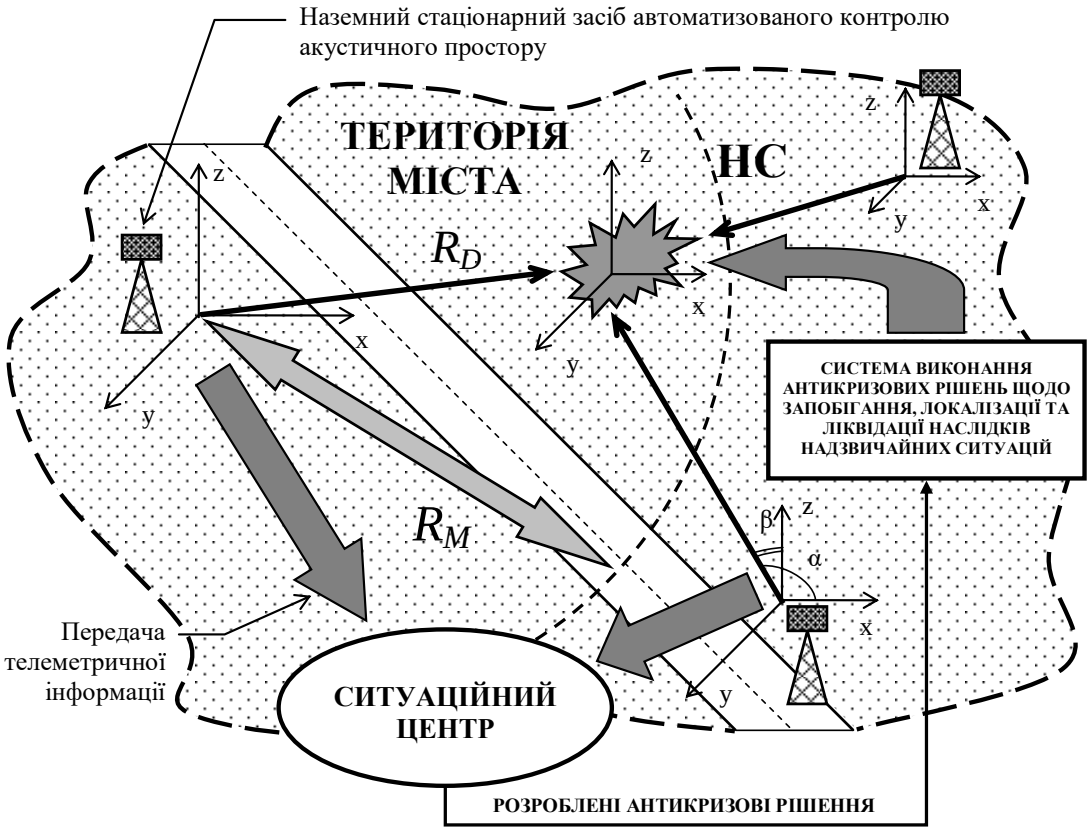


Рис. 2. Схема функціонування на території міста системи наземних стаціонарних засобів автоматизованого контролю акустичного простору, ситуаційного центру, підсистеми зв’язку та передачі телеметричної інформації, а також підсистеми виконання антикризових рішень щодо запобігання, локалізації та ліквідації наслідків надзвичайних ситуацій терористичного характеру

Методи пасивної акустичної локації джерел терористичних небезпек мають свої специфічні особливості, а саме: в умовах відсутності інформації про термін акустичного випромінювання дальність до джерела випромінювання не можливо визначити за даними прийому тільки одного наземного засобу автоматизовано контролю акустичного простору. У зв’язку з цим, для визначення координат джерела терористичної небезпеки необхідно застосовувати комплекс двох або декількох рознесених у просторі засобів автоматизовано контролю акустичного простору, які з’єднані каналами зв’язку та утворюють комп'ютерну мережу; прийом прямого, а не відбитого сигналу, полегшує виявлення і вимір координат джерела терористичної небезпеки, але незнання форми сигналу та наявність інших джерел акустичного випромінювання ускладнює процес оперативного моніторингу за зоною терористичних дій; відсутність передавальних пристроїв при пасивній локації спрощує апаратуру, а також підвищує її енергозбереження та скритність.

Функціональну схему цієї системи наземних стаціонарних засобів автоматизованого контролю акустичного простору, ситуаційного центру, підсистеми зв’язку та передачі телеметричної інформації, а також підсистеми

виконання антикризових рішень щодо запобігання, локалізації та ліквідації наслідків НС, представлено на рис. 2.

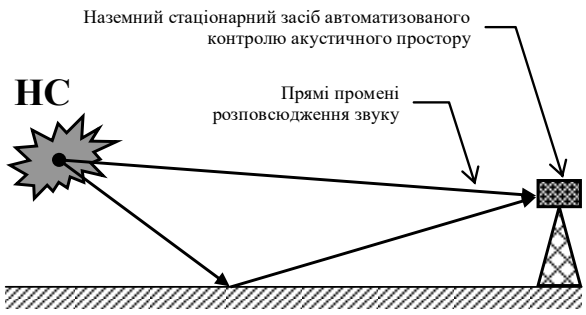
Основним показником ефективності функціонування підсистеми оперативного акустичного моніторингу зони НС на території міста є достовірність ідентифікації джерела небезпеки за видом та місцем виникнення [4].

Фактори, які можуть впливати на достовірність акустичної ідентифікації джерела небезпеки, можливо об’єднати у три групи. До першої групи належать фактори, які характеризують безпосередньо динаміку зміни показників розвитку джерела небезпеки. До другої групи факторів належать тактико-технічні характеристики засобів контролю акустичного простору (метрологічні та експлуатаційні показники засобів отримання та обробки інформації). До третьої групи факторів належать географічні та фізико-хімічні характеристики місця виникнення джерела небезпеки та середовища розповсюдження інформаційного акустичного сигналу.

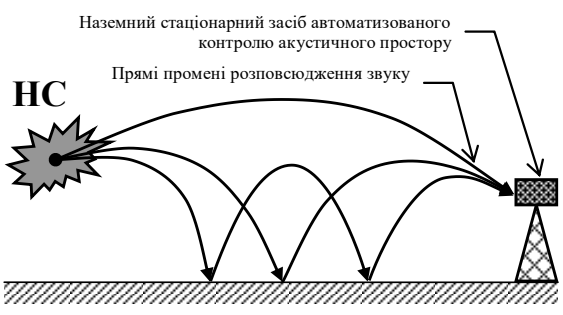
Розглядаючи умови приземного розповсюдження в атмосфері акустичних хвиль від джерела небезпеки, необхідно враховувати високу чутливість звукового випромінювання в атмосфері до значення таких метеорологічних параметрів, як швидкість та напрямок вітру, температура, вологість повітря та атмосферний тиск, а також до їх змін з висотою. Суттєвий вплив на дальність приземного розповсюдження звуку також здійснюють характеристики турбулентності, підстилаючої поверхні, геометрії поширення та джерела звуку.

За умов приземного розповсюдження в атмосфері звуку від джерела небезпеки на великі відстані характеристики акустичних хвиль визначаються головним образом рефракцією на градієнтах температури та швидкості вітру, що призводить до виникнення хвилевідного (рис. 3, б) та антихвилевідного (рис. 8, в) режимів. У першому випадку промені загибаються до низу з багаторазовим відбитком від Землі. Цьому режиму поширення звуку притаманні відносно малі значення ослаблення звуку. В іншому випадку промені загинаються вгору і зона акустичної тіні виникає біля Землі на певній відстані від джерела НС.

а)



б)



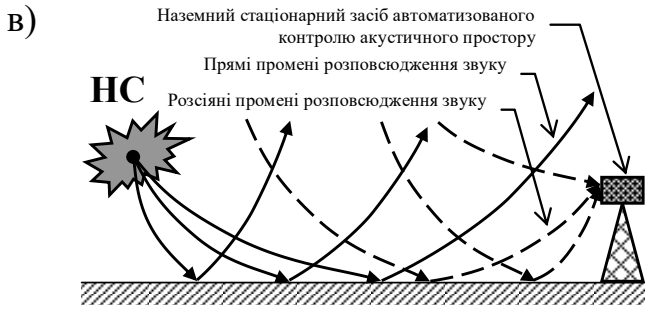


Рис. 3. Променеві картини розповсюдження звуку в атмосфері від джерел терористичних дій до наземних стаціонарних засобів автоматизованого контролю акустичного простору в різних метеорологічних умовах: а) нейтральний режим; б) хвилевідний режим (приведено тільки промені типу "верх–низ"); в) антихвилевідний режим

Тому, тільки дуже слабкий звук, розсіяний турбулентними неоднорідностями у верхніх шарах атмосфери, проникає у цю зону. Ці два режиму розповсюдження звуку працюють в основному на відстанях які перевищують 1 км.

В той же час, територія великого міста характеризується функціонуванням динамічно-розгалуженої системи забудови на великій площі поверхні Земної кулі, де локально та ймовірносно виникають різні атмосферні процеси, а також існує велика концентрація на одиниці площі об’єктів різного функціонального призначення, будівель та споруд з різною кількістю поверхів, автотранспортів шляхів тощо. Всі ці фактори сприяють виникненню перешкод для ефективного прийому інформаційного сигналу засобів контролю акустичного простору. Тому, розглядаючи умови акустичного моніторингу за зоною НС на територія такого міста виникає доцільність встановлення засобів контролю акустичного простору на відстанях які не перевищують 1 км.

В таких умовах виникає необхідність аналізу ефективності функціонування засобів контролю акустичного простору у режиму слабкої рефракції звуку, який можливо віднести до випадку прямого поширення звукової хвилі в точку спостереження. При цьому режимі (рис. 3, а) в точку спостереження приходить тільки два променя: прямий промінь, який не має точки повороту, та відбитий від Землі промінь, де променева картина розповсюдження звуку характеризується зневажливо малою кривизною траєкторій променів. Розрахунок звукових тисків у цьому випадку можливо виконати за виразом:

$$L_{R_M}(f) = L_s(f) + L_{abs}(f) + L_t(f) + L_e(f) + L_{div}(f) + L_{pat}(f), \qquad (1)$$

де R_M – радіус зони імовірнісної акустичної ідентифікації терористичних дій, $L_{R_M}(f)$ – рівень звукового тиску на вході наземного стаціонарного засобу контролю акустичного простору на частоті f від джерела терористичних дій, які виникли на межі зони достовірної акустичної ідентифікації, $L_s(f)$ – звуковий тиск від джерела терористичних дій, що перерахованих до звукового тиску на відстані одного метра від джерела, $L_{abs}(f)$ – вклад класичного та молекулярного поглинання звуку у атмосфері, $L_t(f)$ – вклад турбулентного послаблення звуку, $L_e(f)$ – вклад приземного ослаблення звуку (враховується вплив інтерференції прямої та відбитої хвилі), $L_{div}(f)$ – вклад кутової розбіжності, $L_{pat}(f)$ – доданок, який враховує характеристики діаграми направленості засобу контролю акустичного простору.

Рівняння (1) виражає закон збереження енергії та є рівнянням енергетичного балансу. Всі складові правої частини цього рівняння, крім складової $L_s(f)$, мають, як правило, від'ємне значення. Для достовірної акустичної ідентифікації джерела небезпеки та визначення на території міста місця виникнення НС необхідно виконання наступних умов: $R_D \le R_M$.

Література

1. Андронов В.А. Дівізінюк М.М., Калугін В.Д., Тютюник В.В. Науково-конструкторські основи створення комплексної системи моніторингу надзвичайних ситуацій в Україні: Монографія. Харків: Національний університет цивільного захисту України, 2016. 319 с.
2. Рубан І.В., Тютюник В.В., Тютюник О.О. Особливості створення системи підтримки прийняття антикризових рішень в умовах невизначеності вхідної інформації при надзвичайних ситуаціях. Науковий журнал "Сучасні інформаційні технології у сфері безпеки та оборони". Київ: Національний університет оборони України імені Івана Черняховського. 2021. №1(40). С. 75–84.
3. Тютюник В.В., Ященко О.А., Рубан І.В., Тютюник О.О. Особливості функціонування системи ситуаційних центрів на різних стадіях розвитку надзвичайних ситуацій. Науковий журнал "Сучасні інформаційні технології у сфері безпеки та оборони". Київ: Національний університет оборони України імені Івана Черняховського. 2022. Вип. 1(43). С. 41–52.
4. Дивизинюк М., Гончаренко Ю., Гончаренко Д. О проблеме расчета дальности приема акустической информации с открытых площадок. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Київ: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", 2012. № 1(23). С. 29–35.

УДК 004.896

71. РОЗВИТОК МЕТОДУ ПІДТРИМКИ ТА ПІДВИЩЕННЯ ЗВ'ЯЗНОСТІ БЕЗПРОВОДОВИХ МЕРЕЖ ІЗ ВИКОРИСТАННЯМ БПЛА

Чумаченко С.М.[1], Лисенко О. І.[2], Новіков В.І.[3], Фуртат О.В.[4], Фуртат С.О.[5], Сушин І. О.[6]

[1] Національний університет харчових технологій, Київ, Україна,
[2,3,6] Навчально-науковий інститут телекомунікаційних систем Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна,
[4,5] Таврійський національний університет імені В.І. Вернадського.
E-mail: s_chum@ukr.net, lysenko.a.i.1952@gmail.com, novikov1967@ukr.net, s30041983@meta.ua, furtatsergij@gmail.com, rubin268@ukr.net

Development of the method of support and increase of connectivity wireless networks using UAVs

The proposed method solves the problem of combining the movement control of existing UAVs and the deployment of new UAVs so that the number of newly deployed UAVs to support the communication of ground subscribers can be minimized. Improves the mathematical model of ensuring the connectivity of episodic radio networks using UAVs.

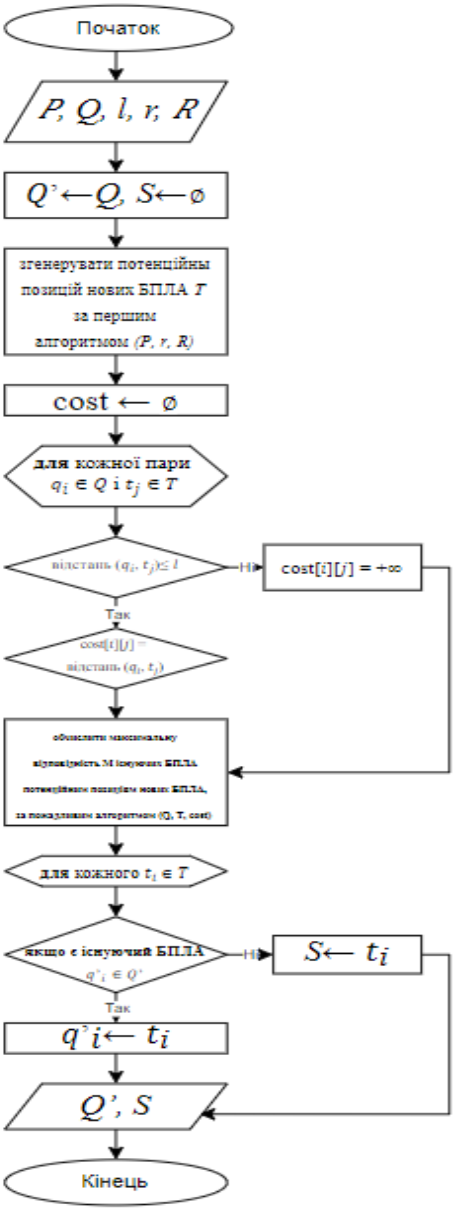
An optimization solution is presented that combines the motion control of existing UAVs and the deployment of newly added UAVs. The movement of land mobile subscribers leads to a rapid and unpredictable change in the topology of episodic radio networks, which can lead to disruption of network connectivity and loss of communication between some subscribers.

Increasing the connectivity of such networks is possible through the introduction of new additional air-based nodes (UAVs), which have a larger area of radio coverage and can connect disconnected sections of the network. To date, the problem of optimal management of the position of such UAVs is not sufficiently solved, namely the problem of combining the movement control of existing UAVs and the deployment of new UAVs so that the number of newly deployed UAVs to support the communication of ground subscribers can be minimized.

Забезпечення зв’язності епізодичних радіомереж із використанням БПЛА представлено в трьох алгоритмах:
1) Алгоритм розміщення нових БПЛА без урахування переміщення існуючих БПЛА
2) Алгоритм розгортання нових БПЛА до початку переміщення існуючих БПЛА.
3) Алгоритм розгортання нових БПЛА під час переміщення вже існуючих [1-3].

