Volodymyr S. Blintsov
Блінцов Володимир Степанович

Pavlo V. Maidaniuk
Майданюк Павло Володимирович

УДК 005.8

MODEL OF INFORMATION PLATFORM OF MANAGEMENT OF PROTECTION PROJECTS OF MARINE CRITICAL INFRASTRUCTURE OBJECT

МОДЕЛЬ ІНФОРМАЦІЙНОЇ ПЛАТФОРМИ УПРАВЛІННЯ ПРОЕКТАМИ ЗАХИСТУ ОБ'ЄКТА МОРСЬКОЇ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

DOI https://doi.org/10.15589/smi2019.2(12).1

Volodymyr S. Blintsov Блінцов Володимир Степанович, докт. техн. наук, проф.
volodymyr.blintsov@nuos.edu.ua
ORCID: 0000-0002-3912-2174

Admiral Makarov National University of Shipbuilding, Mykolaiv
Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв

Pavlo V. Maidaniuk Майданюк Павло Володимирович
udm@dsszzi.gov.ua
ORCID: 0000-0002-1289-019X

State Service of Special Communication and Information Protection of Ukraine in Mykolaiv region, Mykolaiv
Управління Державної служби спеціального зв'язку та захисту інформації України в Миколаївській області, м. Миколаїв

Abstract. The work is devoted to the development of a model of information platform for project management of marine critical infrastructure protection as a theoretical basis for improving the efficiency of project planning in the early stages of development. The basis of the work is a systematic approach to the construction of a system of protection of marine critical infrastructure, which takes into account the relationship between the main components of their operation – material, energy, information and personnel. For each component, it is proposed to systematically analyse and include in the information platform the characteristics of the security objects and the possible threats to these components of the functioning of the security objects. It is also proposed to include in the information platform the methods of counteracting threats and the technologies for building systems for protection against these threats. A typical list of organizations participating in marine critical infrastructure protection projects and consumers of project information has been formed, which forms the basis for planning communications in such projects. The substantive part of the main information modules of the project for protection of marine critical infrastructure objects has been formed in the form of sets of information models of the system components of their functioning. Based on the operations on the sets, the work of the project manager on the planning of the work on the creation of the system of protection of the basic object of marine critical infrastructure is formalized. The structure and main components of the marine critical infrastructure protection project management information platform have been developed. The information platform contains information modules on the basic characteristics of the basics of marine critical infrastructure, threats and methods of counteracting them, as well as an information module on information about technologies for building security systems for such facilities. The resulting information platform forms an effective project manager toolkit and allows you to reduce time spent on the project planning stage. The practical task of developing the substantive parts of information platforms for managing the processes of developing the systems of protection of the underwater part of the offshore stationary platform and its waters has been solved.

Key words: information platform; maritime critical infrastructure; protection project management.

Анотація. Робота присвячена розробці моделі інформаційної платформи управління проектами захисту об'єктів морської критичної інфраструктури як теоретичної основи підвищення ефективності планування проектів на ранніх стадіях розробки. В основу роботи покладено системний підхід до побудови системи захисту об'єктів морської критичної інфраструктури, який передбачає урахування взаємозв'язку між основними складниками їх функціонування – матеріальними, енергетичними, інформаційними і кадровими. Для кожного складника пропонується системно аналізувати та включати до складу інформаційної платформи характеристики об'єктів захисту та можливі

загрози цим складникам функціонування об'єктів захисту. Також пропонується включати до інформаційної платформи методи протистояння загрозам і технології побудови систем захисту від цих загроз. Сформовано типовий перелік організацій – учасників проектів захисту об'єктів морської критичної інфраструктури та споживачів інформації про проект, що утворює основу для планування комунікацій у таких проектах. Сформовано змістовну частину основних інформаційних модулів проекту захисту об'єктів морської критичної інфраструктури у вигляді множин інформаційних моделей системних складників їх функціонування. На основі операцій над множинами формалізовано роботу менеджера проекту щодо планування робіт по створенню системи захисту базового об'єкта морської критичної інфраструктури. Розроблено структуру та основні складники інформаційної платформи управління проектами захисту об'єктів морської критичної інфраструктури. Інформаційна платформа містить інформаційні модулі основних характеристик базових об'єктів морської критичної інфраструктури, загроз та методів протистояння ним, а також інформаційний модуль відомостей про технології побудови систем захисту таких об'єктів. Отримана інформаційна платформа утворює ефективний інструментарій проектного менеджера і дає змогу зменшити витрати часу на стадії планування проекту. Розв'язано практичну задачу розробки змістовної частини інформаційних платформ управління процесами захисту підводної частини морської стаціонарної платформи та її акваторії.

Ключові слова: інформаційна платформа; морська критична інфраструктура; управління проектом захисту.

References

[1] Kontseptsiia stvorennia derzhavnoi systemy zakhystu krytychnoi infrastruktury. № 1009-p. (2017). Retrieved from: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80.

[2] Priorytetni napriamy zakonodavchoho ta orhanizatsiinoho zabezpechennia pasportyzatsii ob'iektiv krytychnoi infrastruktury. Retrieved from: http://old2.niss.gov.ua/content/articles/files/1_Ivaniuta-9af75.pdf.

[3] Lee Gordner, (2014). *Offshore Oil and Gas Safety and Security in the Asia Pacific – The Need for Regional Approaches to Managing Risks*. S. Rajaratnam School of International Studies. Nanyang Technological University, 104 P. Retrieved from: https://www.rsis.edu.sg/wp-content/uploads/2014/07/Monograph2613.pdf.

[4] *Offshore Oil and Gas Resources Sector Security Inquiry*. Office of the Inspector of Transport Security. Commonwealth of Australia 2012. 148 P. Retrieved from: https://www.homeaffairs.gov.au/transport-security/files/offshore-oil-gas-resources-sector-security-inquiry.pdf.

[5] Martin A. Sebastian, (2015). Critical Infrastructures – Offshore Installation Protection. *Maritime Institute of Malaysia*. Centre of Marine Security & Diplomacy. 33 P. Retrieved from: http://www.mima.gov.my/images/page/research/Capt._Martin_National_Key_Infrastructure_AED.pdf.

[6] Mikhail Kashubsky, & Anthony Morrison. (2013). Security of offshore oil and gas facilities: exclusion zones and ships' routeing. *Australian Journal of Maritime & Ocean Affairs*. 5(1), 10 P. Retrieved from: https://doi.org/10.1080/18366503.2013.10815725.

[7] Robert Watts. (2005). Maritime Critical Infrastructure Protection: Multi-Agency Command and Control in an Asymmetric Environment. *Homeland Security Affairs*. I (1,2). Article 3. 12 P. Retrieved from: file:///C:/Users/volodymyr.blintsov/Downloads/1.2.3%20(1).pdf.

[8] Recovery Plan for the National Strategy for Maritime Security. (2006). *The Maritime Infrastructure*, 63 p. Retrieved from: https://www.dhs.gov/sites/default/files/publications/HSPD_MIRPPlan_0.pdf.

[9] The UK National Strategy for Maritime Security. (2014). Presented to Parliament by the Secretary of State for Defence by Command of Her Majesty. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/322813/20140623-40221_national-maritime-strat-Cm_8829_accessible.pdf.

[10] Heiko Borchert. (2014). *Maritime Security at Risk*. Lucerne: Sandfire. 52 p. Retrieved from: https://www.borchert.ch/content/ger/cmsfiles/publications/1407_Borchert_Maritime_Security_at_Risk.pdf.

[11] *The Guidelines on Cyber Security Onboard Ships*. (2018). Version 3. Produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL. 53 Pages. Retrieved from: http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16.

[12] Nineta Polemi. (Elsevier 2017). *Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains*. 214 Pages. Retrieved from: https://www.elsevier.com/books/port-cybersecurity/polemi/978-0-12-811818-4.

[13] *Protecting the Connected Barrels. Cybersecurity for Upstream Oil and Gas.* (2017). A report by Deloitte Center for Energy Solutions. Deloitte Development LLC. 22 Pages. Retrieved from: file:///C:/Users/volodymyr.blintsov/Downloads/DUP_Protecting-the-connected-barrels%20(1).pdf.

[14] Kharytonov, Yu.M., Hordieiev, B.M. ta Berdynskykh, B.V. (2017). Modeliuvannia informatsiinoi platformy upravlinnia proektamy rozvytku portovoi infrastruktury. *Scientific Journal «ScienceRise»*. Kharkiv, 1/2 (30), 39-47. DOI: 10.15587/2313-8416.2017.91279.

[15] Hrytsaienko, M. (2018). Development of the Information Platform Model for the Neutralization of Underwater Potentially Dangerous Objects. *Technology Audit and Production Reserves*. 2/2(40), 57-62. DOI: 10.15587/23112-8372.2018.129208.

[16] Dihé, Pascal, Ralf Denzer, & Sascha Schlobinski. (2015). An Information Model for a Water Information Platform. *International Federation for Information Processing*. p. 91–101. Retrieved from: https://hal.inria.fr/hal-01328529/document.

[17] Ruonan Sun, Shirley Gregor, & Byron Keating. (2015). Information Technology Platforms: Definition and Research Directions. *Australasian Conference on Information Systems*. Adelaide. 17 pages. Retrieved from: https://arxiv.org/ftp/arxiv/papers/1606/1606.01445.pdf

[18] Simon Alterman. *Information Platforms: A Business Model Framework*. Retrieved from: https://www.outsellinc.com/product/information-platforms-a-business-model-framework/.

[19] Blintsov, V.S. ta Maidaniuk, P.V. (2016). Kontseptsiia systemy zakhystu informatsii, shcho tsyrkuliuie na ob'iektakh morskoi infrastruktury. *Zbirnyk naukovykh prats NUK*. 1(463), 57–64. DOI 105589/отт20160109

[20] Gibson, J., Scherer, W., & Gibson, W. (2007). How to Do Systems Analysis (Wiley Series in Systems Engineering and Management). *Wiley-Interscience*. 1, 360 Pages. Retrieved from: https://www.amazon.com/How-Systems-Analysis-John-Gibson/dp/0470007656.