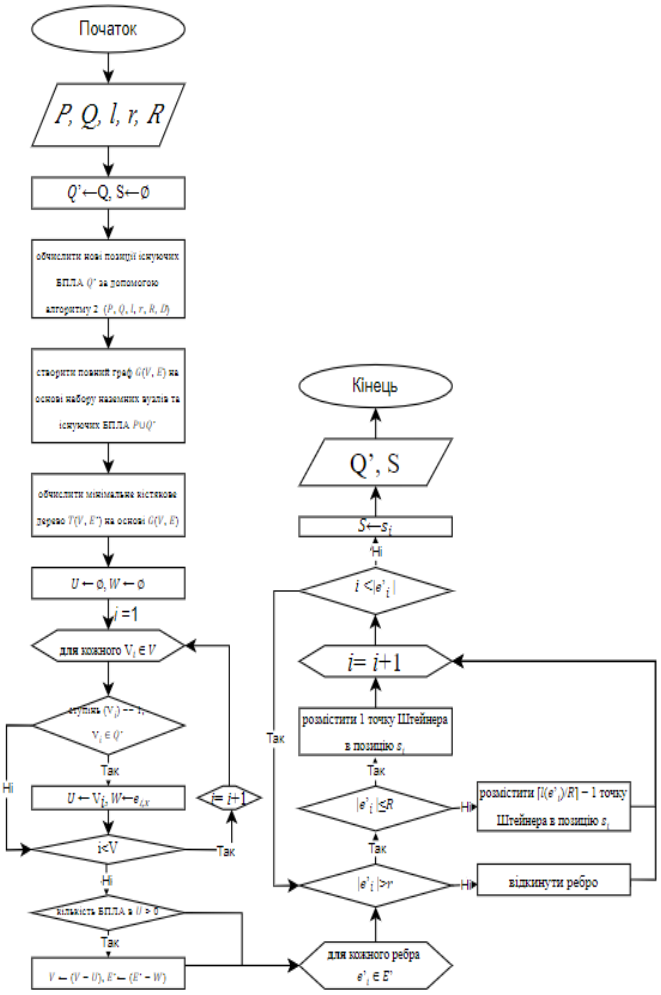
1. Алгоритм розміщення нових БПЛА без урахування переміщення існуючих БПЛА. Оскільки мобільні точки Штайнера не враховуються, евристичний алгоритм МДШ не може бути використаний безпосередньо для задачі мінімального дерева Штейнера з існуючими мобільними точками Штейнера із обмеженням довжини ребер графу мережі. Тут просто беруться методи Лін і Сюе, як порівняльний метод. Оскільки цей метод не враховує існуючі БПЛА, ми називаємо цей метод алгоритмом розміщення нових БПЛА

без урахування переміщення існуючих БПЛА. Даний алгоритм обчислює мінімальну кількість нових БПЛА, необхідну для підключення всіх наземних вузлів. Жоден з існуючих БПЛА не буде повторно використаний для підключення наземних мобільних епізодичних радіомереж. Таким чином, кількість необхідних нових БПЛА, обчислена даним алгоритмом, має бути верхньою межею інших алгоритмів, що враховують розміщення (переміщення) існуючих БПЛА. [3-6]



2. Алгоритм розгортання нових БПЛА до початку переміщення існуючих БПЛА. Основна ідея алгоритму розгортання нових БПЛА до початку переміщення існуючих БПЛА показана наступним чином. По-перше, використовується алгоритм розміщення нових БПЛА без урахування переміщення існуючих БПЛА для створення кандидатських позицій нових доданих БПЛА без урахування існуючих БПЛА. Потім ми порівнюємо наявні БПЛА з кандидатами на новододані БПЛА. Збіг між наявним БПЛА та позицією-кандидатом нового доданого БПЛА означає, що новий доданий БПЛА буде

замінено існуючим БПЛА шляхом переміщення цього існуючого БПЛА на позицію кандидата. Оскільки діапазон руху існуючих БПЛА обмежений, кількість збігів також обмежена. Тут ми використовуємо алгоритм алгоритми розгортання нових БПЛА до початку переміщення існуючих БПЛА (DBM), щоб знайти максимальні збіги, щоб можна було мінімізувати кількість необхідних нових БПЛА.). Основна ідея алгоритму переміщення існуючих БПЛА до початку розгортання нових БПЛА полягає в наступному. По-перше, використовується евристична функція для створення нових позицій існуючих БПЛА $Q`$. Потім об'єднується набір наземних вузлів $P$ і набір існуючих БПЛА з новими позиціями $Q`$ у великий набір вузлів $P \cup Q`$. Після цього ми генеруємо мінімальне охоплююче дерево T над набором $P \cup Q`$, а потім процес відкидання існуючих БПЛА буде використовуватися для вирізання всіх існуючих БПЛА під 1 градус в дереві T, поки всі існуючі БПЛА в дереві не матимуть принаймні два сусідні вузли. [4-8] Для решти піддерева $T`$ з $T$ нові БПЛА будуть додані до країв $T`$, довжина яких перевищує r.



3. Алгоритм розгортання нових БПЛА під час переміщення існуючих БПЛА. Основна ідея алгоритму розгортання нових БПЛА під час переміщення існуючих БПЛА полягає в наступному. Спочатку генерується повний граф $G(V, E)$ на базових вузлах і сортуємо всі ребра E у порядку збільшення довжини. Тоді розглянемо всі ребра ei,j у множині E, що довжина ребра не більше r, а вершини

ребра належать різним компонентам. Після цього кроку ми отримаємо кілька компонентів, які складаються із підключених заземлюючих вузлів. Тепер будемо рекурсивно переміщати існуючі БПЛА та додавати нові БПЛА для з'єднання розділених компонентів, доки всі розділені компоненти не будуть з'єднані в один компонент. У кожному циклі ми спробуємо з'єднати всі пари вершин Vi і Vj, які належать різним компонентам, за допомогою двох різних методів. Один із методів використовує існуючі БПЛА для встановлення ланцюга зв'язку між Vi і Vj шляхом переміщення БПЛА на певні позиції. Нові БПЛА будуть додані до країв ланцюга, довжина яких перевищує r. Інший метод не враховує існуючі БПЛА і просто намагається налаштувати ланцюжок зв'язку між Vi і Vj, додаючи нові БПЛА. Кількість нових доданих БПЛА за допомогою цих двох методів буде порівнюватися, і менша кількість буде записана як мінімальна кількість нових БПЛА (MNN) для з'єднання Vi і Vj. Для з'єднання двох розділених компонентів у цьому циклі буде обрана пара вершин, яка має мінімальний MNN. Нові позиції існуючих БПЛА та позиції нових доданих БПЛА, створених для з'єднання цієї пари вершин, також будуть записані як частина кінцевого результату.[6-9]

Таким чином, запропоновано три нових алгоритми розміщення, як нових так і існуючих БПЛА:

1.Розгортання нових БПЛА до початку переміщення існуючих БПЛА;
2.Переміщення існуючих БПЛА до початку розгортання нових БПЛА;
3.Розгортання нових БПЛА під час переміщення існуючих БПЛА.

Перші два алгоритми розділяють спільну проблему на проблему розгортання нових БПЛА та проблему керування рухом існуючих БПЛА. Алгоритм розгортання нових БПЛА до початку переміщення існуючих БПЛА оптимізує розгортання нових БПЛА перед переміщенням існуючих БПЛА, а алгоритм переміщення існуючих БПЛА до початку розгортання нових БПЛА вирішує проблему навпаки. Алгоритм розгортання нових БПЛА під час переміщення існуючих БПЛА – це змішаний алгоритм, який перехресно вирішує проблему переміщення та розгортання. Імітаційні експерименти показують, що всі алгоритми розміщення нових БПЛА з урахуванням переміщення існуючих БПЛА мають кращу продуктивність з точки зору кількості нових БПЛА, ніж алгоритми без урахуванням переміщення існуючих БПЛА. Алгоритм розгортання нових БПЛА під час переміщення існуючих БПЛА завжди кращий за алгоритми розгортання нових БПЛА до початку переміщення існуючих БПЛА і переміщення існуючих БПЛА до початку розгортання нових БПЛА і може підвищити продуктивність максимум до 70% у порівнянні з алгоритмом алгоритми розгортання нових БПЛА до початку переміщення існуючих БПЛА. [7-9]

Всі поточні положення наземних вузлів і існуючих БПЛА відомі. Також, припускається, що немає фізичних перешкод, які впливають на мобільність БПЛА або радіоканали. Цю проблему можна описати наступним чином: враховуючи набір наземних вузлів і набір існуючих БПЛА, знайти нові позиції для існуючих БПЛА та позиції для нових доданих БПЛА, щоб сформувати дерево, що охоплює всі наземні вузли, щоб кількість нових доданих БПЛА було зведено до мінімуму.

У цій проблемі є два обмеження. Одним з них є відстань між новим положенням і поточним положенням кожного існуючого БПЛА, яка не перевищує заданий діапазон руху. Інше полягає в тому, що довжина кожного ребра в дереві не перевищує заданий діапазон зв'язку.

Математична постановка задачі мінімального дерева Штейнера з існуючими мобільними точками Штейнера із обмеженням довжини ребер графу мережі. Оскільки ця задача подібна до задачі дерева Штейнера з мінімальною кількістю точок Штейнера, в даному розділі сформульовано цю задачу як задачу мінімального дерева Штейнера з існуючими мобільними точками Штейнера із обмеженням по довжині ребер графу мережі. Точки Штейнера тут означають БПЛА, а обмеження по довжині ребер графу мережі — це діапазон максимальної дальності зв’язку вузла мережі, що визначається енергетикою радіолінії (потужністю передавача, чутливістю приймача, характеристиками антени і т.п.), місцевістю та різними завадами [8].

Формальне визначення проблеми мінімального дерева Штейнера з існуючими мобільними точками Штейнера із обмеженням довжини ребер графу мережі показано наступним чином:

Нехай існує набір наземних вузлів P, що характеризується поточною позицією кожного вузла p, набір існуючих БПЛА Q, що характеризується поточною позицією кожного існуючого БПЛА, діапазон руху БПЛА l, дальність зв'язку наземного вузла r, дальність зв'язку земля-повітря R і дальність зв'язку повітря-повітря D.

Таким чином $r < R$,

$$P= \{p_1,p_2,\dots,p_n\}, \quad (1)$$
$$Q = \{q_1,q_2,\dots,q_m\},$$

де n - кількість наземних вузлів, m - кількість існуючих БПЛА.

Нові позиції існуючих БПЛА складатимуть множину U, позиції нових доданих БПЛА – S, а дерево графу мережі T складатиметься з сукупного набору вузлів (P, U та S) та набору ребер E:

$$U= \{u_1,u_2,\dots,u_m\},$$
$$S = \{s_1,s_2,\dots,s_k\} \quad (2)$$
$$T= \{P \cup U \cup S, E\}.$$

Тоді математичну постановку задачі можна сформулювати наступним чином: знайти мінімальну кількість k нових доданих БПЛА, розміщення яких забезпечить зв’язність епізодичної радіомережі

$$min(k). \quad (3)$$

при виконанні наступних обмежень та збереження цілісності мережі:

$$\Omega_1: |e_{i,j}| \le r, (e_{i,j} \in E, i,j \in P),$$
$$\Omega_2: |e_{i,j}| \le R, (e_{i,j} \in E, i \in P, j \in U \cup S), \quad (4)$$
$$\Omega_3: |e_{i,j}| \le D, (e_{i,j} \in E, i, j \in U \cup S),$$
$$|u_i - q_i| \le l, \ 1 \le i \le m,$$

де |ei,j | - довжина ребра графу мережі між вузлами і та j.

Під цілістістю мережі розуміється наявність лише одної компоненти зв’язності графу мережі. Перевірка цілісності мережі можливо шляхом побудови

мінімального дерева Штейнера (МДШ) графу (наприклад, згідно алгоритму Пріма) та перевірка кожного ребра дерева на виконання умови Ω1, Ω2, Ω3. Якщо умови виконуються, то мережа є структурно зв'язаною на момент часу t, інкше – необхідне певне управлінське рішення (наприклад, вивід нового (переміщення існуючого) БПЛА.

Після тестування продуктивності запропонованих алгоритмів у різних сценаріях, зі зміною параметрів моделювання (включаючи кількість наземних вузлів, кількість існуючих БПЛА, дальність зв'язку та дальність руху), можна зробити висновок, що алгоритми з урахуванням переміщення існуючих БПЛА завжди мають кращу продуктивність, ніж метод без урахування переміщення існуючих БПЛА з точки зору кількості нових доданих БПЛА. Серед трьох алгоритмів розміщення нових БПЛА з урахуванням переміщення існуючих БПЛА, алгоритм переміщення існуючих БПЛА до початку розгортання нових БПЛА кращий за алгоритм розгортання нових БПЛА до початку переміщення існуючих БПЛА у більшості сценаріїв, а алгоритм розгортання нових БПЛА під час переміщення існуючих БПЛА завжди має найкращу продуктивність у всіх сценаріях. У деяких сценаріях алгоритм розгортання нових БПЛА під час переміщення існуючих БПЛА може зменшити щонайбільше 70% нових БПЛА порівняно з алгоритмом розгортання нових БПЛА до початку переміщення існуючих БПЛА.

Висновки. БПЛА мають кілька унікальних характеристик, придатних в забезпеченні ретрансляції пакетів в мобільних епізодичних радіомережах.

По-перше, гнучкість руху БПЛА може розширити сферу застосування наземних мереж, особливо в сценаріях з перешкодами.

По-друге, БПЛА можуть взаємодіяти з наземними вузлами в прямій видимості, що може поліпшити зв'язність пропускну здатність між наземними вузлами. І останнє, але не менш важливе: БПЛА інтегровані з системою зв'язку, обчислення та управління, різними датчиками, можуть досліджувати навколишнє середовище та адаптивно керувати їхнім рухом. Адаптивність БПЛА робить їх придатними для надання ретрансляційних послуг для мобільних епізодичних радіомереж, які мають динамічну топологію мережі. В існуючих роботах при розгортанні БПЛА не враховано ситуацію, що деякі БПЛА вже були розгорнуті на місцях. Переміщення наземних мобільних абонентів епізодичних радіомереж моде призвести до того, що існуючі БПЛА не забезпечувати з'язність усіх наземні вузлів. Отже, необхідно вивести нові БПЛА, щоб підтримувати зв'язок наземних абонентів. Але щоб мінімізувати кількість нових доданих БПЛА, необхідно враховувати як переміщення існуючих БПЛА, так і розгортання нових БПЛА. Це спільна задача оптимізації, яка оптимізує як розгортання, так і керування рухом кількох БПЛА.

Література

1. Lysenko, O., Valuiskyi, S., Yavisya, V., Tachinina, O., Novikov, V., Sushyn, I. Method of operational calculation of coordinates of intermediate route points of flying

information robot, in: Information and Telecommunication Sciences, No. 1, 2022, pp.27 – 34. DOI: https://doi.org/10.20535/2411-2976.12022.27-34
2. Lysenko, O., Romaniuk, V., Romaniuk, A., Novikov, V., Yavisya, V., Sushyn, I. (2021). The Method of Using a Telecommunication Air Platform as a Flying Info-Communication Robots. In: Ilchenko, M., Uryvsky, L., Globa, L. (eds) Progress in Advanced Information and Communication Technology and Systems. MCiT 2021. Lecture Notes in Networks and Systems, vol 548. Springer, Cham. https://doi.org/10.1007/978-3-031-16368-5-18
3. Valuiskyi S. Heuristic algorithms for finding the minimum steiner tree in the problem of optimizing the deployment and motion control of several flying information and telecommunication robots / S. Valuiskyi, O. Lysenko, S. Chumachenko, V. Novikov, O. Guida, I. Sushyn // Information and telecommunication sciences, Volume 13, Number 2. – 2022. – P. 53-61. DOI: https://doi.org/10.20535/2411-2976.22022.53-61
4. Романченко І.С., Лисенко О.І., Чумаченко С.М., Данилюк С.Л., Новіков В.І., Тачиніна О.М., Кірчу П.І., Валуйський С.В. Моделі застосування інформаційно-телекомунікаційних технологій на основі безпілотних авіаційних комплексів у надзвичайних ситуаціях. – К.: НАУ, 2016. – 332 с. ISBN 978-966-932-011-7 .
5. Новіков В.І., Лисенко О.І., Валуйський С.В., Гуйда О.Г. Математичні моделі, методи та алгоритми оптимізації показників функціонування безпроводових сенсорних мереж із мобільними сенсорами й телекомунікаційними аероплатформами. Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки. Том 31 (70) № 3 2020. Частина 1, стор. 54-64. Сторінка журналу: www.tech.vernadskyjournals.in.ua ISSN 2663-5941 (Print). ISSN 2663-595X
6. Uryvsky L., Lysenko O., Novikov V., Osypchuk S. Control Methods Research of Indicators for Intelligent Adaptive Flying Information-Telecommunication Platforms in Mobile Wireless Sensor Networks. In: Klymash M., Beshley M., Luntovskyy A. (eds) Future Intent-Based Networking. Lecture Notes in Electrical Engineering, vol 831. P. 444-467. – 2022. Springer, Cham. https://doi.org/10.1007/978-3-030-92435-5-25
7. Romaniuk V. Development of methods of positioning, localization and data collection from nodes of a free mobile sensor network using intelligent adaptive telecommunication aeroplatforms / V. Romaniuk, O. Lysenko, V. Novikov, I. Sushyn// Information and Telecommunication Sciences. – № 2. – 2021. – pp. 40 – 49. DOI: https://doi.org/10.20535/2411-2976.22021.40-49
8. Olexander Lysenko, Olena Tachinina, Valeriy Novikov, Iryna Alekseeva, Serhii Chumachenko, Andrii Tureichuk: Expert-modeling decision support system for the deployment and management of a wireless sensor network with mobile sensors and telecommunication air platforms in the emergency zone . SECURITY FORUM 2021 14th Annual International Scientific Conference February 10 th, 2021 at Matej Bela University in Banská Bystrica, Slovakia Conference Proceedings Banská Bystrica, Slovakia 2021, c. 249-258. ISBN 978-80-973394-5-6 Link to the web-page: https://www.fpvmv.umb.sk/fakulta/bezpecnostne-forum. Link for the direct download: https://www.fpvmv.umb.sk/drive/2021-11-04/security-forum-2021.pdf

9. Dan Popescu, Florin Stoican, Grigore Stamatescu, Oana Chenaru, Loretta Ichim. A Survey of Collaborative UAV–WSN Systems for Efficient Monitoring Sensors, 2019, 19(21), 4690; doi.org/10.3390/s19214690.

УДК 504.75.05/.06 +502.35

72. ЕКОЛОГІЧНА БЕЗПЕКА ЕКСПЛУАТАЦІЇ АВТОМОБІЛЬНИХ ДОРІГ УКРАЇНИ. МЕТОДИ ТА ЗАСОБИ ОЦІНЮВАННЯ ТА КІБЕРБЕЗПЕКА

Г.В. Адамова, Л.А. Пісня
Український науково-дослідний інститут екологічних проблем

Environmental safety of operation of highways of ukraine. Methods and means of evaluation and cybersecurity

By applying a systems approach, it has been determined that the environmental safety of roads is a complex, multi-criteria, multifactor, systemic, hierarchical, scientific and applied problem of forming and making managerial decisions on the application of environmental measures.