[21] *Rukovodstvo k Svodu znanyi po upravlenyiu proektamy (Rukovodstvo PMBOK®)*. Piatoe yzdanye, 1–17. Retrieved from: https://drm.pmi.org/Default.aspx?doc=PMBOKGuideFifthEd.pdf.

[22] *Bila Knyha – Transport*. (2011). Plan rozvytku yedynoho yevropeiskoho transportnoho prostoru na shliakhu do konkurentospromozhnoi ta resursoefektyvnoi transportnoi systemy. Vydavnychyi tsentr Yevropeiskoho Soiuzu v Liuksemburzi. Doi: 10.2832/30955. Retrieved from: https://brdo.com.ua/wp-content/uploads/2016/01/1_Bila-knyga-transport-plan-rozvytku-yedynogo-yevropey-skogo-transportnogo-prostoru-na-shlyahu-do-konkuretnospromozhnoi-ta-resursoefektyvnoi-.pdf.

[23] Babkin, H. V., Blintsov, V. S., Druzhynin, Ye. A., Kiiko, S. H., Knyrik, N. R., Koshkin, K. V., Krytskyi, D. M., Ryzhkov, S. S., & Slobodian S. O. (2017). *Upravlinnia uspishnymy proektamy stvorennia skladnoi tekhniky*. Monohrafiia. Mykolaiv : Torubary V. V., 336 .

[24] Zakharchenko, V.P., & Nenia, V.H. (2015). Systemne proektuvannia informatsiinoi modeli proektnoi operatsii yak elementa vyrobnychoho protsesu. *Skhidno-Ievropeiskyi zhurnal peredovykh tekhnolohii*. 1/3 (73), 53-56. DOI: Retrieved from: https://doi.org/10.15587/1729-4061.2015.37192.

[25] Kharytonov, Yu.N. (2008). Upravlenye proektamy rekonstruktsyy na osnove artefaktnыkh platform. *Avyatsyonno-kosmycheskaia tekhnyka y tekhnolohyy*. 8(55), 189–192.

[26] Moo-Hyun Kim. (2012). *Spar platforms. Technology and analysis methods*. The American Society of Civil Engineers, 240 Pages. Retrieved from: https://www.amazon.com/SPAR-Platforms-Technology-Analysis-Methods/dp/078441209X.

Постановка проблеми. Захист об'єктів морської критичної інфраструктури (МКІ) належить до головних завдань держави і має бути забезпечений у повному обсязі згідно з «Концепцією створення державної системи захисту критичної інфраструктури» [1]. До таких об'єктів передусім належить водний транспорт (Т), критично важливі акваторії (А) з підводними потенційно небезпечними об'єктами, водні транспортні шляхи (Ш), морські та річкові порти і перевантажувальні комплекси (П), морські стаціонарні платформи, підводні трубопроводи та інші стаціонарні споруди, які розташовані на морському шельфі (С), суднобудівні та судноремонтні заводи (З) та військово-морські бази (Б).

З позицій проектного менеджменту завдання побудови системи захисту для кожного виду з переліку вказаних об'єктів МКІ може бути класифіковане як базовий проект (БП), характерний для однотипних (базових) об'єктів МКІ (наприклад, БП «Захист порту», БП «Захист морської стаціонарної платформи» тощо).

Множина базових проектів утворює програму проектів, яку можна представити множиною $PP_{МКІ}$ потужністю L. Управління реалізацією кожного l-го базового проекту P_l ($l \varepsilon L$) є окремим прикладним завданням проектного менеджера, успішний розв'язок якого забезпечить безпеку визначеного переліку об'єктів МКІ держави.

Діяльність групи проектних менеджерів з розробки і реалізації такої програми має спиратись на ґрунтовну інформаційну базу, в якій сконцентровано як характеристики об'єктів захисту, так і відомості про імовірні загрози безпеці об'єктів МКІ, методи нейтралізації цих загроз та способи побудови системи захисту.

На цей час розробка такого інформаційного забезпечення для проектних менеджерів, які працюють у сфері морської індустрії та водного транспорту, знаходиться на стадії становлення. Тому розробка інформаційної платформи $IP_{МКІ}$ управління проектами захисту об'єктів МКІ як теоретичної основи створення інформаційного забезпечення для ефективного управління ними є актуальним прикладним науковим завданням, а її розробка сприятиме прискоренню процесів створення систем надійного захисту таких об'єктів.

У роботі розглядаються питання інформаційного забезпечення проектів захисту об'єктів МКІ від техногенних загроз зловмисного характеру – терористичних та кібератак [2]. Інші загрози, пов'язані з техногенними незловмисними (наприклад, аварії на транспорті), та загрози природного характеру (повені, шторми тощо) у роботі не розглядаються.

Аналіз останніх досліджень і публікацій. Зростаюча залежність економіки морських держав від стабільності функціонування об'єктів МКІ робить їх вразливими від терористичних нападів [3; 4]. Тому завдання створення систем захисту об'єктів МКІ від сучасних техногенних загроз зловмисного характеру постійно знаходиться у центрі уваги науковців. Так, у дослідженні [5] ґрунтовно аналізується стійкість об'єктів газо- і нафтовидобування до можливих атак терористичних суден. Обґрунтовується розширення зон безпеки навколо морських платформ на відстань від трьох до п'яти морських миль, що може суттєво підвищити здатність захищати офшорні платформи від найпоширеніших та доступних методів нападу, особливо з використання суден з вибухівкою.

У роботі [6] обговорюється міжнародне законодавство щодо встановлення зон безпеки навколо морських нафтогазових споруд на континентальному шельфі та дотримання вимог маршрутного судноплавства.

Однак зазначені дослідження стосуються розв'язку окремих складників завдання захисту об'єктів МКІ і не містять необхідних узагальнень для побудови комплексної системи їх захисту.

Більш повно питання організації управління процесами захисту об'єктів МКІ розглядаються у [7], де пропонується концепція об'єднаного управління безпекою таких об'єктів (Joint Harbor Operations Centers, JHOCs) на основі сил Берегової охорона та Військово-Морських Сил як складник морського антитерористичного захисту. Проте питання управління такими проектами автором не досліджуються.

План побудови морської інфраструктури для Національної стратегії морської безпеки США розглядається у [8]. План передбачає комплекс з восьми основних видів організаційних робіт захисту об'єктів МКІ, починаючи з заходів щодо поінформованості учасників проекту та організації захисту і закінчуючи заходами з відновлення об'єктів МКІ після терористичного нападу. Однак пропонований план має загальнодержавний формат і не передбачає розробку завдань інформаційного забезпечення такими проектами.

У документі [9] описано організацію та використання національних можливостей Великобританії для виявлення, оцінки та вирішення питань морської безпеки у власних та міжнародних водах. В основу стратегії безпеки покладено поєднання засобів технічного захисту та дипломатичної роботи, посиленням регіонального ті міжнародного співробітництва.

У роботі [10] обґрунтовується необхідність протистояння ризикам офшорно-енергетичного сектору Великобританії шляхом застосування дипломатичних, розвідувальних, військових та правоохоронних важелів.

Наведені вище дослідження стосуються побудови систем фізичного захисту об'єктів МКІ. Однак виклики сьогодення щодо інформаційного складника функціонування об'єктів МКІ стимулюють науковців на розробку завдань кібербезпеки для таких об'єктів. Це зумовлено активізацією діяльності хакерів на всіх напрямах – від кібертероризму до промислового шпигунства та операцій з викрадення енергоносіїв. Аналіз цього сегменту досліджень показує, що найбільш активно розробляються питання кібербезпеки окремих суден, портів та офшорних споруд – морських стаціонарних платформ, магістральних трубопроводів тощо.

Так, у роботі [11] аналізуються кіберризики, пов'язані з оцифруванням інформації та цифровізацією основних процесів управління судном, інтеграцією управління основними технологічними процесами на суднах та автоматизацією. У роботі надаються вказівки судновласникам та операторам морського транспорту щодо процедур та дій по забезпеченню безпеки кіберсистем у береговому офісі компанії та на борту судна. Проте питання інформаційного забезпечення для організації захисту від кібератак не досліджено.

Фундаментальне дослідження [12] присвячено дослідженню наявної ситуації з кібербезпекою критичних інформаційних інфраструктур комерційних портів та їх ланцюгів поставок. У монографії аналізуються сценарії загрози у морських ланцюгах поставок, уразливості та управління в системах портів, зацікавлені сторони у морській безпеці та рівень обізнаності операторів портів. Однак відомості про особливості створення інформаційних платформ управління проектами захисту об'єктів МКІ у монографії відсутні.

У роботі [13] розглядаються кіберризики для усього технологічного ланцюга добування вуглеводнів на шельфі – від проведення розвідки корисних копалин і до отримання продукції. При цьому реалізується триєдина задача захисту об'єкта МКІ – «безпека людей – надійність роботи – добування сировини». Але питання інформаційного забезпечення діяльності менеджерів з управління проектами безпеки у роботі не розглядаються.

Безпосередньо методологія створення інформаційної платформи об'єктів проектного менеджменту розроблялась авторами робіт [14; 15]. Однак предметна сфера цих досліджень стосувалась управління проектами, відповідно, розвитку портової інфраструктури та знешкодження підводних потенційно небезпечних об'єктів. Питання управління проектами захисту об'єктів МКІ в цих роботах не досліджувались.

Заслуговує на увагу також розробка [16], яка пропонує модель спеціальної інформаційної платформи водного середовища, архітектура якої є горизонтально розділеною на три розрізнені шари: графічний інтерфейс користувача, сервісний шар та рівень даних. Управління цими шарами забезпечується інструментальним шаром з розвиненим інтерфейсом користувача. Вказана робота, однак, не містить необхідних узагальнень, які б забезпечили створення інформаційної платформи управління проектами захисту об'єктів МКІ.

Відокремлення не вирішених раніше частин загальної проблеми. Сучасний етап розробки інформаційних платформ характеризується системним підходом, який ґрунтується на всебічному урахуванні особливостей функціонування всіх значущих складників об'єкту дослідження [17; 18]. Стосовно управління проектами захисту об'єктів МКІ це вимагає врахування місця і ролі цих об'єктів у житті держави та врахування взаємодії системи захисту об'єктів МКІ з регіональними, загальнодержавними та міжнародними інституціями. Крім того, до головних особливостей створення інформаційної платформи управління проектами захисту об'єктів МКІ належать необхідність управління процесами захисту як матеріальних, так і інформаційних ресурсів цих об'єктів. Актуальним на цей час є також управління роботою з кадрами, що залучені до функціонування об'єктів МКІ.

Важливими складниками створення інформаційної платформи управління проектами захисту об'єктів МКІ є також урахування всього комплексу робіт, пов'язаного з виявленням та формалізованим описом загроз таким об'єктам, методів протидії ним та технологіям побудови систем захисту від виявлених загроз [19].

Комплексне врахування зазначених особливостей побудови інформаційної платформи захисту об'єктів МКІ дасть змогу створити більш ефективний інструментарій для проектних менеджерів, які працюють у напряму морської галузі.

Мета дослідження. Метою дослідження є розробка моделі інформаційної платформи управління проектами захисту об'єктів морської критичної інфраструктури як теоретичної основи підвищення ефективності їх планування на ранніх стадіях розробки.

Для досягнення поставленої мети у роботі необхідно розв'язати такі задачі:

– сформувати структуру організацій – учасників інформаційного обміну у проектах захисту об'єктів МКІ;

– розробити структуру та основні складники інформаційної платформи управління проектами захисту об'єктів МКІ;

– розробити змістовну частину інформаційної платформи управління одним з базових проектів захисту об'єктів МКІ.

Методи, об'єкт та предмет дослідження. Розробку інформаційної платформи управління проектами захисту об'єктів МКІ виконано на підставі системного підходу [20], використання якого дає змогу встановити повний спектр інформаційних потреб для проектного менеджера (команди менеджерів) та синтезувати на їх основі ефективні рішення щодо управління процесами побудови системи захисту. Відповідно до предметного поля дослідження формування інформаційної платформи проектів захисту об'єктів МКІ синтезується у взаємозв'язку з основними складниками їх функціонування – матеріальними, енергетичними, інформаційними і кадровими. Обов'язковим є також урахування технологій, що використовуються для побудови систем захисту таких об'єктів.

В основу дослідження покладені термінологічні визначення теорії управління проектами, її основні принципи та положення [21].

Об'єктом дослідження є процеси управління створенням інформаційного забезпечення проектів захисту об'єктів МКІ. Такі проекти мають загальнодержавне значення та характеризуються широким спектром конкретних загроз та методів протистояння ним. Для управління такими проектами використовуються великі обсяги інформації технічного та організаційного характеру. Так, під час планування та виконання проектів захисту об'єктів МКІ створюється та використовується така інформація:

– про характеристики об'єктів захисту;

– про характеристики імовірних загроз об'єктам захисту;

– про характеристики методів та організаційно-технічних засобів протистояння цим загрозам;

– про характеристики технологій практичної побудови систем захисту об'єктів МКІ.

Одним з актуальних завдань управління проектами захисту об'єктів МКІ є побудова відсутнього на цей час єдиного науково обґрунтованого підходу до побудови інформаційного поля для таких проектів. Структуризація інформації, яка використовується у таких проектах, дасть змогу формалізувати процес управління інформаційним складником проектного менеджера та більш повно задовольнити інформаційні потреби всіх учасників проектів захисту об'єктів МКІ.

Основний матеріал. Створення інформаційної платформи для управління програмою проектів захисту об'єктів МКІ $PP_{МКІ}$ є складним прикладним науковим завданням системного характеру, яке має забезпечити задоволення інформаційних потреб широкого кола учасників проектів. Враховуючи міжнародний та загальнодержавний характер цих проектів, можна сформувати наступний перелік організацій, зацікавлених в отриманні такої інформації (рис. 1):

– орган державної влади, відповідальний за формування та реалізацію державної політики у сфері захисту критичної інфраструктури держави загалом і морської її частини зокрема; наразі такий орган в Україні знаходиться на стадії формування [1];

– міжнародні морські організації, з якими має співпрацювати держава як учасник низки міжнародних угод з безпеки мореплавства [22];

– регіональні органи державного нагляду та контролю за станом захищеності об'єктів МКІ; до них належать управління Державної прикордонної служби України (ДПС), Державної служби з надзвичайних ситуацій України (ДСНС), антитерористичні центри Служби безпеки України (СБУ), які розробляють і затверджують регіональні програми протидії загрозам критичній інфраструктурі, а також

проводять перевірки об'єктів критичної інфраструктури і визначають рівні об'єктової та інформаційної безпеки (зокрема, кібербезпеки) на об'єктах МКІ, ведуть облік паспортів безпеки об'єктів МКІ та карт ризику адміністративно-територіальних одиниць;

– галузеві органи забезпечення безпеки об'єктів МКІ, які розробляють плани захисту підпорядкованих їм об'єктів: структурні підрозділи Мінінфраструктури (Державна інспекція України з безпеки на морському та річковому транспорті, Адміністрація морських портів України), Міністерства енергетики та захисту довкілля України (Державна екологічна інспекція України), які виконують збір, аналіз та узагальнення даних щодо стану безпеки об'єктів МКІ та їх функціонування за напрямами;

– органи місцевого самоврядування (територіальні громади), які зацікавлені в безпечній експлуатації об'єктів МКІ та охороні навколишнього середовища; до їх повноважень належить розроблення, затвердження і виконання місцевих програм забезпечення захисту та стійкості об'єктів МКІ, розроблення та погодження місцевих планів взаємодії суб'єктів системи захисту об'єктів критичної інфраструктури, планів відновлення функціонування цих об'єктів після ліквідації кризової ситуації;

– органи об'єктового рівня захисту об'єктів МКІ – служби безпеки нижнього рівня, які складають плани та виконують конкретні заходи щодо захисту конкретних об'єктів.

Крім того, до учасників таких проектів, зацікавлених в отриманні інформації про стан захищеності об'єктів МКІ, слід віднести:

– засоби масової інформації (у разі, коли така інформація не має грифу обмеження доступу);

– науково-дослідні установи, які залучаються до розробки нових технологій захисту, створення нових видів програмно-технічного та організаційного забезпечення захисту об'єктів МКІ;

– підприємства-виробники та постачальники нової техніки та технологій захисту об'єктів МКІ.

Під час формування інформаційної платформи *IP*-захисту об'єктів МКІ доцільно застосовувати методологію системного аналізу, метод декомпозиції та теорію множин. Згідно з цим структуру інформаційної платформи будемо розглядати як систему, до складу якої входять інформаційні модулі, що містять інформаційні характеристики основних системоутворюючих складників об'єкту захисту. До таких характеристик віднесемо фізичні характеристики об'єкта захисту (О), характеристики енергопостачання (Е) та інформаційні характеристики (І) об'єкта захисту та характеристики кадрів (К) – обслуговуючого персоналу, задіяного в експлуатації об'єктів МКІ.

Досвід Національного університету кораблебудування імені адмірала Макарова (НУК) [23] та успішні практики розробки інформаційних моделей виробничих процесів [24] дають змогу представити інформаційну платформу $IP_{\text{МКІ}l}$ управління l-м базовим проектом ($P_l \subset PP_{\text{МКІ}}$) у складі модулів:

– інформаційного модуля $IM_{\text{Х}l}$ типових характеристик l-го базового об'єкта захисту у формі множини інформаційних моделей основних характеристик об'єкту МКІ – фізичних $I_{\text{ХО}l}$, енергетичних $I_{\text{ХЕ}l}$, інформаційних $I_{\text{ХІ}l}$ та кадрових $I_{\text{ХК}l}$ його характеристик;

– інформаційного модуля $IM_{\text{В}l}$ характеристик типових загроз основним складовим l-го базового об'єкта захисту у формі множини інформаційних моделей загроз основним фізичним $I_{\text{ВО}l}$, енергетичним $I_{\text{ВЕ}l}$, інформаційним $I_{\text{ВІ}l}$ та кадровим $I_{\text{ВК}l}$ складникам його функціонування;

– інформаційного модуля $IM_{\text{Тз}l}$ характеристик наявних типових методів та організаційно-технічних засобів протистояння цим загрозам для l-го базового об'єкта захисту у формі множини інформаційних моделей $I_{\text{ТзО}l}$, $I_{\text{ТзВ}l}$, $I_{\text{ТзІ}l}$, $I_{\text{ТзК}l}$, які належать, відповідно, до захисту фізичних, енергетичних, інформаційних і кадрових його складників;

– інформаційного модуля $IM_{\text{Пр}l}$ характеристик типових технологій $I_{\text{Пр}l}$ практичної побудови систем