The authors managed to generalize the results of previous scientific research and, through analytical eco-expert assessment, composed a spectrum of complex measures to reduce the impact on the environment of the "car-road-environment" system. A hierarchical structure for assessing the complex impact of the system on environmental objects, taking into account measures to counteract, fully complies with general requirements for expert-analytical research using the adapted Thomas Saaty's method of hierarchy analysis for environmental tasks. The authors organized and carried out an eco-expert analytical assessment of the effectiveness of the generalized complex measures of the studied system on environmental safety, protection of the natural environment, and the preservation of the population's health as one of the components of critical infrastructure for the sustainable development of the territory of Ukraine using the hierarchy analysis method. According to the results of the environmental-analytical assessment, it has been determined that effective complex measures for reducing the impact of the "vehicle-road-environment" system on the environmental components are as follows: for air - ecologization of transport with a value of 35.1%, and ecologization of the road surface - 24.7%; for water bodies - technological provision of the normative quality of surface wastewater - 37.8%, ecologization of transport - 23.1%; for soil - ecologization of the road surface - 35.0% and preservation of the integrity of road structures - 23.8%; for biota - ecologization of the road surface - 33.5%, eco-economic levers - 22.0%; for human health - ecologization of the road surface - 30.4%, eco-economic levers - 20.9%.

Вступ. Мережа автомобільних доріг забезпечує транспортний зв'язок між містами, регіонами та країнами, дозволяє розвивати торгівлю та перевезення, використовувати швидкий та безпечний доступ до медичної допомоги, інших невідкладних послуг, швидкого доступу до місць небезпеки, таких як пожежі, стихійні лиха, повені тощо. У зв'язку з цим багато країн надають великого значення безпеці та надійності автомобільних доріг, що має важливе значення для економічного розвитку та розвитку країни загалом. Для цього використовуються різні методи, такі як система моніторингу та стану доріг, а

також засоби зв'язку та інформаційні технології, що дозволяють швидко реагувати на можливі ситуації контролю.

У зв’язку з військовою агресією Російської Федерації постало вкрай важливе питання щодо всебічного захисту критичної інфраструктури нашої країни. Необхідно зазначити, що екологічна безпека автомобільних доріг є одним із об’єктів кібербезпеки критичної інфраструктури держави.

Загалом важливо усвідомлювати взаємозв'язок між екологічною безпекою та кібербезпекою та застосовувати цілісний підхід до забезпечення безпеки та захищеності критично важливої інфраструктури. Це включає реалізацію заходів щодо захисту навколишнього середовища під час експлуатації автомобільних доріг, з обов’язковим забезпеченням кібербезпеки цифрових систем та мереж.

Аналіз попередніх досліджень. Екологічна безпека автомобільних доріг – це комплекс заходів, спрямованих на мінімізацію негативного впливу експлуатації автомобільних доріг на складові довкілля.

Автомобільні дороги, разом із транспортними засобами, що рухаються ними, створюють надзвичайно інтенсивний вплив (параметричний, інгредієнтний) на складові прилеглих територій. Екодеструктивний вплив є масштабним через велику протяжність та розгалуженість дорожньої мережі та високу мобільність транспортних потоків разом із постійно зростаючою кількістю транспортних засобів.

Для зниження впливу на довкілля автотранспорту науково обґрунтовано ряд проектно-інженерно-технічних рішень, спрямованих на екологізацію транспортних засобів [1-3]:

- встановлення спеціальних індикаторів на деталях і вузлах, що швидко зношуються (сигналізують про необхідність їх заміни);
- використання у виробництві авто екологічно-чистих матеріалів;
- своєчасне проведення технічного обслуговування і регулювання систем запалювання та живлення двигунів внутрішнього згоряння (ДВЗ);
- впровадження новітніх систем нейтралізації та сажовловлювачів відпрацьованих газів;
- вдосконалення конструкції та технології виробництва ДВЗ;
- проведення систематичного контролю складу відпрацьованих газів;
- збільшення використання альтернативних видів пального;
- застосування якісних паливних та мастильних матеріалів з поліпшеними екологічними властивостями, нетоксичних паливних добавок;
- стимулювання оновлення автомобільного парку та використання екологічно безпечного транспорту.

Традиційно найбільш шкідливом впливом на довкілля від автомобільного транспорту вважаються викиди відпрацьованих газів двигунів внутрішнього згоряння, що являють собою складну багатокомпонентну суміш газів, парів, крапель рідин і дисперсних твердих частинок. В Україні обсяги викидів забруднюючих речовин у розрахунку на один транспортний засіб, розраховують згідно з "Методикою розрахунку викидів забруднюючих речовин та парникових газів у повітря від транспортних засобів" [4].

Також задля забезпечення екологічної безпеки системи «автомобіль-дорога-середовище» (АДС) необхідно проводити роботи щодо контролю якості шарів дорожнього полотна, використання для побудови екологічно-чистих матеріалів, та моніторингу їх стану в процесі експлуатації.

На безпечність та екологічну стабільність автомобільних доріг впливають як природні так і техногенні фактори. Зокрема, порушення водного балансу підземних вод, що виникає під час експлуатації автомобільної дороги може викликати підтоплення полотна дороги і в кінцевому випадку призводить до руйнації покриття. Вирішенням цієї проблеми може слугувати влаштуванням протифільтраційних завіс вздовж автодоріг, що забезпечують відведення ґрунтових вод та поверхневого стоку з доріг [5]. Забруднення придорожнього простору поверхневими стічними водами з полотна дороги упереджується створенням системи водовідведення з очищенням цих вод. Для зменшення концентрації забруднюючих речовин у дощових стічних водах, а також зниження їх накопичення на полотні дороги, необхідним є механізоване прибирання та інтенсивне миття дорожнього покриття з наступною очисткою мийних вод [6]. У боротьбі зі зниженням розповсюдження шуму автомобільних доріг використовуються лісосмуги. Структура посадок дерев має бути багатоярусна із суцільним закриттям кронами рослин придорожнього простору, що досяжне використанням чагарників. Навіть досить вузькі лісосмуги можуть бути ефективними у зниженні шуму дороги за умови, що смуга насаджень добре спроектована. Так відомо, що оптимізована смуга дерев шириною 15 м може конкурувати із захисним екраном висотою 1 м або навіть 2 м [7,8].

Суттєвою перевагою лісозахисних смуг у відношенні до шуму захисних екранів є широкий багатоспектральний та виключно природний спосіб захисної дії. Зелені насадження очищають повітря від пилу і газів, а зокрема суттєво зменшують шкідливу концентрацію відпрацьованих газів авто. Цей процес відбувається шляхом затримання та повільного розсіювання кронами дерев газів у верхні шари повітря, а також поглинанням забруднюючих газів зеленими листям внаслідок дихання та осадження твердих часток.

Завдяки своїй поглинаючій властивості зелені насадження можуть слугувати індикаторами інтенсивності накопичення забруднюючих речовин в придорожній смузі і використовуватись як показники під час моніторингу впливу автомобільних доріг на довкілля [9]. Також, фіторемедіація це один із шляхів вирішення проблеми забруднення вздовж автомобільних доріг. Науково обґрунтований вибір рослин та широке впровадження фіторемедіації це один із перспективних напрямів стійкого та економічно ефективного вирішення проблеми забруднення придорожнього простору [10, 11].

Достатньо ефективними методами захисту придорожнього простору від забруднень, що спричиняються діяльністю автомобільних доріг, є застосування комплексних захисних споруд [11].

Найбільш перспективним у цьому напрямку є використання для моніторингу стану навколишнього середовища вздовж доріг безпілотних літальних апаратів (дронів). Дрони можуть бути оснащені різними датчиками та

камерами, які можуть збирати дані про стан повітря, ґрунту, води, рослинності та тварин поблизу доріг. Вони можуть швидко та легко охоплювати великі території та збирати дані, що дозволяє скоротити витрати на обстеження порівняно з традиційними методами. Дрони дозволяють збирати інформацію з високою точністю та деталізацією, не вимагаючи участі людини у самому процесі і можуть бути використані для швидкого виявлення та адекватного оперативного аналізу різноманітних екологічних проблем та прийняття ефективних та своєчасних управлінських рішень [12, 13].

Таким чином, узагальнюючи результати наукових досліджень попередників можна стверджувати, що екологічна безпека автомобільних доріг є комплексною, багатокритеріальною, багато факторною, системною, ієрархічною, науково-прикладною проблемою формування та прийняття управлінських рішень щодо застосування природоохоронних заходів.

Мета роботи: застосувавши системний підхід та узагальнюючи результати наукових досліджень попередників шляхом аналітичного еколого-експертного оцінювання скомпонувати та узагальнити спектр комплексних заходів зменшення впливу на навколишнє середовище системи «автомобіль-дорога-середовище»(АДС);

провести експерно-аналітичну оцінку дієвості комплексних заходів спрямованих на екологічну безпеку, охорону природного середовища та збереження здоров'я населення та сталого розвитку системи АДС як однієї зі складових критичної інфраструктури території України;

визначити ключові питання кіберзахитсу в системі АДС, що потребують подальшого вивчення та провадження.

Виклад основного матеріалу. Математична постановка завдання на дослідження зменшення впливу АДС на довкілля в загальному вигляді може бути представлена як графічно так і математично у двох підходах: традиційному загальноприйнятому – на (рис.1) і формулі (1) та новому, запропонованому авторами на (рис.2) та формулі (2):

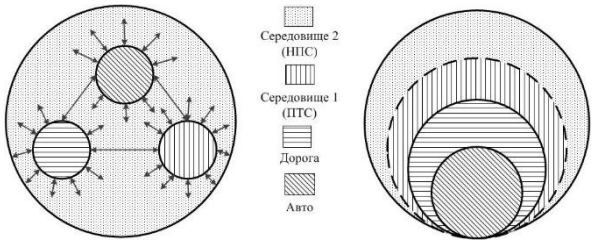


Рис. 1 – Графічне подання існуючого та нового підходів до оцінювання впливу АДС на довкілля

Існуючий підхід:

$$F(S) \rightarrow \min, \quad (1)$$

де $S = \{A, D, LT\}$.

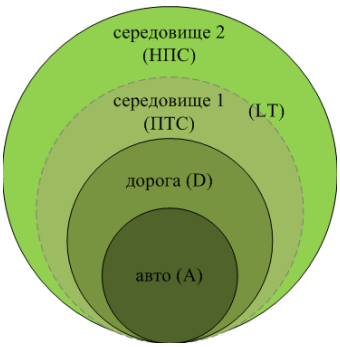


Рис. 2 – Графічне уявлення просторового відображення запропонованого підходу до оцінювання впливу АДС на довкілля

Запропонований підхід:

$$F(S) \rightarrow \min, \qquad (2)$$

де S = {A, D, LT, D(A), LT(D(A))}; F(S) – функція впливу; A – вектор, що характеризує функцію впливу автомобільного транспорту, як джерела; D – вектор, що характеризує функцію впливу дороги, як джерела; LT – вектор, що характеризує природно-техногенне середовище (ПТС) як середовище накопичення та розповсюдження впливу у навколишнє природне середовище (НПС); D(A) – вектор функції впливу експлуатації дороги як сукупності руху транспортних засобів безпосередньо на дорозі; LT(D(A)) – вектор стану ПТС як джерела впливу на НПС, що залежить від експлуатаційного стану автомобільної дороги та сукупності автомобілів безпосередньо на дорозі.

Таким чином А є багатогранною комплексною перемінною величиною, що являє собою вектор, який змінюється безпосередньо у часі та рухається у просторі. Дорога (D) це також перемінна, яка змінюється від пори року, часу експлуатації, метеорологічних умов та ін.

У запропонованому підході LT характеризується додаванням біологічної та природньої складових, які відповідно в свою чергу матимуть свою характеристику.

Перемінна D(A) описує скільки і яких транспортних засобів знаходиться на дорозі, наявність яких на конкретній ділянці характеризує і шумонавантаження, і вібраційне навантаження, і склад хімічних речовин, які потрапляють до середовища, експлуатаційне навантаження на дорогу і т.д.

LT(D(A)) є векторною змінною, що характеризує розповсюдження впливу від системи «автомобіль-дорога», який спочатку буде надходити до ПТС, а далі розповсюджуватись на НПС.

Тобто, ми додатково розглядаємо змінні D(A) та LT(D(A)), що є додатковою експлуатаційною характеристикою, яка описує комплексний емерджентний вплив, тобто розглядаються не окремі статичні об'єкти, а динамічні характеристики, які постійно змінюються в залежності від обставин.

Таким чином, кожна змінна формули (2) має досягти мінімуму. Коли мінімізація параметрів загалом відбулася то це означатиме, що ми досягли максимально-можливого мінімального впливу.

Рис. 3 – Дорога М-29 Харків-Дніпро (досліджувана ділянка: 20 км – 22 км)
Умовні позначення: 1 - 5 – точки прямих вимірів стану атмосферного повітря; 1- 3, 5 – точки відбору проб ґрунту та рослинності; 6 – точка відбору контрольних проб рослинності та ґрунту

Об’єктом для проведення експертно-аналітичного оцінювання та натурних досліджень, з метою перевірки адекватності отриманих оцінок, обрано ділянку дороги М-29 Харків-Дніпро, яка є автошляхом міжнародного значення, являється швидкісним аналогом дороги М-18 та є частиною Європейського маршруту Е-105, що проходить від Норвегії через Росію до України (рис. 3).

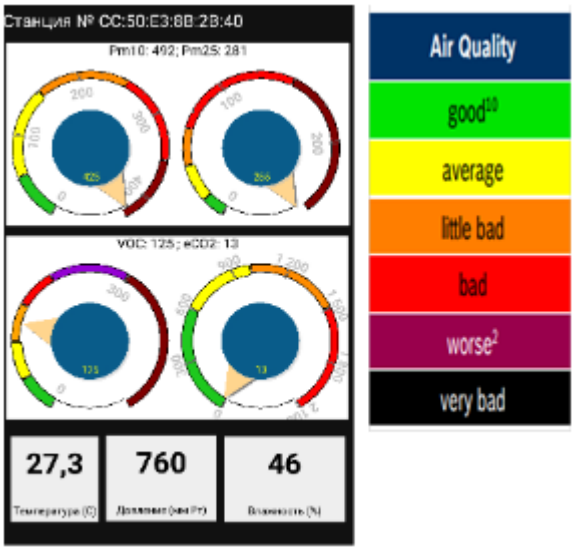


Рис. 4 – Скріншот робочого екрану монітору роботи станції прямих вимірів (ліворуч) та позначення кольорів індикації спектрів кількості наявності домішок у повітрі(праворуч)

Методом прямих натурних досліджень на придорожній території вибраної ділянки автомобільної дороги на місцях відбору проб було проведено індикацію стану забруднення повітряного середовища. Також на даних точках відібрані

зразки ґрунту та рослинності для подальшого їх дослідження в лабораторних умовах. Натурні дослідження проводили з трикратною повторюваністю.

Для вибору оптимальних ділянок відбору проб використовували моноблочний прилад, що являє собою комплексну станцію прямих вимірів з часом відгуку – лише 1с, та часом вимірювання не більше 10 с.

Станція включає лазерний датчик якості повітря PM2.5 пилу Nova SDS011 та датчик параметрів середовища Bosch Sensortec | BME680 HSMI. Використана у станції мікросхема BME680 має вбудований металооксидний датчик (Metal Oxide Semiconductor) летких органічних сполук (ЛОС) та датчики, що дозволяють вимірювати тиск, температуру, вологість і якість повітря.

В SDS011 використано принцип лазерного розсіювання, що дозволяє оцінити концентрацію частинок пилу у повітрі за загальноприйнятою класифікацією - розміром від 0,3 до 2,5 мкм і від 2,5 до 10 мкм. Точність: макс. ± 10 мкг/м3. Діапазон робочої температури: -10 ... +50 °C [14]. На рис. 4 надано скріншот екрану роботи станції та кольорове позначення порогів рівнів концентрації забруднювачів у повітрі. Узагальнивши результати наукових досліджень попередників можна систематизувати широкий спектр комплексних заходів зменшення впливу на навколишнє середовище системи АДС, у сім комплексних блоків щодо дієвості, табл. 1.