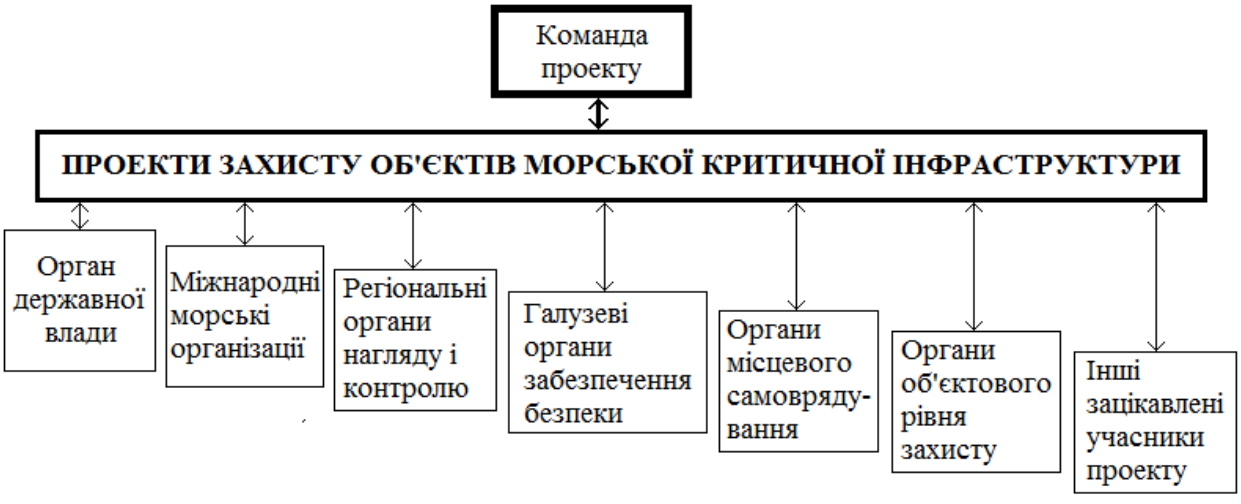

Рис. 1. Структура організацій – учасників інформаційного обміну у проектах захисту об'єктів МКІ

захисту *l*-го базового об'єкта МКІ від зазначених видів загроз у формі множини інформаційних моделей $I_{ПрОl}$, $I_{ПрВl}$, $I_{ПрIl}$, $I_{ПрКl}$, які належать, відповідно, до захисту від загроз несанкціонованого фізичного проникнення на об'єкт, систем захисту енергетичного, інформаційного та кадрового складників функціонування *l*-го базового об'єкта захисту.

Зазначимо, що в багатьох практичних випадках наведені вище множини інформаційних моделей за необхідністю можуть бути розширені шляхом уведення додаткових інформаційних моделей. Наприклад, для інформаційного модуля IM_{Xl} – шляхом включення моделей екологічної безпеки тощо, для інформаційного модуля IM_{Bl} – шляхом включення моделей загроз незловмисного характеру тощо.

Головні складники інформаційної платформи $IP_{МКІl}$ проекту захисту *l*-го об'єкта наведені на рис. 2.

На рис. 2 показано також обов'язкове використання бази даних артефактних проектів захисту об'єктів МКІ, оскільки вони забезпечують економію ресурсів проектів (у першу чергу, ресурсів часу та фінансів) [25]. Структурно вказана база даних може бути організована у вигляді типових (стандартизованих чи рекомендованих практикою) четвірок кортежів (упорядкованих наборів інформації), кожна з яких складається з конкретної характеристики типового об'єкта МКІ, що підлягає захисту, найбільш імовірних загроз та методів протистояння ним, а також з найбільш ефективних технологій побудови системи захисту від них.

Наведена на рис. 2 структура інформаційної платформи проектів захисту об'єктів МКІ слугує основою для створення аналітичного інструментарію, за допомогою якого можна автоматизувати процес формування шаблонів менеджерами проектів. Для цього до структури інформаційної платформи уведено блок «Автоматизована система формування шаблонів проектного менеджера».

Розглянемо створення такого інструментарію більш детально.

Запишемо змістовну частину інформаційних модулів IM_{Xl}, IM_{Bl}, $IM_{Tзl}$ та $IM_{Прl}$ у вигляді наступних множин:

$$IM_{Xl}=\{I_{XOl}, I_{XEl}, I_{XIl}, I_{XKl}\}; \quad (1)$$

$$IM_{Bl}=\{I_{BOl}, I_{BEl}, I_{BIl}, I_{BKl}\}; \quad (2)$$

$$IM_{Tзl}=\{I_{TзOl}, I_{TзEl}, I_{TзIl}, I_{TзKl}\}; \quad (3)$$

$$IM_{Прl}=\{I_{ПрOl}, I_{ПрEl}, I_{ПрIl}, I_{ПрKl}\}. \quad (4)$$

Декартів добуток *D* будь-якої пари множин (1)–(4) дає кортеж (впорядкований набір) усіх можливих

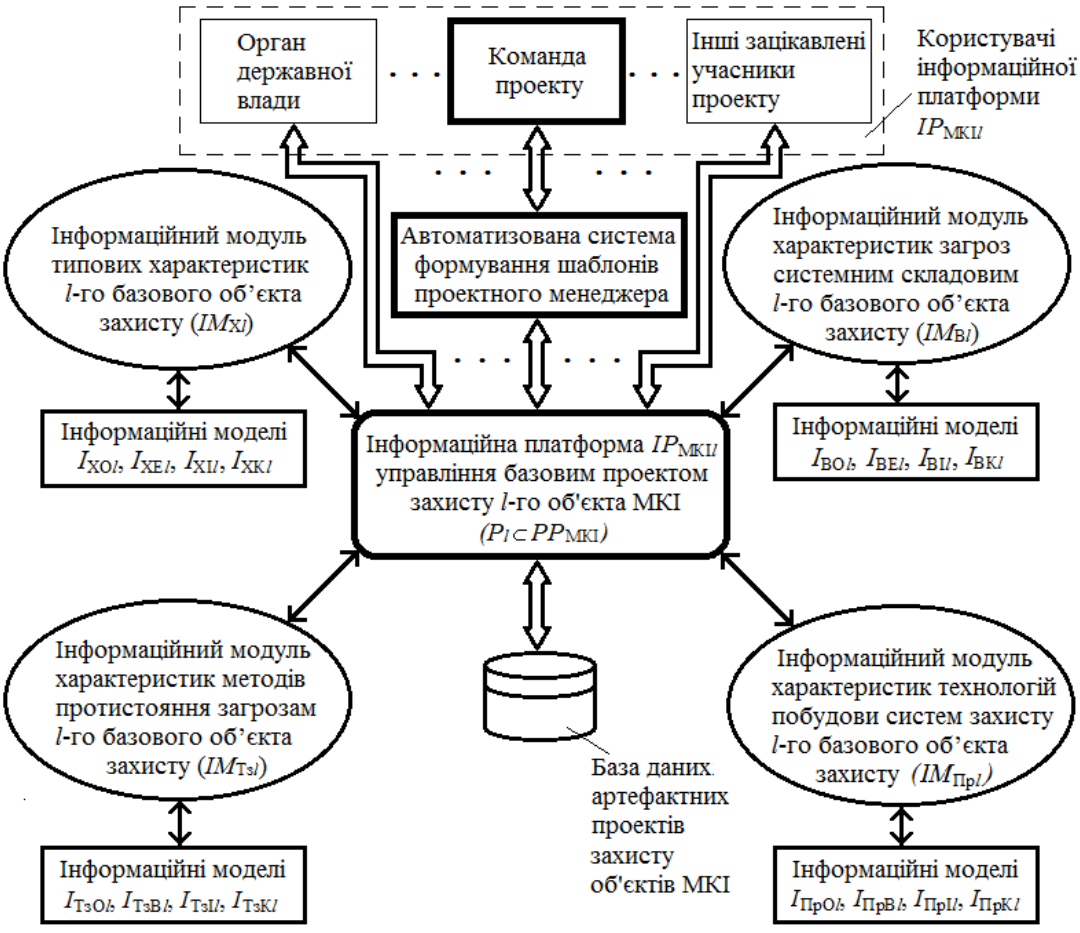

Рис. 2. Основні складники інформаційної платформи проекту захисту l-го базового об'єкта МКІ

пар інформаційних моделей I, у яких перша інформаційна модель належить першій множині, а друга – другій множині добутку. Для проектного менеджера фізичний смисл мають елементи головної діагоналі M_D добутку D, які містять пари інформаційних моделей I, що характеризують інформаційні характеристики основних системоутворюючих складників об'єкту захисту – фізичні характеристики об'єкта захисту (О), енергетичні (Е) та інформаційні (І) характеристики об'єкта захисту та характеристики – обслуговуючого персоналу (К), задіяного в експлуатації об'єктів МКІ.

Таким чином, менеджер проекту захисту l-го базового об'єкта МКІ має змогу на основі множин (1)–(4) формувати в автоматизованому режимі кортеж необхідних йому інформаційних моделей (головну діагональ M_D декартового добутку D) та ефективно управляти процесом розробки системи захисту цього об'єкта. Наприклад, головна діагональ декартового добутку множин (1) і (2) $M_{D\text{ХВ}l}$ має упорядковані пари інформаційних моделей, які описують типові характеристики l-го базового об'єкта захисту та характеристики типових загроз основним його складникам:

$$M_{D\text{ХВ}l}=M_D(IM_{\text{Х}l}\times IM_{\text{В}l})=\begin{array}{|c|c|c|c|}\hline I_{\text{ХО}l},\ I_{\text{ВО}l} & & & \\ \hline & I_{\text{ХЕ}l},\ I_{\text{ВЕ}l} & & \\ \hline & & I_{\text{ХІ}l},\ I_{\text{ВІ}l} & \\ \hline & & & I_{\text{ХК}l},\ I_{\text{ВК}l} \\ \hline\end{array}. \quad (5)$$

Множина інформаційних моделей (5) містить вичерпну інформацію для проектного аналізу можливих загроз l-му базовому об'єкту МКІ як об'єкту захисту. Вона дає змогу менеджеру проекту обґрунтовано планувати заходи протидії виявленим загрозам і заходи практичної реалізації системи захисту.

Так, головна діагональ декартового добутку множин (3) і (4) $M_{D\text{ТзПр}l}$ має упорядковані пари інформаційних моделей, які описують типові характеристики наявних типових методів та організаційно-технічних засобів протистояння цим загрозам та характеристики типових технологій практичної побудови систем від зазначених видів загроз для l-го базового об'єкта захисту:

$$M_{D\text{ТзПр}l}=M_D(IM_{\text{Тз}l}\times IM_{\text{Пр}l})=\begin{array}{|c|c|c|c|}\hline I_{\text{ТзО}l},\ I_{\text{ПрО}l} & & & \\ \hline & I_{\text{ТзЕ}l},\ I_{\text{ПрЕ}l} & & \\ \hline & & I_{\text{ТзІ}l},\ I_{\text{ПрІ}l} & \\ \hline & & & I_{\text{ТзК}l},\ I_{\text{ПрК}l} \\ \hline\end{array}. \quad (6)$$

Зазначимо, що множини (5) і (6) можуть мати більшу розмірність, яка залежить від кількості n прийнятих до розгляду основних системоутворюючих складників об'єкту захисту, однак розмір декартового добутку завжди буде ($n\times n$).