Таблиця 1 – Основний зміст комплексних заходів зменшення впливу на довкілля

Захід	Основний зміст
3.1 – еколого-економічні важелі	- фінансове забезпечення заходів із забезпечення екологічної безпеки в системі АДС (СЕО, ОВНС, ОВД); - стимулювання фізичних і юридичних осіб для дотримання норм екологічної безпеки; - систему виховних заходів (екобігборди, внесення екоскладової до програм автошкіл); - введення економічних важелів стимулювання оновлення автомобільного парку; - просування екологічно-чистих видів транспорту; - відповідальність учасників приймання і введення автомобільної дороги в експлуатацію; - формування мотиваційних важелів у інноваційній діяльності підприємств дорожнього господарства; - систему штрафів (у випадку недотримання вимог природоохоронного законодавства у сфері дорожнього господарства та автомобільних доріг); - пільгові умови інвестування (для підприємств дорожньої галузі, що впроваджують програми із захисту НПС).
3.2 – екологічний контроль та моніторинг системи «АДС»	- організацію та проведення моніторингу стану придорожніх територій; - проведення екоконтролю при будівництві, ремонті (реконструкції) автомобільних доріг; - здійснення контролю за використанням у конструкції автомобілів матеріалів та рідин зі шкідливими речовинами; - залучення органів місцевого самоврядування для забезпечення виконання програм Укравтодору щодо захисту НПС на місцях; - контроль за дотриманням вимог екостандартів «ЄВРО»; - моніторинг експлуатації автомобільної дороги;

Захід	Основний зміст
	- створення постійно діючої мережі спостережних пунктів за станом НПС.
3.3 – технічний контроль та моніторинг системи «АДС»	- контроль якості конструкцій дорожнього полотна; - організація та проведення моніторингу стану дорожнього полотна в процесі експлуатації; - експлуатаційний моніторинг систем автомобіля; - контроль якості будівництва, ремонту (реконструкції) автомобільних доріг; - організація та забезпечення безпеки дорожнього руху; - проведення технічного нагляду (технічна інвентаризація, паспортизація) за будівництвом, ремонтом (реконструкцією) автомобільних доріг; - контроль якості утримання автомобільних доріг; - здійснення контролю за організацією будівельних робіт, дотримання технологічного регламенту, контролю якості водовідвідних конструкцій; - своєчасне технічне обслуговування і точне регулювання системи запалювання та живлення двигунів внутрішнього згорання.
3.4 – екологізація дорожнього полотна	- проведення робіт з підтримки експлуатаційного стану проїзної частини, відповідного безпечного і безперебійного дорожнього руху (своєчасне усунення або зниження ризику виникнення ДТП); - використання новітніх технологій та матеріалів у будівництві та експлуатаційному утриманні дорожнього полотна; - насадження лісосмуг в комбінації з чагарниками та газоном;
	- встановлення захисного екранування; - улаштування біопереходів, скотопрогонів, шляхопроводів, об'їзних доріг; - влаштування організованих площадок відпочинку і стоянок автомобілів; - установка дорожніх знаків, що попереджують про імовірність зіткнення з твариною; - встановлення дорожньої огорожі в потенційно небезпечних місцях можливого виникнення ДТП; - встановлення спеціальних дзеркал, що відбивають світло фар.
3.5 – екологізація транспортних засобів	- збільшення кількості екоматеріалів у виробництві авто; - вдосконалення конструкції й технології виробництва ДВЗ; - здійснення законодавчого регулювання в сфері контролю відпрацьованих газів ДВЗ; - додавання присадок та домішкок для зменшення токсичності ВГ; - впровадження новітніх систем нейтралізації шкідливих викидів та сажовловлювачів; - організація раціонального дорожнього руху; - транспортування пилових та сипучих матеріалів в транспортних засобах з брезентовим або іншим накриттям; - установлення на вузлах і деталях автотранспорту, спеціальних індикаторів, які надають інформацію щодо необхідності їх заміни; - своєчасна та якісна діагностика і регулювання всіх систем двигуна.
3.6 –збереження цілісності дорожніх конструкцій	- укріплення укосів, узбіч, бокових канав; - проектування інженерних заходів щодо захисту доріг від впливу небезпечних природніх і техногенних факторів на стадіях будівництва, реконструкції, капітального ремонту та експлуатації; - облаштування на зсувонебезпечних ділянках перехоплюючого дренажу; - здійснення габаритно-вагового контролю;

Захід	Основний зміст
	- удосконалення ДТС за рахунок обґрунтованих темпів автомобілізації, раціонального регулювання дорожнього руху; - влаштування протифільтраційних завіс; - зміцнення дорожнього полотна армуванням георешітками; - проведення планово-попереджувальних (профілактичних) робіт щодо усунення (запобігання) на ранній стадії руйнування споруд; - влаштування штучних водовідвідних споруд з забезпеченням їх безперебійної роботи.
3.7 – технологічне забезпечення нормативної якості поверхневих стічних вод	- створення системи поверхневого водовідводу (лотки, бистрини, кювети тощо) з очищенням стічних вод; - будівництво тротуарних бордюрів; - укріплення укосів, узбіч, бокових канав; - використання екологічно безпечних матеріалів у експлуатаційному утриманні дорожнього полотна; - насадження лісосмуг в комбінації з чагарниками та газоном; - своєчасне усунення дефектів (засмічення, руйнація, знос) водовідвідних споруд; - проведення організаційно-технічних заходів по скороченню кількості винесених домішок; - забезпечення власниками автомобільних доріг та мостових споруд санітарного стану підвідомчих територій; - забезпечення якості дорожнього полотна в період експлуатації.

Проаналізувавши питання щодо методів та заходів, що використовуються для зменшення впливу на складові довкілля нами була розроблена ієрархічну структуру комплексної екологічної оцінки впливу системи «АДС» на об'єкти довкілля (рис. 4) з урахування заходів протидії та попередніх напрацювань авторів [13, 14].

За розробленою структурою була проведена оцінка дієвості комплексних заходів зменшення впливу експлуатації вибраної автомобільної дороги на складові довкілля з застосуванням методу аналізу ієрархій з використанням підходу експертно-аналітичної оцінки для визначення вагових коефіцієнтів вкладу кожного елементу структури, наданої на рис.1, що включає в себе результати попередньої оцінки щодо комплексного впливу експлуатації автомобільної дороги на об'єкти НПС [13].

За результатами еколого-аналітичної оцінки було виявлено, що дієвими комплексними заходами для зменшення впливу на стан повітря у системі «АДС» є екологізація транспортних засобів зі значенням 35,1 %, та екологізація дорожнього полотна – 24,7 % (рис. 5).

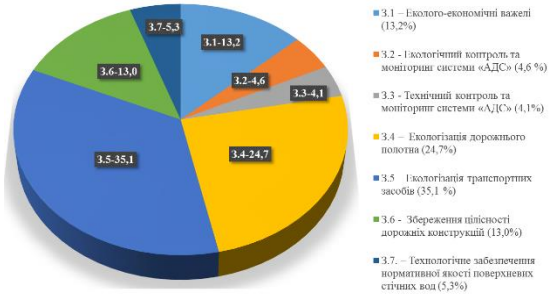


Рис. 5 - Результати еколого-аналітичної оцінки дієвості комплексних заходів зменшення впливу системи «АДС» на стан повітря

Для зменшення впливу на стан водних масивів у системі «АДС» найбільш пріоритетними комплексними заходами є: технологічне забезпечення нормативної якості поверхневих стічних вод – 37,8 %, екологізація транспортних засобів – 23,1 % (рис. 6).

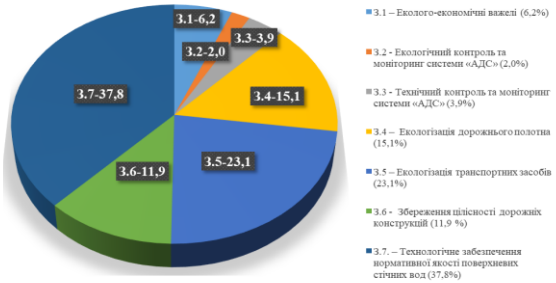


Рис. 6 – Результати еколого-аналітичної оцінки дієвості комплексних заходів зменшення впливу системи «АДС» на стан водних масивів

Встановлено, що найбільш дієвими комплексними заходи зменшення впливу на стан ґрунту у системі «АДС» є: екологізація дорожнього полотна – 35,0 % та збереження цілісності дорожніх конструкцій – 23,8 % (рис. 7).

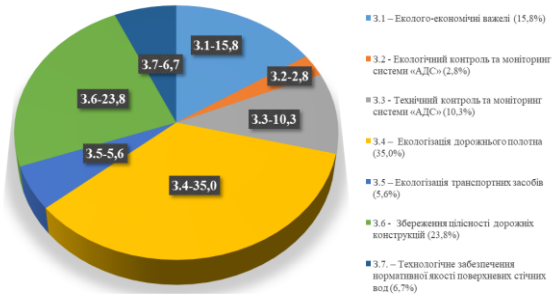


Рис. 7 – Результати еколого-аналітичної оцінки дієвості комплексних заходів зменшення впливу системи «АДС» на стан ґрунту

Для зменшення впливу на стан біоти в системі «АДС» більш дієвими заходами є екологізація дорожнього полотна – 33,5 %, еколого-економічні важелі – 22,0 % (рис. 8).

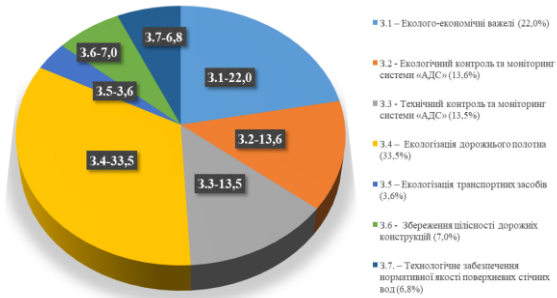


Рис. 8 – Результати еколого-аналітичної оцінки дієвості комплексних заходів зменшення впливу системи «АДС» на стан біоти

За результатами еколого-аналітичної оцінки дієвості комплексних заходів зменшення впливу системи «АДС» на стан здоров'я людини більш дієвими є екологізація дорожнього полотна – 30,4 %, еколого-економічні важелі – 20,9 % (рис. 9).

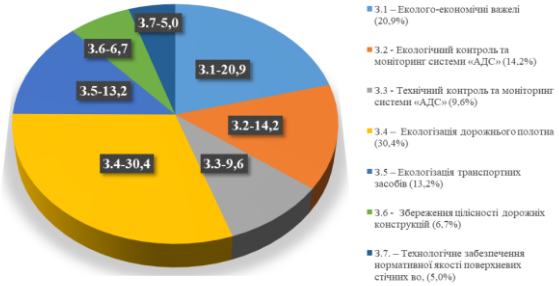


Рис. 9 – Результати еколого-аналітичної оцінки дієвості комплексних заходів зменшення впливу системи «АДС» на стан здоров'я людини

Обговорення результатів. Вплив системи «АДС» на здоров'я людини може бути оцінено за показниками вмісту важких металів в рослинах та ґрунті придорожнього простору, які можуть споживатися у вигляді лікарських рослин та у вигляді корму домашніми травоїдними тваринами населення, що проживає поряд з дорогою. Визначення вмісту проводилося методом атомно-абсорбційної спектроскопії в лабораторії «Еколого-аналітичних досліджень» УКРНДІЕП (http://www.niiep.kharkov.ua/node/179) на атестованому оптико-емісійному спектрометрі високої роздільної здатності з індуктивно-зв'язаною плазмою PlasmaQuant PQ 9000 Elite. Автор, поряд зі співробітниками лабораторії, приймав безпосередню участь у відборі проб рослинності та ґрунту, пробопідготовці та проведенні лабораторних досліджень. Результати проведених досліджень доповідались на міжнародних конференціях та опубліковані в [17- 19].

Для здійснення комплексної оцінки нами була розроблена структура оцінювання комплексного впливу експлуатації автомобільної дороги на об'єкти НПС, яка складається з елементів, пов'язаних один з одним системними взаємозв'язками, що характеризують та описують критерії формування оцінок, комплексність факторів, що враховує їх фізичну та хімічну природу, умови розповсюдження і накопичення в природному середовищі (рис. 10).

Особливої уваги заслуговує те, що в ній враховано біотичні та абіотичні умови середовища, що мають досить суттєве значення у розповсюдженні впливу системи «АДС» [17, 20].

Лінія зв'язку, що поєднує верхній елемент рівня та нижній елемент рівня пояснює природу, характеристику та умови, що описують взаємодію між ними.

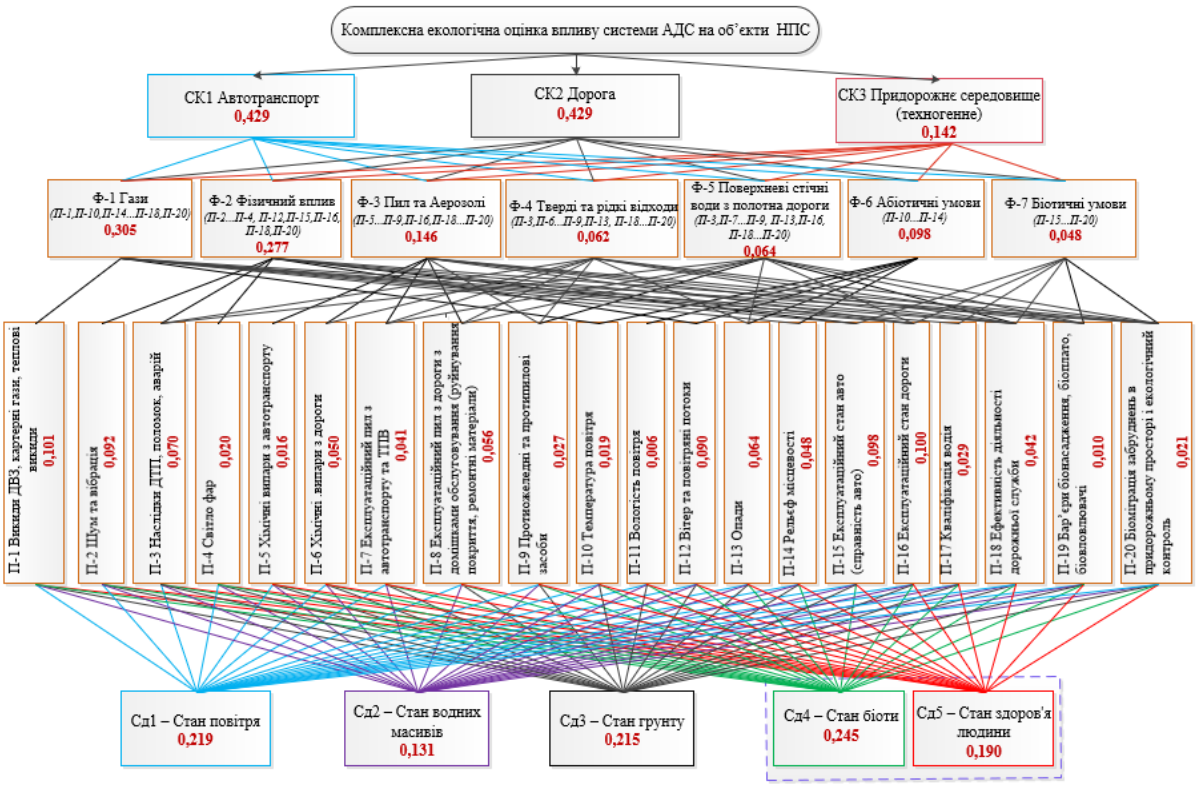


Рис. 10 – Структура оцінки комплексного впливу автомобільної дороги на об'єкти НПС (розроблено автором Г.В. Адамовою)

Питання формування експертно-аналітичної групи для проведення досліджень потребує особливої уваги, що зазначено в [21, 22]. Підбір експертної групи відбувається у декілька етапів. Спершу встановлюють галузі знань, що прямо або опосередковано пов'язані з проблемою, що досліджується. Далі намічають список "потенційних" експертів, які за своїми професійними якостями компетентні в цих галузях знань. Зазвичай для цього використовуються показники, що відображають професійний рівень фахівця (посада, вчений ступінь і звання, кількість опублікованих наукових праць і ін.). Після цього вирішується питання про чисельний склад експертної групи, який залежить від обмежень фінансового, часового й організаційного характерів. Остаточно група формується шляхом виділення "потенційних" експертів, які з погляду конкретного вирішуваного завдання є найбільш компетентними. При цьому, задля виключення впливу відомчих інтересів на мету оцінювання, у складі групи по можливості забезпечують рівне представництво фахівців різних напрямів, які існують в досліджуваній галузі. Для отримання узгоджених результатів опитування експертів, як правило, проводять або декілька турів оцінювання з проміжним висвітленням результатів та їх обговоренням, або в 2 етапи, де на

першому експерти висвітлюють кожен окремо свої думки, а узагальнююче оцінювання проводять у вигляді колективної комплексної оцінки, де в режимі диспуту уточнюються значення попарних порівнянь та їх обґрунтованість кожним з експертів і використовують або узагальнену середню оцінку, або в кожному конкретному оцінюванні надають перевагу профільному фахівцю [21, 22].

Таким чином, нами, для проведення еколого-аналітичної оцінки впливу системи «автомобіль-дорога-середовище» на придорожній простір (рисунки 4 та 10), було встановлено склад експертно-аналітичної групи, до якої ввійшли експерти з фахом: інженер-еколог в галузі експлуатації автомобільних доріг (для оцінювання факторів впливу, що розкриваються за допомогою параметрів П-1…П-3, П-5…П-9, П-14…П-20), біолог (аналогічно для параметрів – П-1…П-9, П-12, П-19, П-20), фахівець в галузі ОВД (аналогічно для параметрів – П-1…П-9, П-12, П-14…П-20), хімік-аналітик (аналогічно для параметрів – П-1, П-5…П-16, П-19, П-20), фахівець в області геоінформаційних технологій (аналогічно для параметрів – П-10…П-16, П-19,П-20).

Комплексна оцінка впливу системи «АДС» на об'єкти НПС була проведена з застосуванням методу аналізу ієрархій та включала експертно-аналітичне визначення вагових коефіцієнтів вкладу кожного елементу структури, наданої на рис.4, та синтезу всіх отриманих вагових коефіцієнтів, що формує загальний результат оцінки впливів. Для здійснення оцінювання було використано комп'ютерну програму «МАІ», яка реалізує відомий метод аналізу ієрархій Томаса Сааті з доопрацюваннями УКРНДІЕП в частині підходу до експертно-аналітичної оцінки та шкали оцінювання, що детально описані в роботах Аніщенко Л.Я., Пісні Л.А., Гончаренко І.О. та частково висвітлені стосовно АДС в [20]. Застосована в роботі комп'ютерна програма МАІ, розроблена в УКРНІЕП, перевірена зазначеними дослідниками та має своєю особливістю те, що в ній узгодження думок експертів перевіряється автоматично, в процесі заповнення попарних порівнянь з заданою точністю перед початком роботи, що відповідає вимогам до методу аналізу ієрархій, сформованим Томасом Сааті. Таким чином, вагові коефіцієнти кожного з елементів структури за рівнями розподілу впливу в системі АДС на складові навколишнього природного середовища надано на рис. 4 та рис. 10.

В результаті дослідження вперше вдалося побудувати пріоритетний ряд параметрів, що характеризують фактори впливу, що в подальшому дозволить ефективно оцінювати та впроваджувати заходи зменшення впливу. Пріоритетний ряд параметрів виглядає наступним чином: П-1 > П-16 > П-15 > П-2 > П-12 > П-3 > П-13 > П-8 > П-6 > П-14 > П-18 > П-7 > П-17 > П-9 > П-20 > П-4 > П-10 > П-5 > П-19 > П-11.