Розглянемо тепер зміст і особливості побудови власне інформаційних моделей $I_{\text{Х}}$, $I_{\text{В}}$, $I_{\text{Тз}}$, $I_{\text{Пр}}$ як складників інформаційних моделей модулів $IM_{\text{Х}}$, $IM_{\text{В}}$, $IM_{\text{Тз}}$ та $IM_{\text{Пр}}$. У якості базового об'єкта захисту визначимо морську стаціонарну платформу (МСП) – автономну морську інженерну споруду, встановлену у відкритому морі на якорях чи на палях і призначену для видобутку вуглеводнів [26].

Виходячи з системного підходу для базового проекту «Захист морської стаціонарної платформи», сформуємо такі чотири групи інформаційних моделей типових характеристик МСП згідно з (1): групу інформаційних моделей фізичних характеристик самої МСП ХО-*МСП-Пл* та прилеглої до неї акваторії ХО-*МСП-А*; групу інформаційних моделей ХЕ-*МСП* характеристик системи енергозабезпечення МСП; групу інформаційних моделей ХІ-*МСП* комунікаційних характеристик МСП; групу інформаційних моделей ХК-*МСП* характеристик обслуговуючого персоналу, задіяного в експлуатації об'єктів МСП.

Першу групу інформаційних моделей доцільно представити наступними множинами:

$$I_{\text{ХО-}МСП\text{-}Пл}=\{I_{\text{ХО-}МСП\text{-}ПлП},\ I_{\text{ХО-}МСП\text{-}ПлН},\ I_{\text{ХО-}МСП\text{-}ПлВ}\}; \quad (7)$$

$$I_{\text{ХО-}МСП\text{-}А}=\{I_{\text{ХО-}МСП\text{-}АД},\ I_{\text{ХО-}МСП\text{-}АС},\ I_{\text{ХО-}МСП\text{-}АБ}\}, \quad (8)$$

де індекси «$_{МСП\text{-}ПлП}$»,«$_{МСП\text{-}ПлН}$»,«$_{МСП\text{-}ПлВ}$» – відповідно, це індекси інформаційних моделей підводної і надводної частин МСП як об'єктів охорони та верхньої будівлі МСП, де розташоване інженерне обладнання МСП та житлові блоки; індекси «$_{МСП\text{-}АД}$», «$_{МСП\text{-}АС}$», «$_{МСП\text{-}АБ}$» – це індекси інформаційних моделей, відповідно, дальньої, середньої і ближньої зон акваторії як об'єктів охорони.

Друга група інформаційних моделей ХЕ-*МСП* містить характеристики системи енергозабезпечення МСП як об'єкта захисту, яка складається з підсистем електро- (ЕП), водо- (ВП) та теплопостачання (ТП), тому її доцільно представити наступною множиною (індекси множин відповідають позначенням підсистем):

$$I_{\text{ХЕ-}МСП}=\{I_{\text{ХЕ-}МСП\text{-}ЕП},\ I_{\text{ХЕ-}МСП\text{-}ВП},\ I_{\text{ХЕ-}МСП\text{-}ТП}\}. \quad (9)$$

Третя група інформаційних моделей ХІ-*МСП* містить характеристики інформаційного складника функціонування МСП – підсистем зовнішнього (ЗЗ) і внутрішнього (ВЗ) зв'язку, сигналізації (С) та обробки інформації (ОІ), яка циркулює на МСП. Окрему задачу виконує підсистема технічного захисту інформації (ЗІ), яка забезпечує захист інформації від несанкціонованого доступу, викривлення чи знищення.

Множину інформаційних моделей третьої групи ХІ-*МСП* можна представити таким чином:

$$I_{\text{ХІ}МСП}=\{I_{\text{ХІ-}МСП\text{-}ЗЗ},\ I_{\text{ХІ-}МСП\text{-}ВЗ},\ I_{\text{ХІ-}МСП\text{-}С},\ I_{\text{ХІ-}МСП\text{-}ОР},\ I_{\text{ХІ-}МСП\text{-}ЗІ}\}. \quad (10)$$

Четверта група інформаційних моделей ХК-*МСП* містить характеристики обслуговуючого персоналу, задіяного в експлуатації об'єктів морської стаціонарної платформи. Укрупнені кадри, які обслуговують МСП, можна представити трьома основними групами – співробітниками, які забезпечують функціонування берегових служб МСП (БС),

співробітниками вахтових бригад (ВБ), які працюють на МСП вахтовим методом, та екіпажі надводних (судно) і повітряних (гелікоптери) транспортних засобів, які виконують перевезення вахтових бригад і матеріально-технічне забезпечення МСП (ТС).

Тоді множину інформаційних моделей четвертої групи ХК-*МСП* можна представити таким чином:

$$I_{\text{ХК-МСП}}=\{I_{\text{ХК-МСП-БС}}, I_{\text{ХК-МСП-ВБ}}, I_{\text{ХК-МСП-ТС}}\}. \quad (11)$$

Синтез конкретних інформаційних моделей множин (7)–(11) є окремою прикладною науковою задачею. Тут як приклад розглянемо лише деякі складники.

Попередній аналіз свідчить, що до найбільш небезпечних загроз для об'єктів МКІ є загрози з-під води, оскільки вони, по-перше, характеризуються значними складнощами своєчасного виявлення і, по-друге, вимагають застосування складних організаційно-технічних засобів для протистояння ним. Тому надалі як приклади розробки інформаційних моделей будемо синтезувати моделі для підводної частини МСП та її акваторії.

Так, для інформаційних моделей $I_{\text{ХО-МСП-ПлП}}$ та $I_{\text{ХО-МСП-ПлН}}$ підводної і надводної частин конструкції МСП можна вказати на наступні обов'язкові характеристики:

$$I_{\text{ХО-МСП-ПлП}}=ГПХ_{ПлП}\cup К_{ПлП}\cup АКЗ_{ПлП}\cup ДП_{ПлП}\cup ДА_{ПлП}\cup ЗЗ_{ПлП}\cup ВС; \quad (12)$$

$$I_{\text{ХО-МСП-ПлН}}=ГПХ_{ПлН}\cup К_{ПлН}\cup АКЗ_{ПлН}\cup ПС_{ПлН}\cup ПО_{ПлН}\cup ПС, \quad (13),$$

де $ГПХ_{ПлП}$, $ГПХ_{ПлН}$ – географічні та просторові характеристики, відповідно, підводної і надводної частин МСП; $К_{ПлП}$, $К_{ПлН}$, $АКЗ_{ПлП}$, $АКЗ_{ПлН}$, – відповідно, конструктивні та корозійні характеристики підводної і надводної частин МСП; $ДП_{ПлП}$ – характеристики рельєфу та гідрології морського дна; $ДА_{ПлП}$ – конструктивні та експлуатаційні характеристики донної (свердловинної) апаратури МСП; $ЗЗ_{ПлП}$, $ВС$ – фізико-хімічні характеристики, відповідно, зони змінного змочування конструкції МСП та водного середовища, в якому знаходиться конструкція МСП; $ПС_{ПлН}$, $ПО_{ПлН}$ – відповідно, конструктивні та експлуатаційні характеристики причальних споруд та палубного обладнання МСП; $ПС$ – гідрометеорологічні характеристики повітряного середовища в районі установки МСП.

Інформаційні моделі $I_{\text{ХО-МСП-АД}}$, $I_{\text{ХО-МСП-АС}}$, $I_{\text{ХО-МСП-АБ}}$ акваторії МСП можна представити множинами таких основних характеристик:

$$I_{\text{ХО-МСП-АД}}=ГПХ_{МСП-АД}\cup ГЛХ_{МСП-АД}\cup ГФХ_{МСП-АД}\cup ГХХ_{МСП-АД}\cup ГАХ_{МСП-АД}\cup ГПХ_{МСП-АД}; \quad (14)$$

$$I_{\text{ХО-МСП-АС}}=ГПХ_{МСП-АС}\cup ГЛХ_{МСП-АС}\cup ГФХ_{МСП-АС}\cup ГХХ_{МСП-АС}\cup ГАХ_{МСП-АС}\cup ГПХ_{МСП-АС}; \quad (15)$$

$$I_{\text{ХО-МСП-АБ}}=ГПХ_{МСП-АБ}\cup ГЛХ_{МСП-АБ}\cup ГФХ_{МСП-АБ}\cup ГХХ_{МСП-АБ}\cup ГАХ_{МСП-АБ}\cup ГПХ_{МСП-АБ}, \quad (16)$$

де $ГПХ_{МСП-АД}$, $ГПХ_{МСП-АС}$, $ГПХ_{МСП-АБ}$ – географічні та просторові характеристики, відповідно, дальньої, середньої і ближньої зон акваторії МСП як об'єктів охорони; *ГЛХ*, *ГФХ*, *ГХХ*, *ГАХ*, *ММХ* – відповідно, гідрологічні, гідро фізичні, гідрохімічні, гідроакустичні та магнітометричні характеристики відповідних акваторій МСП; індекси «$_{МСП-АД}$», «$_{МСП-АС}$», «$_{МСП-АБ}$» вказують на приналежність інформаційних моделей, відповідно, дальньої, середньої і ближньої зон акваторії МСП як об'єктів охорони.

Сформуємо тепер для базового проекту «Захист морської стаціонарної платформи» такі чотири групи інформаційних моделей типових загроз основним складникам МСП згідно з (2): групу інформаційних моделей загроз основним фізичним складникам власне морської стаціонарної платформи ВО-*МСП-Пл* та прилеглої до неї акваторії ВО-*МСП-А* (загроз несанкціонованого проникнення на вказані об'єкти); групу інформаційних моделей ВЕ-*МСП* загроз для функціонування системи енергозабезпечення МСП; групу інформаційних моделей ВІ-*МСП* загроз для комунікаційних характеристик МСП; групу інформаційних моделей ВК-*МСП* загроз з боку обслуговуючого персоналу, задіяного в експлуатації об'єктів МСП.

Першу групу інформаційних моделей загроз доцільно представити наступними множинами:

$$I_{\text{ВО-МСП-Пл}}=\{I_{\text{ВО-МСП-ПлП}}, I_{\text{ВО-МСП-ПлН}}, I_{\text{ВО-МСП-ПлВ}}\}; \quad (17)$$

$$I_{\text{ВО-МСП-А}}=\{I_{\text{ВО-МСП-АД}}, I_{\text{ВО-МСП-АС}}, I_{\text{ВО-МСП-АБ}}\}, \quad (18)$$

де індекси «$_{МСП-ПлП}$»,«$_{МСП-ПлН}$»,«$_{МСП-ПлВ}$» – відповідно, це індекси інформаційних моделей загроз підводній і надводній частинам МСП, верхній будівлі МСП як об'єктам захисту від несанкціонованого доступу; індекси «$_{МСП-АД}$», «$_{МСП-АС}$», «$_{МСП-АБ}$» – це індекси інформаційних моделей загроз несанкціонованого проникнення, відповідно, на дальню, середню і ближню зони акваторії як об'єктів охорони.

Друга група інформаційних моделей ВЕ-*МСП* загроз має характеризувати загрози функціонуванню системи енергозабезпечення МСП і в загальному випадку може бути представлена такою множиною:

$$I_{\text{ВЕ-МСП-Пл}}=\{I_{\text{ВЕ-МСП-ЕП}}, I_{\text{ВЕ-МСП-ВП}}, I_{\text{ВЕ-МСП-ТП}}\}, \quad (19)$$

де індекси «$_{МСП-ЕП}$», «$_{МСП-ВП}$» і «$_{МСП-ТП}$» належать до характеристик загроз, відповідно, підсистем електро-, водо- та теплопостачання МСП.

Третя група інформаційних моделей ВІ-*МСП* загроз для комунікаційних характеристик МСП може бути описана такою множиною моделей:

$$I_{\text{ВІМСП}}=\{I_{\text{ВІ-МСП-ЗЗ}}, I_{\text{ВІ-МСП-ВЗ}}, I_{\text{ВІ-МСП-С}}, I_{\text{ВІ-МСП-ОІ}}\}, \quad (20)$$

де індекси «$_{МСП\text{-}ЗЗ}$», «$_{МСП\text{-}ВЗ}$», «$_{МСП\text{-}С}$» та «$_{МСП\text{-}ОІ}$» належать до характеристик загроз, відповідно, підсистемам зовнішнього і внутрішнього зв'язку, сигналізації та обробки інформації, яка циркулює на МСП. В окремих випадках доцільним є уведення у розгляд інформаційної моделі загроз підсистемі технічного захисту інформації, яка розгорнута на МСП.

Нарешті, четверту групу інформаційних моделей ВК-*МСП*, які характеризують загрози з боку обслуговуючого персоналу МСП, можна представити наступною множиною:

$$I_{ВК\text{-}МСП}=\{I_{ВК\text{-}МСП\text{-}БС}, I_{ВК\text{-}МСП\text{-}ВВ}, I_{ВК\text{-}МСП\text{-}ТС}\}, \quad (21)$$

де індекси «$_{МСП\text{-}БС}$», «$_{МСП\text{-}ВВ}$» і «$_{МСП\text{-}ТС}$» належать до груп співробітників, відповідно, берегових служб МСП, вахтових бригад МСП та екіпажів транспортних засобів, які можуть утворювати загрози функціонуванню МСП через несумлінність, нелояльність чи злочинні наміри.

Як приклад, для інформаційних моделей загроз $I_{ВО\text{-}МСП\text{-}ПлП}$ та $I_{ВО\text{-}МСП\text{-}А}$ можна вказати на наступні основні характеристики загроз:

$$I_{ВО\text{-}МСП\text{-}ПлП}=ЦК_{ПлП} \cup СП_{ПлП} \cup ПЗ_{ПлП} \cup МО_{ПлП}; \quad (22)$$

$$I_{ВО\text{-}МСП\text{-}АД}=I_{ВО\text{-}МСП\text{-}АС}=I_{ВО\text{-}МСП\text{-}АБ}=ПТ_{МСП\text{-}А} \cup АПА_{МСП\text{-}А} \cup ТПА_{МСП\text{-}А} \cup$$

$$ДПА_{МСП\text{-}А} \cup ПДО_{МСП\text{-}А} \cup СТП_{МСП\text{-}А}, \quad (23)$$

де $ЦК_{ПлП}$, $СП_{ПлП}$, $ПЗ_{ПлП}$, $МО_{ПлП}$ – відповідно, показники конструктивної цілісності підводної частини платформи, наявності сторонніх предметів на її конструкції, стану елементів її протекторного захисту та ступеню обростання морськими організмами та водоростями; $ПТ_{МСП\text{-}А}$, $АПА_{МСП\text{-}А}$, $ТПА_{МСП\text{-}А}$, $ДПА_{МСП\text{-}А}$, $ПДО_{МСП\text{-}А}$, $СТП_{МСП\text{-}А}$ – інформаційні моделі порушників підводної охоронної зони МСП, відповідно, підводного терориста, автономного, телекерованого та донного підводних апаратів, підводного дрейфуючого об'єкта та морської тварини (дельфіна, тюленя тощо).

Зазначимо, що у (23) загрози несанкціонованого проникнення, у загальному випадку, є однаковими для усіх трьох зон акваторії як об'єкта охорони і відрізняються лише методами боротьби з ними.

Сформуємо тепер для базового проекту «Захист морської стаціонарної платформи» такі чотири групи інформаційних моделей типових методів та організаційно-технічних засобів протистояння цим загрозам згідно (3): групу інформаційних моделей ТзО-*МСП-Пл* і ТзО-*МСП-А* типових методів та організаційно-технічних засобів протистояння загрозам несанкціонованого проникнення, відповідно, на платформу чи на контрольовану акваторію навколо неї; групу інформаційних моделей ТзЕ-*МСП* типових методів та організаційно-технічних засобів протистояння загрозам нормальному функціонуванню системи енергозабезпечення МСП; групу інформаційних моделей ТзІ-*МСП* типових методів та організаційно-технічних засобів захисту системи інформаційних комунікацій МСП; групу інформаційних моделей ТзК-*МСП* типових методів та організаційно-технічних засобів протистояння можливим зловмисникам з числа персоналу МСП.

Так, для першої групи можна сформувати наступні множини інформаційних моделей:

$$I_{ТзО\text{-}МСП\text{-}Пл}=\{I_{ТзО\text{-}МСП\text{-}ПлП}, I_{ТзО\text{-}МСП\text{-}ПлН}, I_{ТзО\text{-}МСП\text{-}ПлВ}\}; \quad (24)$$

$$I_{ТзО\text{-}МСП\text{-}А}=\{I_{ТзО\text{-}МСП\text{-}АД}, I_{ТзО\text{-}МСП\text{-}АС}, I_{ТзО\text{-}МСП\text{-}АБ}\}, \quad (25)$$

де індекси «$_{МСП\text{-}ПлП}$»,«$_{МСП\text{-}ПлН}$»,«$_{МСП\text{-}ПлВ}$», «$_{МСП\text{-}АД}$», «$_{МСП\text{-}АС}$», «$_{МСП\text{-}АБ}$» – відповідно, це індекси інформаційних моделей типових методів та організаційно-технічних засобів протистояння загрозам несанкціонованого проникнення на платформу та на контрольовану акваторію навколо неї.

Для другої групи інформаційних моделей ТзЕ-*МСП* можна сформувати наступну множину інформаційних моделей:

$$I_{ТзЕ\text{-}МСП\text{-}Пл}=\{I_{ТзЕ\text{-}МСП\text{-}ЕП}, I_{ТзЕ\text{-}МСП\text{-}ВП}, I_{ТзЕ\text{-}МСП\text{-}ТП}\}, \quad (26)$$

де індекси «$_{МСП\text{-}ЕП}$», «$_{МСП\text{-}ВП}$» і «$_{МСП\text{-}ТП}$» належать до характеристик типових методів та організаційно-технічних засобів протистояння загрозам нормального енергозабезпечення, відповідно, підсистем електро-, водо- та теплопостачання МСП.

Для третьої групи інформаційних моделей ТзІ-*МСП* типових методів та організаційно-технічних засобів захисту системи інформаційних комунікацій МСП доцільним є формування такої множини:

$$I_{ТзІ МСП}=\{I_{ТзІ\text{-}МСП\text{-}ЗЗ}, I_{ТзІ\text{-}МСП\text{-}ВЗ}, I_{ТзІ\text{-}МСП\text{-}С}, I_{ТзІ\text{-}МСП\text{-}ОІ}\}, \quad (27)$$

де індекси «$_{МСП\text{-}ЗЗ}$», «$_{МСП\text{-}ВЗ}$», «$_{МСП\text{-}С}$» та «$_{МСП\text{-}ОІ}$» належать до характеристик інформаційних моделей типових методів та організаційно-технічних засобів захисту системи інформаційних комунікацій МСП – підсистем зовнішнього і внутрішнього зв'язку, сигналізації та обробки інформації, яка циркулює на МСП.