За результатами еколого-аналітичної оцінки визначено пріоритетність показників складових довкілля, що зазнають впливу від «АДС», а саме: вплив на зміни стану біоти складає 24,5 % загального впливу, на зміни стану повітря – 21,9 %, на зміни стану ґрунту – 21,5 %, на зміни стану здоров'я людини – 19,0 %, та зміни стану водних масивів – 13,1 %

Розроблений комплексний ієрархічний підхд до оцінки АДС із застосуванням МАІ потребує подальшого уточнення кількісних характеристик впливу на складові довкілля шляхом лабораторних досліджень біотичних компонентів та ґрунту придорожнього простору за стандартизованими методиками.

Таблиця 3 – Технічні характеристики вибраної ділянки дослідження автомобільної дороги М-29

Показник	Характеристика
Тип дороги	магістральна а/д
Тип покриття	асфальт
Ширина земляного полотна	26,5 м.
Ширина проїзної частини	16 м. (4 смуги руху)
Ширина центральної розділової смуги	8 м.
Ширина смуги для зупинки	2,5 м.
Інтенсивність руху	2 680 авт./добу
Склад руху: легкі вантажні автомобілі (до 2,5 т) середні вантажні автомобілі (до 5 т) важкі вантажні автомобілі (більше 8 т) мікроавтобуси автобуси легкові автомобілі	 21,6 %, 13,4 %, 6,0%, 17,2 %, 1,5 %, 40,3 %;
Середня швидкість руху	110 км/год

*Примітка: таблиця складена автором Г.В. Адамова.

Водночас з відбором зразків рослинності на тих самих ділянках було проведено відбір проб ґрунту методом «конверту» з шарів 0-5 см та 5-10 см.

Аналіз проведених лабораторних досліджень виявив накопичення в рослинності та ґрунті важких металів вище ГДК на відстані 10 м, 50 м та 100 м від полотна дороги:

- осика звичайна - Mn, Co, Zn, Cr;
- верба біла - Cu, Mn, Co, Cd, Cr;
- деревій щетинистий - Cu, Mn,Cr;
- парило звичайне, сосна звичайна,
- береза бородавчаста та вільха клейка - Mn, Cr.

Встановлено перевищення ГДК також і в зразках ґрунту за Cu, Mn, Cd, Cr, Ni та Pb [17-20, 23].

Діапазон перевищень ГДК для різних хімічних речовин у різних рослинах та ґрунті різний, зокрема:

Cu (1,3 ГДК – 1,5 ГДК); Mn (1,3 ГДК – 3,6 ГДК);
Co (1,1 ГДК – 1,9 ГДК); Cd (1,3 ГДК – 2,5 ГДК);
Cr (2,3 ГДК – 4,3 ГДК); Zn (не більше 1,3 ГДК);

Pb (1,3 ГДК – 2,7 ГДК); Ni (1,1 ГДК-2,4 ГДК).

Після опрацювання лабораторних досліджень, за інтенсивністю накопичення важких металів у досліджуваних зразках рослинності та ґрунту придорожнього простору було встановлено рангові ряди (табл. 4).

Таблиця 4 – Ранговий ряд накопичення важких металів у рослинності та ґрунті придорожнього простору*

Зразок рослинності/ ґрунту	Ранговий ряд
Береза бородавчаста	Mn>Fe>Zn>Cu>Cr>Ni>Cd>Pb>Co
Сосна звичайна	Mn>Fe>Zn>Cu>Cr>Ni>Cd>Pb>Co
Парило звичайне	Fe > Mn > Zn > Cu > Cr > Ni > Pb > Cd > Co
Вільха клейка	Fe > Mn > Zn > Cu > Cr > Ni > Pb > Cd > Co
Деревій щетинистий	Fe > Mn > Zn > Cu > Cr > Ni > Pb > Cd > Co
Верба біла	Fe>Zn>Mn>Cu>Ni>Cr>Co>Cd>Pb
Осика звичайна	Zn > Mn > Fe > Cu > Ni > Cr > Co > Cd > Pb
Ґрунт	Fe > Mn > Cr > Zn > Cu > Ni > Co > Pb > Cd

*Примітка: Таблицю складено автором Г.В. Адамова на підставі власних досліджень, що корелює з аналогічними дослідженнями [22, 24-26]. Рангові ряди встановлювалися за І. М. Волошиним (1998).

Зразки рослинності відбирались на протязі вегетаційного періоду рослин, тому рангові ряди вказують на кількість накопичення важких металів за весь період їх життя. З таблиці видно, що у зразках придорожньої рослинності переважає накопичення Mn, Fe та Zn, а найменшу інтенсивність накопичення має Co, а у верби білої та осики звичайної менш інтенсивно накопичується Pb. У ґрунті придорожнього простору серед важких металів найбільшу інтенсивність накопичення має Fe, а найменшу Cd.

Аналіз отриманих результатів корелює зі схожими результатами попередніх досліджень інших дослідників, що займались даною тематикою, зокрема [22, 24-26] в частині вибору рослин-акумуляторів та послідовності і кількості накопичення важких металів.

Висновки. Швидкі темпи розвитку транспортно-дорожнього комплексу призводять до збільшення навантаження на природні системи, внаслідок чого погіршується екологічний стан в країні.

Звичайно, неможливо повністю усунути шкідливий вплив, що завдається довкіллю експлуатацією автомобільної дороги, однак необхідно намагатися звести його до мінімуму.

Розроблена ієрархічна структура включає в себе комплекси заходів зі зниження впливу від експлуатації автомобільних доріг на довкілля для кожної з її складових, що дозволить зменшити рівень впливу від системи «АДС» до мінімуму. Також завдяки структурі будуть розроблятися заходи необхідні саме для конкретної дороги або її ділянки, що забезпечить більш ефективне

використання бюджетних коштів, що будуть виділятися у післявоєнний час на відбудову дорожньої інфраструктури нашої країни.

На прикладі вибраної ділянки автомобільної дороги М-29, підтверджено накопичення важких металів в придорожньому просторі, зокрема виявлено забруднення рослинності придорожнього простору з перевищенням ГДК: верба біла - Cu, Mn, Co, Cd, Cr; осика звичайна - Mn, Co, Zn, Cr; деревій щетинистий - Cu, Mn,Cr; парило звичайне - Mn,Cr; сосна звичайна - Mn,Cr; береза бородавчаста - Mn,Cr; вільха клейка - Mn,Cr. Також встановлено перевищення норм ГДК важких металів в зразках ґрунту Cu, Mn, Cd, Cr, Ni та Pb. Значення отриманих результатів корелює зі значеннями схожих попередніх досліджень інших авторів на інших автомобільних дорогах. За узагальненими результатами лабораторних досліджень побудовано ранговий ряд накопичення важких металів у досліджуваних зразках рослинності та ґрунтів придорожнього простору досліджуваної ділянки дороги. Підтверджено, що дослідження важких металів в придорожньому просторі може слугувати як додатковий моніторинг екологічної безпеки експлуатації автомобільної дороги.

Тому важливо враховувати як екологічну безпеку, так і кібербезпеку у проектуванні та обслуговуванні такої критично важливої інфраструктури, як автомобільні дороги.

Література

1. Кашканов В.А. Шляхи підвищення екологічної безпеки автомобільного транспорту/ В.А. Кашканов,О.В. Устюшенко – [Електронний ресурс]. – URL: http://ir.lib.vntu.edu.ua/bitstream/handle/123456789/11114/780.pdf?sequence=3
2. Стороженко М.С. Снижение воздействия на окружающую среду совершенствованием дорожно-транспортной системы/ М.С. Стороженко, Н.С. Аринушкина, Т.М. Грищенко// Вестник ХНАДУ. – Харків: ХНАДУ. – 2011. – № 52.– С. 35– 38.
3. Вамболь С.О. Строков В.В., Вамболь В.В., Кондратенко О.М. Сучасні способи підвищення екологічної безпеки експлуатації енергетичних установок. Монографія. Харків. НУЦЗУ. –2015. – 212 с.
4. Оцінка впливу на навколишнє середовище Капітальний ремонт автомобільної дороги під'їзд до ДП МА «Бориспіль» км 0+000 – км2+800 (інв. №47590) з системою освітлення (інв №47273) (коригування). *РОБОЧИЙ ПРОЕКТ*. ТОМ 5. 37-14.2/5-3-ОВНС. ТОВ «ІНТЕРПРОЕКТ». 2017. 51 с.
5. Сєрікова О.М. Прогнозування і управління рівнем ґрунтових вод для підвищення екологічної безпеки забудованих територій України: дис. на здобуття наук. ступ. к.т.н.: спец. 21.06.01 «Екологічна безпека» / Сєрікова Олена Миколаївна. – Харківський національний університет міського господарства ім. О.М. Бекетова. Харків. – 2019. –166 с.
6. Мацак А.О. Підвищення рівня екологічної безпеки водних об'єктів шляхом зменшення впливу дощових стічних вод з урбанізованих територій: дис. на здобуття наук. ступ. к.т.н. спец. 21.06.01 «Екологічна безпека»/ Мацак Антон Олександрович.

– Наукова Дослідна Установа «Український Науково Дослідний Інститут Екологічних Проблем». Харків. –2021. –151 с.
7. Черноносова Т.О. Міське зелене будівництво. : конспект лекцій для студентів денної, заочної, прискореної форм навчання, слухачів другої вищої освіти спеціальності 192 – Будівництво та цивільна інженерія фахового спрямування «Міське будівництво та господарство» / Т. О. Черноносова ; Харків. нац. унт міськ. госп-ва ім. О. М. Бекетова. –2018. – 68 с.
8. Van Renterghem, T. Using natural means to reduce surface transport noise during propagation outdoors/ Van Renterghem, T. ; Forssén, J. ; Attenborough, K. et al./ – [Електронний ресурс]. – https://research.chalmers.se/publication/213823 http://dx.doi.org/10.1016/j.apacoust.2015.01.004
9. Dilhara Ranasinghe. Effectiveness of vegetation and sound wall-vegetation combination barriers on pollution dispersion from freeways under early morning conditions/ Dilhara Ranasinghe, Eon S. Lee, Yifang Zhu, Isis Frausto-Vicencio, Wonsik Choi, Wu Sun, Steve Mara, Ulrike Seibt, Suzanne E. Paulson// Science of The Total Environment – V. 658. – 2019. – [Електронний ресурс]. – URL: https://www.sciencedirect.com/science/article/abs/pii/S0048969718350046?via%3Dihub
10. Irfan Ullah Khan. A Green Approach Used for Heavy Metals 'Phytoremediation' Via Invasive Plant Species to Mitigate Environmental Pollution: A Review/ Irfan Ullah Khan, Shan-Shan Qi, Farrukh Gul, Sehrish Manan, Justice Kipkorir Rono, Misbah Naz, Xin-Ning Shi, Haiyan Zhang, Zhi-Cong Dai, Dao-Lin Du. – [Електронний ресурс]. – URL: https://www.mdpi.com/2223-7747/12/4/725 https://doi.org/10.3390/plants12040725
11. Вознюк С.В. Обґрунтування параметрів конструкції лабіринту лакунарних порожнин в структурі газо-пилозахисних лісосмуг автомобільних доріг: дис. на здобуття наук. ступ. к.т.н.: спец. 21.06.01 «Екологічна безпека»/ Вознюк Світлана Володимирівна – Кам'янець-Подільський: ПДАТУ – 2017. – 180 с.
12. Yong Chen. Volatile Organic Compound Sampling through Rotor Unmanned Aerial Vehicle Technique for Environmental Monitoring/ Yong Chen, Xiaoxu Zhang, Xiaofeng Wu , Jia Li, Yang Qiu, Hao Wang, Zhang Cheng, Chengbin Zheng, Fumo Yang – [Електронний ресурс]. – URL: https://www.mdpi.com/2073-4433/13/9/1442. https://doi.org/10.3390/atmos13091442
13. Abdul Samad. Concept of Using an Unmanned Aerial Vehicle (UAV) for 3D Investigation of Air Quality in the Atmosphere—Example of Measurements Near a Roadside/Abdul Samad, Diego Alvarez Florez, Ioannis Chourdakis,Ulrich Vogt– [Електронний ресурс]. – URL: https://www.mdpi.com/2073-4433/13/5/663. https://doi.org/10.3390/atmos13050663
14. Аболмасова Г. В., Пісня Л.А., Черба О.В. (вересень. 9-13. 2019).Елементи інтегрального підходу в екологічній оцінці стану забрудненості придорожнього простору. *Екологічна безпека: проблеми і шляхи вирішення*. Зб. наук, статей XV міжнар. наук.-практ. конф., м. Харків. УКРНДІЕП. ПП «Стиль-Іздат». 2019. С.5-8. URL: http://www.niiep.kharkov.ua/sites/default/files/Konfer2019.pdf
15. Адамова Г.В. Комплексна еколого-аналітична оцінка системи «Автомобіль-Дорога-Середовище» на прикладі ділянки дороги М-29. Вісник Харківського національного університету імені В. Н. Каразіна серія «Екологія». – 2021.– №25. – С.55-69.

16. Адамова Г. В. Застосування комплексної еколого-аналітичної оцінки впливу системи «автомобіль-дорога-середовище» для виконання завдань відбудови у післявоєнний час/ Адамова Г. В., Пісня Л. А.// Екологічна безпека: проблеми і шляхи вирішення: зб. наук. статей XVIII Міжнародної науково-практичної конференції (м. Харків, 15-16 вересня 2022 р.) / УКРНДІЕП., 2022. — С. 7-12.
17. Адамова Г.В. (червень 4, 2021). Аналіз впливу системи «автомобіль-дорога-середовище» на об'єкти навколишнього природного середовища. *The current state of development of world science: characteristics and features.* Collection of scientific papers «SCIENTIA» with Proceedings of the I International Scientific and Theoretical Conference (Vol. 1),. Lisbon, Portuguese Republic: European Scientific Platform. DOI:10.36074/scienta-04.06.2021. URL:https://ojs.ukrlogos.in.ua/index.php/scientia/issue/download/04.06.2021/545
18. Аболмасова Г.В., Пісня Л.А. (14-18 вересня 2020 р.) Важкі метали у ґрунтах та рослинності придорожнього простору. *Екологічна безпека: проблеми і шляхи вирішення.* Зб. наук, статей XVI Міжнародної науково-практичної конференції. Харків. УКРНДІЕП. ПП «Стиль-Іздат», 2020. 292 с. URL:http://www.niiep.kharkov.ua/sites/default/files/konfer2020.pdf
19. Аболмасова Г.В. (15-17 жовтня 2020 р.). Система «автомобіль-дорога» як джерело надходження важких металів у придорожній простір. *Збірник тез доповідей IV Спеціалізованого міжнародного Запорізького екологічного форуму «ЕКО ФОРУМ - 2020»*. Запорізька міська рада, Запорізька торгово-промислова палата, 2020. URL: https://new.ziif.in.ua/wp-content/uploads/2020/12/Zbirka-tez-Eko-Forum-2020.pdf
20. Аболмасова Г.В., Пісня Л.А., Черепньов І.А., Калінін І.В. Комплексна екологічна оцінка впливу системи «автомобіль-дорога-середовище» на об'єкти навколишнього природного середовища. *Науковий Журнал "Інженерія природокористування"*. Х. 2019. №4(14). С.75-85. URL: http://enm.khntusg.com.ua/index.php/enm/issue/view/24
21 Пепина Л.А., Созонтова А.Н., Загрязнение атмосферного воздуха автомобильнодорожным комплексом. Alfabuild. 2017. №1 (1). С. 99-110. URL: https://alfabuild.spbstu.ru/userfiles/files/AlfaBuild/AlfaBuild_2017_1/8_1.pdf
22.Rolli N.M et al. 2019, Phytoassay of Heavy Metals Pollution in Roadside Environment: Bioindicators. Int J Recent Sci Res. 10(12), pp. 36499-36503. DOI: http://dx.doi.org/10.24327/ijrsr.2020.1012.4934. URL: http://recentscientific.com/phytoassay-heavy-metals-pollution-roadside-environment-bioindicators
23. Адамова Г.В., Пісня Л.А. Визначення впливу транспортно-дорожнього комплексу на довкілля на прикладі ділянки автомобільної дороги М-29 Харків-Дніпро. *Проблеми охорони навколишнього природного середовища та екологічної безпеки*. Зб. наук. пр. УКРНДІЕП; ХНУ імені В. Н. Каразіна. Х.: ПП «Стиль-Іздат». 2020. Вип.42. 214 с. URL: http://www.niiep.kharkov.ua/sites/default/files/Sbornik2020.pdf

24. Pankaj Kumar and Kuldeep. 2018. Potential Toxic Heavy Metal Contamination of Roadside Soil. Int.J.Curr.Microbiol.App.Sci. 7(07): 465-471. doi: https://doi.org/10.20546/ijcmas.2018.707.056
25. Леонидова Т. В., Сидоренкова Н. К., Блохина Н. А., Харитонов И. Д. Содержание тяжелых металлов в придорожной зоне автомобильных трасс. *Международный журнал прикладных и фундаментальных исследований*. 2019. № 1. С. 146–149. URL: https://www.applied-research.ru/ru/article/view?id=12657
25. Leony`dova T. V., Sy`dorenkova N. K., Bloxy`na N. A., Xary`tonov Y`. D. Soderzhany`e tyazhelыx metallov v pry`dorozhnoj zone avtomoby`l`nыx trass. Mezhdunarodnыj zhurnal pry`kladnыx y` fundamental`nыx y`ssledovany`j. 2019. # 1. S. 146–149. URL: https://www.applied-research.ru/ru/article/view?id=12657
26. Hyun-Min Hwang,Matthew J. Fiala,Terry L. Wade &Dongjoo Park. Review of pollutants in urban road dust: Part II. Organic contaminants from vehicles and road management. *International Journal of Urban Sciences*. Volume 23, 2019 - Issue 4. Pages 445-463. https://doi.org/10.1080/12265934.2018.1538811

УДК 519.876.5:628.472

73. ПОВОДЖЕННЯ З БУДІВЕЛЬНИМИ ВІДХОДАМИ ПІД ЧАС РЕКОНСТРУКЦІЇ ТЕРИТОРІЙ З МЕТОЮ ЗАХИСТУ ДОВКІЛЛЯ

Міщенко І.В.[1*], Вамболь С.О.[2], Вамболь В.В.[3,4]
[1]*Харківський національний автомобільно-дорожній університет, Харків, Україна*
[2]*Национальный технический университет "ХПІ", Харків, Україна*
[3] *Університет природничих наук у Любліні, Люблін, Польща*
[4]*Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна*
**E-mail: ivmishch@gmail.com*

CONSTRUCTION WASTE MANAGEMENT DURING THE TERRITORIES RECONSTRUCTION IN ORDER TO ENVIRONMENT PROTECTION

The solution of the problem of restoration of territories for the secondary processing of construction waste is considered, taking into account the requirements for ensuring the ecological safety of the environment. The possibility of reusing various construction wastes, both in structure, materials, and in size, which are formed during the industrial dismantling of buildings and structures, is analyzed. Particular attention is paid to overcoming the negative consequences of dust formation during dismantling. Using the example of sorting-grinding technology, methods for organizing the production and use of secondary aggregate from concrete scrap are proposed, possible further directions for the use of materials obtained after processing are provided, which increases the efficiency of construction waste disposal and partially solves the problem of pollution of territories by landfills of building materials.