Для четвертої групи інформаційних моделей ТзК-*МСП* типових методів та організаційно-технічних засобів протистояння можливим зловмисникам з числа персоналу, який експлуатує МСП:

$$I_{ТзК\text{-}МСП}=\{I_{ТзК\text{-}МСП\text{-}БС}, I_{ТзК\text{-}МСП\text{-}ВВ}, I_{ТзК\text{-}МСП\text{-}ТС}\}, \quad (28)$$

де індекси «$_{МСП\text{-}БС}$», «$_{МСП\text{-}ВВ}$» і «$_{МСП\text{-}ТС}$» належать до методів та організаційно-технічних засобів, які передбачають профілактичну та інспекційну роботу з групами співробітників, відповідно, берегових служб МСП, вахтових бригад МСП та екіпажів транспортних засобів, які можуть утворювати загрози її функціонуванню через несумлінність, нелояльність чи злочинні наміри.

Як приклад для інформаційних моделей типових методів протистояння загрозам несанкціонованого проникнення на платформу $I_{\text{ПрО-}МСП\text{-}Пл}$ та на контрольовану акваторію навколо неї $I_{\text{ТзО-}МСП\text{-}А}$ вкажемо на основні характеристики цих методів:

$$I_{\text{ТзО-}МСП\text{-}Пл}=КПП_{МСП\text{-}Пл} \cup ВСД_{МСП\text{-}Пл} \cup САС_{МСП\text{-}Пл}; \quad (29)$$

$$I_{\text{ТзО-}МСП\text{-}АД}=I_{\text{ТзО-}МСП\text{-}АС}=I_{\text{ТзО-}МСП\text{-}АБ}=ПГАС_{МСП\text{-}А} \cup АГАС_{МСП\text{-}А} \cup ССВП_{МСП\text{-}А} \cup МСПП_{МСП\text{-}А} \cup СПЗС_{МСП\text{-}А} \cup СТЗ_{МСП\text{-}А} \cup СФПП_{МСП\text{-}А}, \quad (30)$$

де $КПП_{МСП\text{-}Пл}$ – інформаційна модель обладнання контрольно-пропускного пункту на МСП (турнікетів з електронною ідентифікацією, металодетекторів тощо); $ВСД_{МСП\text{-}Пл}$ – інформаційна модель обладнання систем охоронного відеоспостереження на документування МСП; $САС_{МСП\text{-}Пл}$ – інформаційна модель обладнання систем аварійної сигналізації МСП; $ПГАС_{МСП\text{-}А}$ – інформаційні моделі пасивних гідроакустичних систем виявлення порушників (гідрофонних систем); $АГАС_{МСП\text{-}А}$ – інформаційні моделі активних гідроакустичних систем виявлення порушників (сонарів секторного і кругового огляду); $ССВП_{МСП\text{-}А}$ – інформаційні моделі сейсмічних систем виявлення порушників; $МСПП_{МСП\text{-}А}$ – інформаційні моделі мобільних систем виявлення порушників (автономних та телекерованих підводних апаратів-роботів); $СПЗС_{МСП\text{-}А}$ – інформаційні моделі систем підводного загородження і сигналізації (електрифікованих підводних сіток, донних магнітометричних систем тощо); $СТЗ_{МСП\text{-}А}$ – інформаційні моделі службових тварин-захисників акваторій; $СФПП_{МСП\text{-}А}$ – інформаційні моделі систем фізичної протидії порушнику (попередження та нелетальної протидії).

Інформаційні моделі (30) зазвичай є однотипними для дальньої, середньої та ближньої зон захищених акваторій і відрізняються лише технічними характеристиками задіяного обладнання.

Нарешті сформуємо для базового проекту «Захист морської стаціонарної платформи» такі чотири групи інформаційних моделей типових технологій практичної побудови систем захисту від виявлених загроз згідно з (4): групу інформаційних моделей ПрО-*МСП-Пл* і ПрО-*МСП-А,* що описують типові технології практичної побудови систем захисту, відповідно, МСП і її акваторії як фізичних об'єктів захисту від зазначених видів загроз; групу інформаційних моделей ПрЕ-*МСП,* які характеризують типові технології побудови систем захисту для системи енергозабезпечення МСП; групу інформаційних моделей ПрІ-*МСП,* які характеризують типові технології практичної побудови систем захисту для системи інформаційних комунікацій МСП; групу інформаційних моделей ПрК-*МСП,* які характеризують типові технології практичної побудови систем захисту від дій зловмисників з числа персоналу, який експлуатує МСП.

Так, для першої групи моделей ПрО-*МСП-Пл* і ПрО-*МСП-А* можна сформувати наступні множини інформаційних моделей:

$$I_{\text{ПрО-}МСП\text{-}Пл}=\{I_{\text{ПрО-}МСП\text{-}ПлП}, I_{\text{ПрО-}МСП\text{-}ПлН}, I_{\text{ПрО-}МСП\text{-}ПлВ}\}; \quad (31)$$

$$I_{\text{ПрО-}МСП\text{-}А}=\{I_{\text{ПрО-}МСП\text{-}АД}, I_{\text{ПрО-}МСП\text{-}АС}, I_{\text{ПрО-}МСП\text{-}АБ}\}, \quad (32)$$

де індекси «$_{МСП\text{-}ПлП}$»,«$_{МСП\text{-}ПлН}$»,«$_{МСП\text{-}ПлВ}$», «$_{МСП\text{-}АД}$», «$_{МСП\text{-}АС}$», «$_{МСП\text{-}АБ}$» – відповідно, це індекси інформаційних моделей типових технологій побудови систем захисту від несанкціонованого проникнення, відповідно, на платформу чи на контрольовану акваторію навколо неї.

Як приклад змістовних складників інформаційних моделей для вказаної групи моделей можна вказати на такі роботи з побудови систем захисту підводної частини МСП на її підводної акваторії, управління якими має організувати і забезпечити менеджер проекту (індекси «$_{Д}$»,«$_{С}$» та «$_{Б}$» у залежності (34) на даному етапі розробки опущені через системну схожість робіт для всіх зон захищеної акваторії:

$$I_{\text{ПрО-}МСП\text{-}ПлП}=ПНД_{МСП\text{-}ПлП} \cup РКМ_{МСП\text{-}ПлП} \cup ПСЗ_{МСП\text{-}ПлП} \cup МПН_{МСП\text{-}ПлП} \cup ЕСЗ_{МСП\text{-}ПлП}; \quad (33)$$

$$I_{\text{ПрО-}МСП\text{-}А}=ПНД_{МСП\text{-}А} \cup РКМ_{МСП\text{-}А} \cup ПСЗ_{МСП\text{-}А} \cup МПН_{МСП\text{-}А} \cup ЕСЗ_{МСП\text{-}А}, \quad (34)$$

де *ПНД* – інформаційні моделі процесів виконання прикладних наукових досліджень зі створення високоефективних систем захисту підводної частини МСП та її акваторії; $РКМ_{МСП}$ – інформаційні моделі розробки концепції та прикладних проектних методик оцінки ефективності систем захисту підводної частини МСП та її акваторії; *ПСЗ* – інформаційні моделі управління процесами проектування вказаних систем захисту; *МПН* – інформаційні моделі управління роботами з монтажу та пуско-налагодження запроектованих систем захисту; *ЕСЗ* – інформаційні моделі процесів управління роботами з уведення в експлуатацію створених систем захисту підводної частини МСП та її акваторії.

Для другої групи інформаційних моделей ПрЕ-*МСП* можна сформувати наступну множину інформаційних моделей:

$$I_{\text{ПрЕ-}МСП\text{-}Пл}=\{I_{\text{ПрЕ-}МСП\text{-}ЕП}, I_{\text{ПрЕ-}МСП\text{-}ВП}, I_{\text{ПрЕ-}МСП\text{-}ТП}\}, \quad (35)$$

де індекси «$_{МСП\text{-}ЕП}$», «$_{МСП\text{-}ВП}$» і «$_{МСП\text{-}ТП}$» належать до характеристик типових технологій побудови систем захисту, відповідно, підсистем електро-, водо- та теплопостачання МСП.

Для третьої групи інформаційних моделей ПрІ-*МСП* типових технологій побудови систем захисту інформаційних комунікацій МСП доцільно формувати таку множину:

$$I_{\text{ПрІ}МСП}=\{I_{\text{ПрІ-}МСП\text{-}ЗЗ}, I_{\text{ПрІ-}МСП\text{-}ВЗ}, I_{\text{ПрІ-}МСП\text{-}С}, I_{\text{ПрІ-}МСП\text{-}ОІ}\}, \quad (36)$$

де індекси «$_{МСП\text{-}ЗЗ}$», «$_{МСП\text{-}ВЗ}$», «$_{МСП\text{-}С}$» та «$_{МСП\text{-}ОІ}$» належать до характеристик типових технологій побудови систем захисту інформаційного складника функціонування МСП – відповідно, підсистем зовнішнього і внутрішнього зв'язку, сигналізації та обробки інформації, яка циркулює на МСП.

Для четвертої групи інформаційних моделей ПрК-*МСП* типових технологій побудови систем захисту від загроз, які породжуються зловмисниками з числа персоналу МСП, можна віднести такі моделі:

$$I_{\text{ПрК-}МСП}=\{I_{\text{ПрК-}МСП\text{-}БС}, I_{\text{ПрК-}МСП\text{-}ВБ}, I_{\text{ПрК-}МСП\text{-}ТС}\}, \quad (37)$$

де індекси «$_{МСП\text{-}БС}$», «$_{МСП\text{-}ВБ}$» і «$_{МСП\text{-}ТС}$» належать до технологій профілактичної, упереджувальної та аналітичної роботи з групами співробітників, відповідно, берегових служб МСП, вахтових бригад МСП та екіпажів транспортних засобів, які можуть утворювати загрози функціонуванню МСП через несумлінність, нелояльність чи злочинні наміри.

Таким чином, множини (7)–(11), (17)–(21), (24)–(28), (31), (32) та (35)–(37) утворюють повний перелік інформаційних моделей як складників інформаційних модулів $IM_{\text{Хl}}$, $IM_{\text{Вl}}$, $IM_{\text{Тзl}}$ та $IM_{\text{Прl}}$ (множини (1)–(4)) інформаційної платформи $IP_{\text{МКІl}}$ проекту захисту базового об'єкта – морської стаціонарної платформи.