Проблема відновлення трерріторій що построждали в наслідок небезпечних явищ природного, техногенного та військового походження завжди є актуакльною. У більшості випадків це є складний технологічний процес, який потребує використання значних ресурсів. Зазвичай, у цьому процесі захист довкілля не є приоритетним і головним завданньям, оскільки є необхідність як найшвидше розчистити територію для подальшої забудови. Слід акцентувати, що залишки будівельних матеріалів, як правило (в кращому випадку), потряпляють на сміттєзвлища, що призводить до нераціонального використання земель. Проте демонтаж будівель і споруд пов'язаний з утворенням великої кількості будівельних відходів, доступних для повторного використання у житловому, промисловому та дорожньому будівництві.

Житлове та промислове будівництво є одним з найбільших споживачів мінеральних ресурсів – піску, глини, щебеню тощо – видобуток яких призводить до суттєвого негативного впливу на довкілля. За заявою ООН нині більш ніж удвічі збільшено загальносвітовий видобуток природних ресурсів проти 1990 роком і до 2060 року видобуток ресурсів знову може подвоїтися, якщо ставлення до споживання зміниться [1]. Чорні метали, азбест, вапняк, глина, пісок - це матеріали, необхідні для будівництва, відносяться до ресурсів, обсяги видобутку яких зростають найшвидше [2, 3]. Статистика показує, що в період з 1988 по 2018 роки обсяг видобутку заліза та феросплавів зріс з 545 млн. тонн до 1,6 млрд. тонн, оскільки ці сплави є головним компонентом конструкційних матеріалів; промислових мінералів (гіпс, сіль, сірка, каолін, фосфатна сировина, будівельний пісок, польовий шпат, магнезит, тальк та ін.) – з 505 млн. тонн до 811 млн. тонн, що вкрай необхідно металургії та будівництві [4]. У зв’язку з цим важливими стають питання збереження ресурсів, що використовуються як при виконанні будівельних робіт, так і у подальшій експлуатації та утилізації конструкцій будівлі.

Стратегії скорочення будівельних відходів покращуються, коли правова база охоплює екологічні правила та зобов'язання з переробки. У багатьох розвинених країнах, у тому числі у Фінляндії, Німеччині, Австралії та Данії, діють правові норми, що заохочують стратегії управління будівельними відходами, такі як скорочення, повторне використання та переробка [5].

Сучасне будівництво характеризується великим об’ємом та номенклатурою будівельних сумішей на основі цементу – штукатурок, шпаклівок, стяжок та покрить полу, розчинів для укладання цегли та блоків, а також для спорудження монолітних залізобетонних конструкцій. Питання економії цементу викликали необхідність удосконалення технологічних процесів виробництва та підготовки будівельних сумішей, і перш за все, за рахунок введення в них спеціальних добавок для покращення властивостей – пластичності, гідрофобності тощо. Використання таких домішок дозволило підвищити для сумішей час готовності до укладки, зменшити витрату суміші, втрати внаслідок утворення осадів, непридатних до укладання, а також скоротити час кінцевого висихання суміші та підвищити її експлуатаційні якості.

Промисловий демонтаж є найбільш економічним та безпечним, особливо у випадках комбінації різних конструктивних матеріалів. Технологічність процесу демонтажу, який виконується механізованим способом, дозволяє значно скоротити термін виконання робіт та підвищити їх безпеку, оскільки, наприклад, при методі обвалення будівлі ніколи немає точної впевненості у тому, куди та в який час відбудеться руйнування.

Обов'язковою умовою забезпечення екологічної безпеки при демонтажі є організація пиловловлювання. Для зменшення кількості пилу від конструкцій, які руйнуються, їх перед початком процесу зволожують, а при сильному виділенні пилу організують постійну водно-крапельну завісу. В умовах близького розташування інших будівель та споруд, дільницю, яка демонтується, огороджують за допомогою пиловловлюючої сітки, тканини або поліетиленової плівки. За необхідності забезпечення підвищеної міцності пиловловлюючої огорожі її виготовляють у вигляді щитів з листового металу.

Після демонтажу споруди утворюється будівельний лом, який складається з важкого та легкого залізобетону, цегли, утеплювачів, полімерних матеріалів, бітуму, асфальту тощо. Біля 80 % відходів є залізобетон, який після спеціальної переробки (здрібнення, сортування, фракціонування) може бути використаний знову [6, 7]. Застосування вторинного щебеню дозволяє знизити витрати на зведення нових об'єктів за рахунок скорочення зустрічних потоків нерудних матеріалів та одночасно зменшити навантаження на міські полігони, виключити утворення несанкціонованих звалищ, а також зберегти земельні ресурси, які відводяться під розміщення нових кар'єрів.

Організація виробництва та використання вторинного заповнювача з бетонного лому здійснюється наступними способами:

- отримання заповнювача з бетонного лому та виробництво на його основі організується безпосередньо на місці демонтажних робіт з використанням мобільних дробильних комплексів;
- обладнання для отримання заповнювача з бетонного лому встановлюють на місці демонтажу, а отриманий заповнювач відправляють на бетонний завод або будівельний об'єкт (одна транспортна операція);
- бетонний лом з місця демонтажу транспортується на установку з виробництва щебеню, а отриманий заповнювач направляється на бетонний завод або будівельний об'єкт (два транспортні операції).

Отримані після переробки матеріали можна використовувати:

- при заводському виробництві бетонних та залізобетонних виробів класу міцності В25;
- при влаштуванні основ та приготуванні бетону для покриттів пішохідних доріжок, внутрішніх майданчиків гаражів, автостоянок, прогулянкових алей та сільських доріг, для укосів вздовж рік і каналів;
- при облаштуванні фундаментів під складські та виробничі приміщення, а також невеликі механізми;
- при влаштуванні шару підстилання під'їзних та малонавантажених доріг.

Визначною перевагою запропонованого рішення є також можливість використання для фінансування створення вказаного технологічного процесу коштів з фондів фінансування цільових екологічних програм міського та обласного бюджетів.

Схему пропонованої технології сортування-подрібнення поводження з будівельними відходами можна поділити на декілька етапів:

На першому єтапі сировина (будівельні відходи, уламки, тощо) завантажуються до пластинчатого живильника, який забезпечує рівномірну подачу до циклу переробки;

Далі маємо етап першого рівеня грохочення, що відділяє щебінь товарного розміру (0…50 мм), який не потрібно додатково переробляти;

На третьому етапі відбувається сортування, де уламки розміру, більшого за 50 мм, надходять до пристрою первинного подрібнення. Для дроблення можуть бути використані різні типи дробарок, як ріжуча валкова дробарка для грубого дроблення композитних матеріалів та проміжного вибіркового дроблення; валкова дробарка для тонкого дроблення та кругло-валкова дробарка для кругового вальцевого подрібнення крупністю частинок діапазоні від 1 до 80 мкм [7];

Станній етап передбачає, що після подрібнення відбувається первинне сортування відходів, під час якого відділяються залізовмісні відходи (уламки арматури, тощо), а також неметалеві матеріали (деревина та пластмаса);

Перевагою запропонованої схеми є забезпечення відокремлення різних матеріалів один від одного, що підвищує ефективність утилізації будівельних відходів.

Як висновки слід вказати наступне.

По перше, промисловий демонтаж слід проводити з урахуванням умов забезпечення екологічної безпеки, виключаючі забруднення будівельним пилом, шляхом є організації процесу пиловловлювання.

По друге. Вже на етапі демонтажу планувати сортування будивельних відходів з метою подальшої утілізації.

На останнє, для більш ефективного поводження з будівельними відходами використовувати запропоновану технологію сортування-подрібнення, яка підвищує ефективність утилізації будівельних відходів, шляхом переобки та майбутнього використання у будівельних конструкціях. Таким чином, частково вирішується проблема забруднення територій сміттєзвалищами будівельних матеріалів.

Література

1. ООН: протягом останніх тридцять років обсяги видобутку природних ресурсів у світі подвоїлися. Новини ООН. Глобальний погляд Людські долі. Доступно: https://news.un.org/ua/story/2021/04/1401412.

2. Крупеніна О. Світовий видобуток корисних копалин. Україна у рейтингу добувних країн. Прес-центр ІА "ЛІГАБізнесІнформ". Доступно: https://biz.liga.net/ekonomika/all/opinion/mirovaya-dobycha-poleznych-iskopaemyh-ukraina-v-reytinge-dobyvayuschih-stran

3. We're gobbling up the Earth's resources at an unsustainable rate. UN Environment programme. Доступно: https://www.unep.org/ru/novosti-i-istorii/story/my-pogloschaem-resursy-zemli-absolyutno-neracionalnymi-tempami

4. World Mining Data 2020. International Organization Committee for the World Mining Congresses. Доступно: https://www.world-mining-data.info/wmd/downloads/PDF/WMD2020.pdf.

5. Negash, Y.T., Hassan, A.M., Tseng, M.L., Wu, K.J., Ali, M.H. (2021). Sustainable construction and demolition waste management in Somaliland: Regulatory barriers lead to technical and environmental barriers. Journal of Cleaner Production, 297, 126717. doi: 10.1016/j.jclepro.2021.126717.

6. Youcai, Z., Sheng, H. (2017). Recycling technologies and pollution potential for contaminated construction and demolition waste in recycling processes. Pollution Control and Resource Recovery, 195-331. doi: 10.1016/B978-0-12-811754-5.00008-7.

7. Bergonzoni, M., Melloni, R., Botti, L. (2023). Analysis of sustainable concrete obtained from the by-products of an industrial process and recycled aggregates from construction and demolition waste. Procedia Computer Science, 217, 41-51.

UDK 519.876.5

74. APPLICATION OF OBJECT BASED TECHNIQUE FOR ASSESSMENT OF URBAN LAND-USE/LAND COVER AND AIR QUALITY

Anila Kausar[1*], Ambreen Afzal[2], Altaf Hussain Lahori[3],
Viola Vambol[4,5]
[1] *University of Karachi, Karachi, Pakistan*
[2] *Bahria University Karachi Campus, Karachi, Pakistan*
[3] *Sindh Madressatul Islam University, Karachi, Pakistan*
[5] *University of Life Sciences in Lublin, Lublin, Poland*
[5] *National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine*
[*]*E-mail: anilak@uok.edu.pk*

Rapid population growth, the development of megacities due to the concentration of people in large cities leads to the development of new territories that were previously intended for green spaces, arable fields, countryside, parks, etc. All this refers to negative environmental trends. Using high resolution SAR images for urban Land-Use/Land Cover mapping, Land Use/Land Cover Index and Air Quality Index can be monitored for subsequent environmental protection decisions. An example of such a study is shown on a plot of 200 meters on both sides of the main Shahrah-e-Faisal road, Karachi (Pakistan). An object-oriented analysis and land use classification according to the LBC format was applied.

The growing trend of urbanization is fuelling a rapid transformation of land use patterns and land cover, the change of which accelerates the release of greenhouse gases into the environment and leads to climate change. Too rapid urban growth in

developing countries affects not only urban but also suburban areas. With the development of megacities, which, due to the natural overpopulation of cities, seize nearby land for new construction, the risk of air pollution increases, the ecological state worsens, and the quality of suburban arable land decreases.

Current trends are such that urban planning strategies should include walkable projects with mixed land use development.

An object-oriented approach using high-resolution SAR data for urban Land-Use/Land Cover mapping has been repeatedly used by researchers [1, 2]. Recently Alsharif et al. (2022) [3] reported that Land-Use/Land Cover and urban growth forecasting and analysis methods can help decision-makers involved in the management of administrative divisions at various levels to ensure effective sustainable planning.

Thus, the application of object-oriented analysis and land use classification according to the LBC format (ground classification), as well as the identification of the relationship of air quality with the presence and density of green cover AOI (area of interest) is an innovative approach to prevent and eliminate environmental problems.

This approach was tested on a 200-meter stretch on both sides of Shahrah-e-Faisal, the main road in Karachi, Pakistan, which connects more than ten main roads and many secondary roads. A very high resolution SAS Planet image was used for this, which was about 0.07 m/pixel. Visual (not automatic) identification and subsequent digitization were used. Using information from public domains like Wikimapia or Google Earth made it possible to geocode. A field survey was carried out in situ to identify or confirm objects that were not accurately classified (Fig. 1).

Fig. 1. The field survey

The analysis of Land-Use/Land Cover showed the development of residential areas in a mixed form, that is, along with residential buildings, business, retail and social infrastructure was actively expanding. At the same time, there were no industrial facilities and territories associated with the accumulation and processing of waste, which is a positive moment for the ecological state of the study area. 6,880,148 m^2 (or 5,075,838 m^2 excluding road surfaces) of an area of which 26.22% was green cover was surveyed. Air quality index (AQI) PM2.5 measurements were taken at 13 locations, showing the worst situation during peak hours from 12:00 to 16:00 with demonstrating a deterioration in the situation at a rapid pace at the intersection, while after 20:00 the situation was becoming acceptable. Shahrah-e-Faisal has connected almost all major and minor roads originating from almost the entire metropolitan area of Karachi and even from suburban areas.

The ecological framework in the city is necessary to maintain a favourable ecological state of the urban environment. The grass cover of the earth serves as a protection against soil erosion, a home for insects (including beneficial ones), and protects the earth from overheating. In addition to this, most green spaces have a positive impact on health in both the short and long term. Green zones of any type help to cope with perceived stress. Therefore, green cover is an important urban planning strategy and its importance can be judged by the air quality of the study area.

In the present study, the green cover in the study area is approximately 1804310 m^2 and is divided into six classes (Fig. 2)

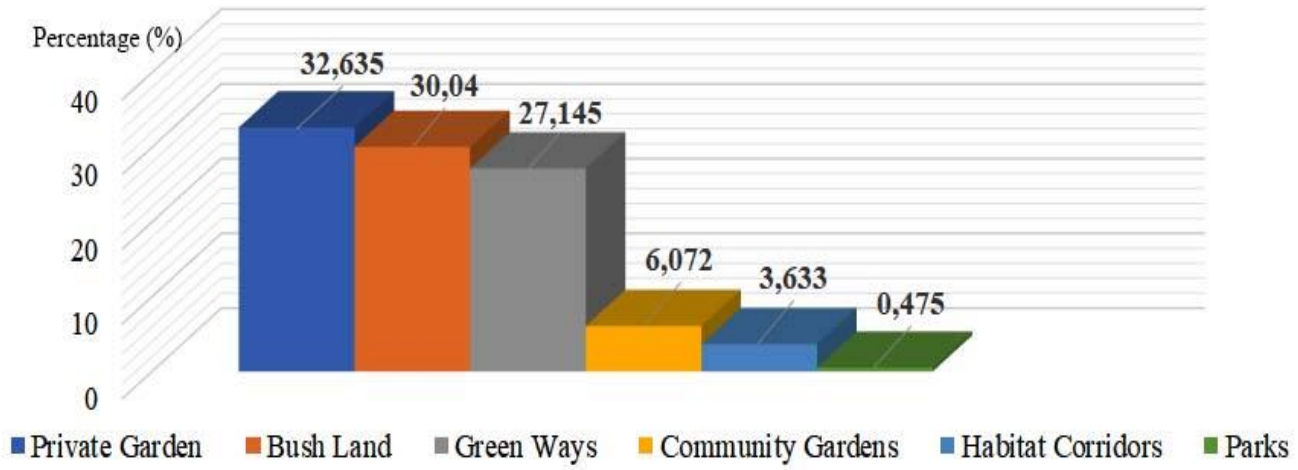


Fig. 2. Green Cover of Area of Interest

At the intersection of various main roads with Shahrah-e-Faisal, where the junction is being created, different air quality was found at different times of the day (Table 1, Fig. 3).

Table 1. Air quality index along Shahrah-e-Faisal (November 2022)

Locations	00:00	04:00	08:00	12:00	16:00	20:00
N5	10	12	65	178	287	134
FTC Flyover	20	10	74	201	300	153
Jinnah International Terminal	45	13	99	185	315	110
Karsaz Flyover and Road	34	17	97	200	250	137
PAF Base Flyover	52	6	83	245	274	161
Rashid Minhas Road	10	5	82	184	200	158
Regent Plaza Flyover	40	9	45	192	214	109
Shah Faisal Bridge	36	10	50	137	269	151
Shaheed e Millat Road and Flyover	25	16	102	241	302	130
Shahrah e Quaideen Road and Flyover	20	5	85	204	198	110
Star Gate	56	10	114	169	149	154
Tipu Sultan Road	40	14	64	100	286	116
University Avenue	25	13	81	185	200	100

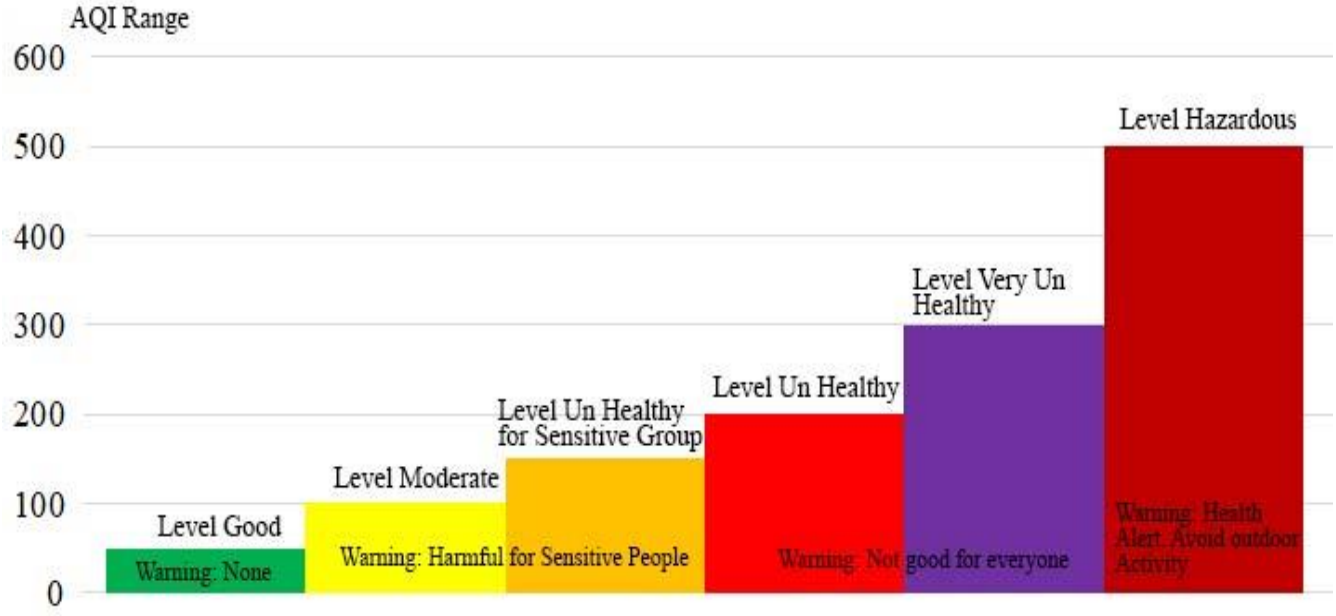


Fig. 3. Air quality index scale conventions

The area of green cover is insufficient along the road, which can also cause health problems. Therefore, there is an urgent need to create more trees near the node with the highest air quality index values in order to improve it.

Reference

1. Ban Y., Hu H. & Rangel I.M., 2010, Fusion of Quickbird MS and RADARSAT SAR data for urban land-cover mapping: Object-based and knowledge-based approach. International Journal of Remote Sensing 31(6): 1391-1410.

2. Hu H. & Ban Y., 2008, Urban land use/land cover mapping with high-resolution SAR imagery by integrating support vector machines into object-based analysis, [in:] Remote Sensing for Environmental Monitoring. GIS Applications, and Geology VIII 7110: 137-144.

3. Alsharif M., Alzandi A.A., Shrahily R. & Mobarak, B., 2022, Land Use Land Cover Change Analysis for Urban Growth Prediction Using Landsat Satellite Data and Markov Chain Model for Al Baha Region Saudi Arabia. Forests 13(10): 1530.

РОЗДІЛ 9

ВИКЛИКИ ТА ЗАГРОЗИ КРИТИЧНІЙ ІНФРАСТРУКТУРІ ПРИ ЕКСПЛУАТАЦІЇ ТА ЗАКРИТТІ ВУГІЛЬНИХ ШАХТ

УДК 622.83+ 321.323

75. THREATS OF THE ECOLOGICAL CHAOS STATE FOR CRITICAL INFRASTRUCTURE FACILITIES WITHIN DONBASS AND KRYVBASS IN THE CONDITIONS OF RUSSIAN AGGRESSION

Yakovliev Ye.O.[1], Rudko G. I. [2]

1 Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine, Київ, Україна

2 State Geology and Subsoil Service of Ukraine, Київ, Україна;

E-mail: yakovleve1939@gmail.com, rudko@dkz.gov.ua

Загрози стану екологічного хаосу для об'єктів критичної інфраструктури Донбасу і Кривбасу за умови російської агресії

У статті проведено аналіз загроз виникнення екологічного хаосу для об'єктів критичної інфраструктури Донбасу і Кривбасу внаслідок воєнно-техногенного впливу чинників збройного конфлікту. Гірничодобувні райони (ГДР) Донбасу та Кривбасу є одними із найбільших у світі природно-техногенних геосистем (ПТГС) "гірничо-промисловий комплекс- навколишнє природне середовище" і мають довгостроковий період індустріального формування (більше 150 років). Крім того, в межах обох ГДР було використано більше 7 млн. тон вибухових речовин (ВР), що суттєво знизило геотехнічну стійкість ділянок розташування об'єктів критичної інфраструктури (ОКІ).

За умови ракетно-артилерійських обстрілів (вага заряду вибухівки від 50 до 450-950 кг) відбувається зростання небезпечних порушень геологічного середовища (ГС) -активізація техногенної тріщинуватості, осадкові деформації земної поверхні, розвиток ділянок приповерхневого виділення вибухонебезпечного метану і ін.). і погіршення еколого-геологічних умов експлуатації ОКІ та життєдіяльності населення..

The mining regions of Donbass and Kryvbass are one of the largest in the world of natural-technogenic geosystems (NTGS) "mining-industrial complex - natural environment" and have a long-term period of industrial formation (more than 150 years). The Donetsk coal and Kryvorizka iron ore basins within three regions - Luhansk, Donetsk, Dnipropetrovsk cover an area of up to 16,000 km2, within which more than a thousand mines have been built, of which several dozen are currently being exploited with a maximum depth of up to 1.5 km. In general, up to 17 billion tons of mineral raw materials were mined inm the mining districts (MD) of Donbas and Kryvbas with a total volume of mining galleries of up to 10 billion cubic meters. In addition, more than 7 million tons of explosive substances (ES) were used within both MD , which significantly reduced the geotechnical stability of critical infrastructure

objects (CIO), the spatial density of which is up to 2-3 times higher than the average indicators for Ukraine, and disturbed the balance of the upper zone of the geological media GM within the NTGS (table. 1).

Table 1. Environmental and geotechnical parameters of the mining districts of Donbass and Kryvbass

№№	Name,	Mining-technogenic parametres		Extraction of mineral raw		Mine water inflow	
		Quantity of mines (pits)	Maximum depth of galleries,m	Млрд. тон	Об'єм гірничих виробок, млрд.м^3	Mln m^3/**year** (max)	Mineralisation, g/dm^3
1	Donbas	**>220**	>1500	12.9	8.1	780	2.6-3.5
2	Kryvbas	11 (9)	1400	6.2	2.1	40	5-40

During the industrial development of Donbas and Kryvbas, as a result of the abnormal concentration of environmentally hazardous mining, chemical, metallurgical, energy, processing and other enterprises within the NTGS, the main factors for the deterioration of the environmental parameters of the GM are:

- chemical pollution of landscapes;
- significant lowering of groundwater levels, undwemining of surface reservoirs;
- discharge of highly mineralized aggressive mine waters into the river system;
- the development of subsidence of the day surface with the complication of the engineering and geological condition of CIO, residential and industrial facilities and the activation of dangerous exogenous geological processes (flooding, man-made subsidence of the earth's surface, landslides, karst, etc.);
- decrease in the engineering-seismological stability of rock massifs under the influence of the rocks mobility growth in the zones of their undwemining by galleries , manifestations of hydromechanical shocks, etc.;
- creation of a large number of mine rock hills ("terricons"), including with carbon particles, which is also a source of pollution of water resources, soils and surface atmosphere due to burning and explosions;

- contamination of underground water intakes due to the deterioration of the conditions of their formation and quality in the zones affected by flooding and land overmoisturing.

- pollution of sources of local drinking water supply, development of areas of near-surface release of explosive methane, etc.). and the deterioration of the ecological and geological conditions of the operation of OKI and the life of the population in the regions.

Under the conditions of rocket and artillery fire (the weight of the explosive charge is from 50 to 450-950 kg), there is an increase in dangerous violations of the geological environment (activation of man-made fracturing, destruction of dams storing toxic waste, subsidence deformations of the earth's surface, an increase in the area of catastrophic inundation and flooding within the boundaries of cities and settlements.

The most dynamic and dangerous deterioration of the ecoparameters of the GM of Donbass and Kryvbas is associated with the uncontrolled flooding of mines and the regional self-rehabilitation rise of groundwater levels to dangerous depths (less than 150-200m), when additional activation of the above-mentioned man-made violations of the GM occurs. The increase of the dangerous changes in the GM of Donbass and Kryvbass is influenced by counterfeiting of mining productions of rivers, streams, and reservoirs (more than 174 objects, up to 700 cases).

The restoration of the historical surface of groundwater during the closure and flooding of mines is the main factor of chaotic and dangerous changes in the ecological parameters of the geological environment and the environment as a whole. The fact is that the area of groundwater level rise is 5-10 times more greater than the area of mining operations, which causes long-term (tens of years) chaotic reshaping of trchnogenic geological systems (TGS) "OKI-geological environment".

The performed analysis confirms that most of the changes in the ecological state of the Donbas and Kryvbas regions are irreversible, which is due mainly to the extraction of large volumes of mineral raw materials with a spatio-temporal disturbance of the ecologically-forming balance of the system "lithosphere-biosphere" and the slowing down of lithospheric processes (water-energy transfer , lithogenesis, etc.).

As a result, almost the majority of man-made changes in the environmental parameters of the GMMwithin the developed ("old") MD of Ukraine at the post-mining stage have a critical reduction in biodiversity and the natural resource potential of socio-economic and ecological-technological recovery. In this regard, it is sufficient to compare the ecological state of the Donbas MD and the Chernobyl Nuclear Power Plant Exclusion Zone (Table 2).

Additional complications of operating conditions of OKI within Donbass and Kryvbass may be due to flooding of tericons (up to 1,350 objects, including more than 230 burning (Donbas) and toxic waste landfills (up to 1,200 objects), flooding of

chemically contaminated workings of the mine "Olexandr- Zahid" and chambers of an underground atomic explosion ("Yunkom mine"). The city-forming character of the mines has led to the formation of up to 60 industrial-urban agglomerations above the mining workings, where a large number of CIOs are exploited under conditions of flooding and destructive deformations of the earth's surface.

In the current conditions of Russian aggression, the decommissioning of the majority of Donbas mines takes place according to the scheme of "wet conservation" (self-rehabilitation flooding) within the hydrogeofiltration system "water divided aeria-river " (ac. V. M. Shestopalov, Prof. G. I. Rudko, Prof. A.V. Lushchyk, prof. O.M. Trofymchuk, Ph.D. G.G. Lutiy, Ph.D. V.O. Slyadnev and etc.) provided there is a practical absence of anticipatory environmental protection measures.

Table 2. Dangerous technogenic impact to environment in Donbass and Chernobyl (*Comparative analysis*)

Chernobyl	Donbass
Chemical and radioactive contamination of landscape will disappear in natural way up to 2035 year. More than 90% of the area will be available for human living	Contamination of landscape is irreversible. Soil and bottom sludge will keep sustainable capacity of pollutants
Rock mass still intact	Subsidence of rock mass started. Many underground crack formed over mines working zone
Surface water contaminated with radionuclides on period up to 15 years	Sustainable contamination of local rivers with water from flooded coal-mines
Limited short-term contamination of underground water with radionuclides	The ongoing elimination of underground water sources as a result of active infiltration of different technogenyc pollutants from surface (waste sites) and underground (coal-mines)
Short-term (up to 1 year) contamination of atmosphere and surface level of soil	Increasing contamination of atmosphere and surface level of soil with methane and radon

Seismological risks are almost absent. Only earthquakes in Romania (Vrancha) may affect sarcophagus.	Permanent risk of “technogenic earthquakes” as a result of flooding of coal-mines

In general, the formation of "ecological chaos" state within the NTGS "MD-environment" and the complication of the CIO operating conditions will be characterized by the following long-term consequences:

1) dangerous changes in the eco-parameters of the local population life , including local sources of drinking water supply (domestic wells, springs, ponds, etc.);

2) irreversible disruption of the interaction between the biosphere and the lithosphere and the reduction of biodiversity;

3) increase in the impact of negative factors of global climate change (warming, uneven rainfall, increase in height and frequency of floods).

Conclusions

1. The influence of Russian aggression on the formation of "ecological chaos" a state for the conditions of operation of CIO within the borders of the MD of Donbas and Kryvbas is mainly connected with the development of regional flooding and land owermoisturing.

2. The spatio-temporal variability of changes in the ecological and geological state of CIOs within the borders of the MD of Donbas and Kryvbas causes the need for their accelerated zoning according to the sequence and composition of protective measures to increase the stability of CIOs.

List of references

1. Yakovlev Ye.O. Critical changes in the ecological state of the Donbas subsoil. Mineral resources of Ukraine, No. 3, 2017, pp. 34-39.

2. Rudko G.I., Yakovlev Ye.O. Regional technogenic changes in the ecological and geodynamic conditions of iron ore deposits development within Kryvbas. Mineral resources of Ukraine, No. 2, pp. 43-50.

3. Monograph "Ecological safety of coal deposits of Ukraine", co-authors Rudko G.I., Bondar O.I. etc.. Kyiv, BukRek, 2016, 508 p.

4. Kuznetsov B.T., Chumachenko S.M., Yakovlev Ye.O., Morshch E.V. The potential impact of the flooding of Donbas mines on the natural and man-made safety of the military infrastructure of the Armed Forces of Ukraine. Modern information technologies for management of environmental safety, nature management, measures in emergency situations: trends of 2020. Collective monograph based on the materials of the 19th International Scientific and Practical Conference (Kyiv, October 06-07,

2020) / By general ed. S.O. For a long time Kyiv: Yuston Publishing LLC, 2020. P.142-147.

УДК 621.396.4

76. ЕКОЛОГО-ГЕОЛОГІЧНІ ЧИННИКИ ВРАЗЛИВОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗА УМОВИ РОСІЙСЬКОЇ АГРЕСІЇ

Єрмаков В. М.[1], Чумаченко С. М.[2], Кодрик А.І.[3], Яковлєв Є.О.[4]

3 Державна екологічна академія післядипломної освіти та управління, Київ, Україна

4 Національний університет харчових технологій, Київ, Україна;

5 Державна екологічна академія післядипломної освіти та управління, Київ, Україна

6 Інститут телекомунікацій та глобального інформаційного простору президії НАН України, Київ, Україна

E-mail: evn54@ukr.net, s_chum@ukr.net, kodrik@ukr.net, yakovleve1939@gmail.com

Environmental and geological factors of the vulnerability of critical infrastructure objects under the conditions of Russian aggression

The article presents approaches to assessing the sensitivity of the geological environment of Ukraine to imbalances under the influence of the impact factors of the armed conflict. This leads to a decrease in the engineering-geotechnical stability of the foundation of critical infrastructure objects (OKI) and the occurrence of emergencies. Ukraine is a developed country and has a large number of critical infrastructure facilities (CIF), most of which are located in mining areas (MA) and large industrial urban agglomerations (IUA). These areas have significant man-made and natural disturbances of the geological media (GM) by dangerous processes that can be activated under the conditions of rocket and artillery fire, bombings and the destruction of protective constructions.

Україна є розвиненою європейською країною, що має велику кількість об'єктів критичної інфраструктури (ОКІ). До ОКІ відносяться об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам. Більшість з цих об'єктів розташовані в гірничо-добувних районах (ГДР) видобутку корисних копалин і великих промислових міських агломераціях (ПМА).

Внаслідок російської агресії здійснюються ураження ОКІ України із застосуванням усіх можливих військових засобів ураження:

- артилерійських великокаліберних гаубиць;
- ракетних систем залпового вогню;
- зенітно-ракетних комплексів С-300 та С-400;
- крилатих ракет повітряного і морського базування;
- - ударних безпілотних літальних апаратів та дронів-камікадзе;
- - оперативно-тактичних ракетних комплексів.

Рис. 1. Результати ураження об’єктів критичної інфраструктури України

Враховуючи те, що ці території мають значні техногенні та природні порушення геологічного середовища (ГС) небезпечними екзогенними геологічними процесами (НЕГП- підтоплення, зсуви, просідання, карст і т.ін.), що можуть активізуватися в умовах ракетно-артилерійських обстрілів, авіаційних бомбардувань та руйнування під цими уражаючими впливами захисних споруд, постає цілий ряд питань щодо визначення науково-обґрунтованих категорій та визначень для територіальних угрупувань ОКІ.

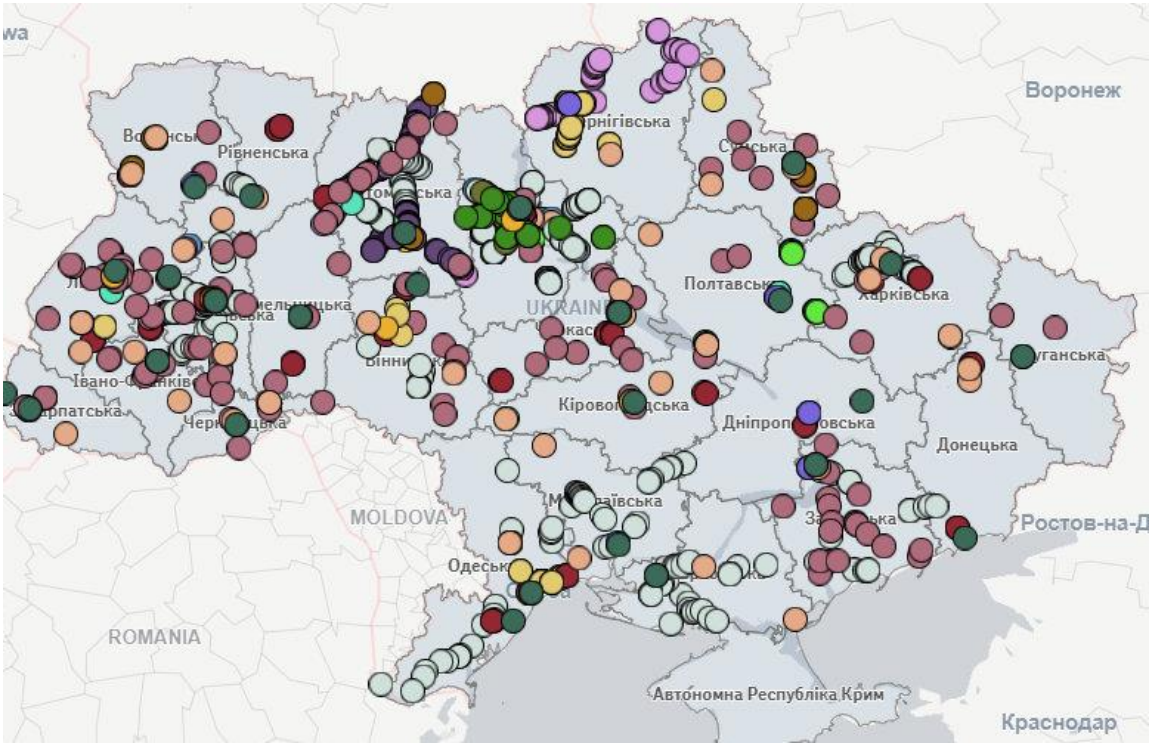


Рис. 2. Електронна карта ураження об’єктів критичної інфраструктури України

Критичною інфраструктурою називають такі засоби, обладнання, мережі та служби, які, у разі їх пошкодження чи руйнування, будуть значно впливати на здоров’я, безпеку, економічний стан чи ефективне функціонування як окремих об’єктів, так і регіону та країни в цілому. Така інфраструктура, у разі її незахищеності, може бути вразливою до впливу небезпечних чинників природного, техногенного чи військового характеру, а також терористичних атак [1].

Чутливість ГС України до впливу уражаючих чинників збройного конфлікту призводить до зменшення інженерно-геотехнічної стійкості підґрунтя ОКІ і виникнення надзвичайних ситуацій воєнно-техногенного походження.

Проведений аналіз засвідчив, що за умови повномасштабного збройного конфлікту захисний потенціал ОКІ значною мірою залежить від здатності верхньої зони ГС до асиміляції (депонування та нейтралізації) порушень його рівноваги у складних природно- техногенних системах (ПТГС) “техногенний комплекс- геологічне середовище” (гірничо-добувні райони, промислово-міські агломерації, промислові майданчики, АЕС, ГЕС, ТЕС, ТЕЦ і т. ін.).

На нашу думку, переважна концентрація ОКІ у складних ПТГС, уражених небезпечними екзогенними геологічними процесами (підоплення, зсуви, просадки, карст та т.ін.) обумовлює необхідність розробки наукових основ зонування України за рівнем територіальної вразливості за умови збройних впливів російської агресії.

Враховуючи вищенаведені чинники, необхідним є:

1) удосконалення моніторингу територій розташування ОКІ, перш за все інженерно-геотехнічного та екологічного стану ГС;

2) юридичне визначення категорії “території вразливості ОКІ”, враховуючи їх взаємозв’язок в ГДР , ПМА та великих ПТГС.

Моніторинг геологічного середовища територій із розташованою на них критичною інфраструктурою необхідно виконувати із використанням сучасних засобів і методів [2, 5, 6].

Категорія критичності ОКІ, ступінь (відносний рівень) важливості об’єкта критичної інфраструктури, класифікована (категоризована) залежно від його впливу на виконання життєво важливих функцій та/або надання життєво важливих послуг. Категорія “території вразливості ОКІ” — ступінь (відносний рівень) небезпечності (загрозливості) території, на якій розташовані ОКІ, класифікована (категоризована) залежно від її впливу на виконання екологічно важливих функцій та/або забезпечення життєдіяльності ОКІ.

Захист критичної інфраструктури є ключовим у заходах планування цивільного захисту будь якої країни [3, 4]. Таким чином, виникає гостра необхідність розроблення ефективних засобів попередження надзвичайних ситуацій із використанням перспективних інформаційно-телекомунікаційних технологій та сучасних методів і засобів зі створенням безпроводових сенсорних мереж [2, 3].

Висновки

Виконаний аналіз еколого-геологічної стійкості територій розподілу ОКІ України за умови російської агресії дозволяє зробити наступні висновки:

1. Території підвищеної вразливості ОКІ переважно формуються у гірничо-добувних районах та промислово-міських агломераціях (ПМА) Придніпровського регіону з розповсюдженням просадкових лесових грунтів.

2. Сучасне зростання глобальної сейсмічності підвищує вразливість ОКІ України в Причорноморському регіоні з масштабним розвитком територій підтоплення у ПМА та схилових комплексів.

3. Система екологічного моніторингу території підвищеної вразливості ОКІ вимагає удосконалення на базі використання високочутливих до змін ГС технологій ДЗЗ (інтерферометрія, спектрометрія, газогеохімія, термометрія) та математичних моделей.

Література

1. Лисенко О.І., Чумаченко С.М., Новіков В.І., Сушин І.О., Тачиніна О.М., Фуртат О.В. Оперативне керування рухом розподіленого інформаційно-телекомунікаційного робота. // Наукові праці Четвертої міжнар. наук.-практ. конф. «Сучасні тенденції розвитку інформаційних систем і телекомунікаційних технологій», 1–2 лютого 2022 р. (Київ, Україна). – К. : НУХТ, 2022. –с. 108-114.

2. Methodological Bases for Monitoring the Ecological State of the Geological Environment in the Mine Flooding Zone of Donbas Under the Influence of Armed Conflict. - K.: EAGE Publications BV, XVI 16th International Conference Monitoring of Geological Processes and Ecological Condition of the Environment. Nov 2022, Volume 2022, p.1 – 5. DOI: https://doi.org/10.3997/2214-4609.2022580081
3. Лисенко А.И., Чумаченко С.М., Шевченко В.Л. Математически модели и информационни технологии за оценка и прогнозиране състоянието на околната среда в изпитателни полигони. Издател: Про Лангс, език: Български. – 2017 р.
4. Тачиніна О.М. Условия оптимальности траектории движения носителя при размещении сенсоров в зоне чрезвычайной ситуации /О.М.Тачиніна, О.І. Лисенко, С.М.Чумаченко// Техническая механика: научный журнал. –2016. – №. 3 – С.87-93.
5. Dr Ye. Yakovliev and Dr S. Chumachenko Ecological Threats in Donbas Ukraine (assessment of ecological hazaedsin donbas impacted by the armed conflictsin eastern Ukraine). with contributions from HD staff.-2017 - Canada, 60 p.
6. Гавриленко Ю.М., Ермаков В.Н., Кренида Ю.Ф. и др. Техногенные последствия закрытия угольных шахт Донбасса. НОРД-ПРЕСС, Донецк, 2004, 631с.

УДК 622.5:504.4.054

77. РЕСТРУКТУРИЗАЦІЯ ШАХТ ДОНБАСУ В УМОВАХ ВІЙСЬКОВИХ ДІЙ

Дятел О.О. [1], Лубенська Н.О. [2], Єрмаков В.М. [1]
[1]Державна екологічна академія післядипломної освіти та управління, Київ, Україна
[2]Центр постмайнінгу, Вища технічна школа Георга Агріколи, Німеччина
alexandr_dyatel@ukr.net

Restructuring of mines of donbas in the conditions of military actions

All wars end sooner or later, and despite the difficult times for Ukraine, it is necessary to think about the future right now. Because, after the end of the war, we have to rebuild Ukraine, and the acquired experience of international partners should be useful in the restoration of destroyed or damaged infrastructure and territories as a whole. Therefore, it is already necessary to conduct an analysis of the state of Donbas mines as a basis for their restructuring.

Військовий конфлікт в Україні призвів до прямого небезпечного впливу бойових дій на усі екологічні складові довкілля, у т. ч. на поверхневі і підземні води, оскільки значно збільшилися ризики виникнення аварійних ситуацій на

вугільних підприємствах, що розташовані поблизу лінії зіткнення. Основна небезпека в умовах конфлікту пов'язана з можливістю забруднення навколишнього середовища через аварії та неконтрольоване затоплення суміжних шахт на територіях, що не контролюються Урядом України.

Понад 35 шахт регіону затоплюється або вже повністю затоплені та не підлягають подальшій експлуатації. Частину пошкоджених або зупинених шахт на Донбасі було демонтовано [1]. Найбільша проблема в тому, що переважна більшість з них – на непідконтрольній території. Це одна з основних причин потенційного забруднення підземних та поверхневих вод при їх контакті з шахтними водами, забрудненими, зокрема, залізом, хлоридами, сульфатами, іншими мінеральними солями й важкими металами.

Неконтрольоване затоплення шахт несе в собі величезну небезпеку. Підйом рівня шахтних вод до критичних відміток спричинить незворотні зміни у масивах гірських порід, внаслідок чого відбуватиметься підтоплення територій, просідання денної поверхні, активізування обвалів, зсуви ґрунту тощо. Шахтні води окислюються, насичуються металами, оскільки все обладнання, яке колись існувало під час гірничих робіт, залишилось там, у шахтах. Тож при контакті з залізобетонними конструкціями відбувається процес насичення шахтних вод небезпечними сполуками. Найбільшу ж небезпеку несе просідання поверхні, яка викликає деформацію фундаментів та руйнування споруд.

Підземні та поверхневі води, які проникають у гірничі виробки називаються шахтними водами. Вони зазвичай мають високу мінералізацію та можуть бути забруднені як механічними так і хімічними домішками. Шахтні води негативно впливають на процес видобування корисних копалин, пошкоджують техніку та підземні споруди, знижують якість видобутих корисних копалин. Тому під час експлуатації шахти ці води постійно відкачують, а перед скиданням у водойми очищують – відстоюють у ставках-освітлювачах, нейтралізують чи демінералізують у залежності від хімічного складу.

Процес шахтного водовідливу не повинен припиняється навіть коли шахта припинила функціонувати, аби запобігти її затопленню. Такий спосіб закриття шахт називається «сухою» консервацією та є найефективнішим, але потребує значних капітальних та експлуатаційних витрат.

Існує простіший, але небезпечний для довкілля спосіб «мокрої» ліквідації шахти – неконтрольоване затоплення гірничої виробки шахтною водою. Саме такий процес через брак фінансування та халатність відповідальних осіб відбувається протягом останніх дев'яти років на багатьох шахтах, які розташовані на тимчасово окупованих територіях Донбасу.

Проте для шахт, які утворюють єдину гідравлічно взаємопов'язану підземну систему, не існує лінії розмежування, і як наслідок підняття рівня води в одній шахті може призводити до ланцюгової реакції на інших гідравлічно пов'язаних шахтах. Саме така картина спостерігається протягом останніх років.

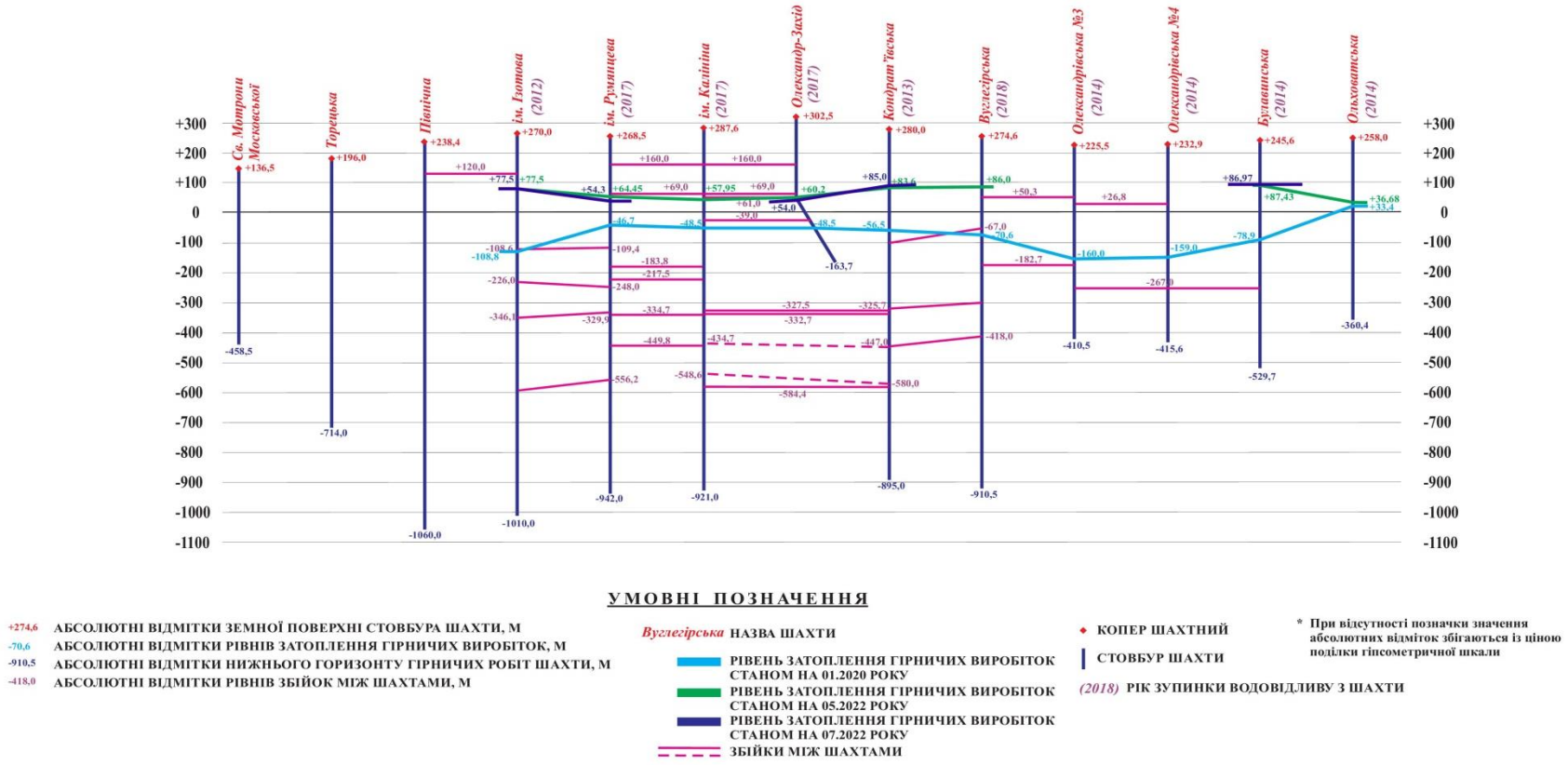


Рис.1. Рівень затоплення гірничих виробок шахт північного крила ЦРД

Як видно з рисунка 1 рівень затоплення гірничих виробок шахт північного крила ЦРД з кожним роком збільшується, тобто відбувається неконтрольоване затоплення шахтних виробок.

Оскільки відновити видобування вугілля у затоплених шахтах практично не можливо, то потрібно прийняти цей виклик і побудувати систему менеджменту, яка б забезпечила прийнятний екологічний та соціально-економічний стан вуглевидобувного регіону тобто розробити концепцію пост-майнінгу.

Схожий шлях свого часу пройшла Німеччина. Так, земля Північний Рейн-Вестфалія, пройшла важкий шлях, від колапсу економіки після Другої Світової війни, поступової відбудови, енергетичної кризи у 60-х роках минулого сторіччя, відмови від дотаційних шахт і припинення вуглевидобутку у 2018 році до повної трансформації у інноваційний хаб Німеччини.

Оскільки некероване затоплення може призвести до непередбачених наслідків, то ключовим в процесі закриття шахт чи пост-майнінгу, з технічної точки зору, являється управління шахтними водами. Успішне управління таким процесом уже втілене в життя на прикладах так званих «водних провінцій» вугільних басейнів Рур та Саар, з поступовим переходом з підземних водовідливів на центральні водовідливи «колодязного типу». Такий комплексний підхід дає можливість значно скоротити витрати на вирішення «вічних» проблем пост-майнінгу, пов’язаних з шахтними водами [2,3]. Саме створення державно-громадського партнерства, яке успішно функціонує у Німеччині, дозволить вирішити проблему пост-майнінгу не тільки на території Донбасу, а і дасть поштовх для розвитку нового напрямку науки в Україні.

В Німеччині реструктуризація вугільної промисловості відбувалась поступово і за підтримки держави та ініціатив державно-громадського партнерства. За цей час вдалося створити новий імідж колишніх мономіст: від старої промислової зони до головного офісу з виробничою компетенцією та інноваціями. Міська агломерація з 5-мільйонним населенням отримала нові горизонти: спеціалізація на основі екологічних технологій і нової мобільності, цифрових комунікацій і кібербезпеки, логістики та охорони здоров’я.

Зараз земля Північний Рейн-Фестфалія – це один з культурних центрів Німеччини із 130 музеями, 6 університетами, 15 коледжами та 60 дослідницькими центрами, 6 оперними театрами та багатьма об’єктами культурно-промислової спадщини [4].

Саме тому, вже зараз потрібно вивчити та розробити власну концепцію управління шахтними водами, базуючись на прикладі «водних провінцій» RAG AG в Німеччині. Звісно, що Україні передує довгий та складний шлях відновлення проте для розробки подібної концепції не потрібно очікувати завершення війни. Всі необхідні дані, такі як схеми шахтних полів та гірничих виробок є в наявності у відповідних міністерствах та установах.

Література

1. Оцінка екологічної шкоди та пріоритети відновлення довкілля на сході України. – К.: BAITE, 2017. – 88 с.
2. Електронний ресурс: http://www.zechenkarte.de/
3. Електронний ресурс: www.rag.de
4. Електронний ресурс: «EURACOAL Market Report 2022 no.1»