Обговорення отриманих результатів (SWOT-аналіз результатів досліджень). *Strengths*. Отриманий типовий перелік організацій – учасників проектів захисту об'єктів МКІ та споживачів інформації щодо цих проектів є базовим та утворює множину основних груп стейкхолдерів таких проектів. Це спрощує планування комунікацій у проектах захисту об'єктів МКІ на ранніх стадіях їх розробки.

Запропонована структура моделі інформаційної платформи проектів захисту об'єктів МКІ охоплює основні види інформаційного забезпечення і може бути використана менеджерами проектів як базова під час планування таких проектів.

Отримані інформаційні моделі управління процесами побудови систем захисту підводної частини МСП та її акваторії є узагальненими та утворюють інструментальну основу для створення прикладного програмного забезпечення для автоматизації управління проектами захисту об'єктів МКІ.

Weaknesses. Отримані моделі інформаційної платформи захисту об'єктів МКІ дещо підвищують трудомісткість робот з планування таких проектів на ранніх стадіях їх розробки.

Opportunities. Розробка змістовних складників інформаційних моделей для повного переліку базових проектів $PP_{\text{МКІ}}$ (множини потужністю L), виконана за викладеною у статті методологією, утворить практичне підґрунтя для успішного розв'язку прикладного наукового завдання галузевого значення – ефективного управління проектами захисту об'єктів МКІ від техногенних загроз зловмисного характеру.

Threats. Постійний розвиток технічних засобів, які використовують зловмисники на морі, та світові тенденції щодо збільшення протиправних акцій на об'єктах МКІ вимагають постійного удосконалення засобів захисту об'єктів МКІ. Це зумовлює необхідність проведення наукових досліджень «на випередження», що забезпечило б своєчасне та ефективне протистояння новим загрозам, що виникають.

Висновки. Розв'язано прикладне наукове завдання проектного менеджменту щодо розробки моделі інформаційної платформи управління проектами захисту об'єктів морської критичної інфраструктури як теоретичної основи підвищення їх ефективності на ранніх етапах планування.

Сформовано структуру організацій-учасників інформаційного обміну у проектах захисту об'єктів морської критичної інфраструктури, яка включає державний орган центральної влади, відповідальний за формування й реалізацію державної політики у сфері захисту критичної інфраструктури держави, регіональні та галузеві органи нагляду та контролю безпеки, органи місцевого самоврядування та органи об'єктового захисту, а також міжнародні морські організації. Отримана структура утворює організаційну основу менеджеру проекту для забезпечення інформаційних потреб широкого кола учасників проектів захисту об'єктів МКІ.

На основі системного підходу розроблено структуру та основні складники інформаційної платформи управління проектами захисту об'єктів морської критичної інфраструктури у складі інформаційних модулів основних характеристик базових об'єктів МКІ, загроз та методів протистояння ним, а також інформаційного модуля відомостей про технології побудови систем захисту об'єктів МКІ. Використання отриманої інформаційної платформи скорочує витрати часу проектного менеджера на стадії планування проекту та підвищує ефективність його роботи.

На прикладі захисту від найбільш небезпечної загрози об'єктам МКІ, яка пов'язана з підводним простором, розроблено змістовні частини інформаційних платформ управління процесами розробки систем захисту підводної частини морської стаціонарної платформи та її акваторії.

Подальші дослідження планується проводити у напрямах розробки змістовних частин інформаційних платформ для управління процесами розробки систем захисту інших базових об'єктів МКІ – суден, морських портів, суднобудівних та судноремонтних заводів тощо.

Список літератури

[1] Концепція створення державної системи захисту критичної інфраструктури. № 1009-р. (2017). URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80.

[2] Пріоритетні напрями законодавчого та організаційного забезпечення паспортизації об'єктів критичної інфраструктури. URL: http://old2.niss.gov.ua/content/articles/files/1_Ivaniuta-9af75.pdf.

[3] Lee Gordner, (2014). *Offshore Oil and Gas Safety and Security in the Asia Pacific – The Need for Regional Approaches to Managing Risks*. S. Rajaratnam School of International Studies. Nanyang Technological University, 104 P. URL: https://www.rsis.edu.sg/wp-content/uploads/2014/07/Monograph2613.pdf.

[4] *Offshore Oil and Gas Resources Sector Security Inquiry*. Office of the Inspector of Transport Security. Commonwealth of Australia 2012. 148 P. URL: https://www.homeaffairs.gov.au/transport-security/files/offshore-oil-gas-resources-sector-security-inquiry.pdf.

[5] Martin A. Sebastian, (2015). Critical Infrastructures – Offshore Installation Protection. *Maritime Institute of Malaysia*. Centre of Marine Security & Diplomacy. 33 P. URL: http://www.mima.gov.my/images/page/research/ Capt._Martin_National_Key_Infrastructure_AED.pdf.

[6] Mikhail Kashubsky, & Anthony Morrison. (2013). Security of offshore oil and gas facilities: exclusion zones and ships' routeing. *Australian Journal of Maritime & Ocean Affairs*. 5(1), 10 P. URL: https://doi.org/10.1080/18366503.2013.10815725.

[7] Robert Watts. (2005). Maritime Critical Infrastructure Protection: Multi-Agency Command and Control in an Asymmetric Environment. *Homeland Security Affairs*. I (1,2). Article 3. 12 P. URL: file:///C:/Users/volodymyr.blintsov/Downloads/1.2.3%20(1).pdf.

[8] Recovery Plan for the National Strategy for Maritime Security. (2006). *The Maritime Infrastructure*. 63 p. URL: https://www.dhs.gov/sites/default/files/publications/HSPD_MIRPPlan_0.pdf.

[9] The UK National Strategy for Maritime Security. (2014). Presented to Parliament by the Secretary of State for Defence by Command of Her Majesty. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/322813/20140623-40221_national-maritime-strat-Cm_8829_accessible.pdf.

[10] Heiko Borchert. (2014). *Maritime Security at Risk*. Lucerne: Sandfire. 52 Pages. URL: https://www.borchert.ch/content/ger/cmsfiles/publications/ 1407_Borchert_Maritime_Security_at_Risk.pdf.

[11] *The Guidelines on Cyber Security Onboard Ships*. (2018). Version 3. Produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL. 53 Pages. URL: http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16.

[12] Nineta Polemi. (Elsevier 2017). *Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains*. 214 Pages. URL: https://www.elsevier.com/books/port-cybersecurity/polemi/978-0-12-811818-4.

[13] *Protecting the Connected Barrels. Cybersecurity for Upstream Oil and Gas*. (2017). A report by Deloitte Center for Energy Solutions. Deloitte Development LLC. 22 Pages. URL: file:///C:/Users/volodymyr.blintsov/Downloads/DUP_Protecting-the-connected-barrels%20(1).pdf.

[14] Харитонов, Ю.М., Гордєєв, Б.М., & Бердинських, Б.В. (2017). Моделювання інформаційної платформи управління проектами розвитку портової інфраструктури, *Scientific Journal «ScienceRise»*. Харків, 1/2 (30), 39-47. DOI: 10.15587/2313-8416.2017.91279.

[15] Hrytsaienko, M. (2018). Development of the Information Platform Model for the Neutralization of Underwater Potentially Dangerous Objects. *Technology Audit and Production Reserves*. 2/2(40), 57-62. DOI: 10.15587/2312-8372.2018.129208.

[16] Dihé, Pascal, Ralf Denzer, & Sascha Schlobinski. (2015). An Information Model for a Water Information Platform. *International Federation for Information Processing*. p. 91–101. URL: https://hal.inria.fr/hal-01328529/document.

[17] Ruonan Sun, Shirley Gregor, & Byron Keating. (2015). Information Technology Platforms: Definition and Research Directions. *Australasian Conference on Information Systems*. Adelaide. 17 pages. URL: https://arxiv.org/ftp/arxiv/papers/1606/1606.01445.pdf.

[18] Simon Alterman. *Information Platforms: A Business Model Framework*. URL: https://www.outsellinc.com/product/information-platforms-a-business-model-framework/.

[19] Блінцов, В.С., & Майданюк, П.В. (2016). Концепція системи захисту інформації, що циркулює на об'єктах морської інфраструктури. *Збірник наукових праць НУК*. 1(463). С. 57–64. DOI 105589/отт20160109.

[20] Gibson, J., Scherer, W., & Gibson, W. (2007). How to Do Systems Analysis (Wiley Series in Systems Engineering and Management). *Wiley-Interscience*. 1, 360 Pages. URL: https://www.amazon.com/How-Systems-Analysis-John-Gibson/dp/0470007656.

[21] *Руководство к Своду знаний по управлению проектами (Руководство PMBOK®)*. Пятое издание. С. 1–17. URL: https://drm.pmi.org/Default.aspx?doc=PMBOKGuideFifthEd.pdf

[22] *Біла Книга – Транспорт*. (2011). План розвитку єдиного європейського транспортного простору на шляху до конкурентоспроможної та ресурсоефективної транспортної системи. Видавничий центр Європейського

Союзу в Люксембурзі. Doi: 10.2832/30955. https://brdo.com.ua/wp-content/uploads/2016/01/1_Bila-knyga-transport-plan-rozvytku-yedynogo-yevropey-skogo-transportnogo-prostoru-na-shlyahu-do-konkuretnospromozhnoi-ta-resursoefektyvnoi-.pdf.

[23] Бабкін, Г.В., Блінцов, В.С., Дружинін, Є.А., Кійко, С.Г., Книрік, Н.Р., Кошкін, К.В., Крицький, Д.М., Рижков, С.С., & Слободян С.О. (2017). Управління успішними проектами створення складної техніки. Монографія. Миколаїв : Торубари В.В. 336 с.

[24] Захарченко, В.П., & Неня, В.Г. (2015). Системне проектування інформаційної моделі проектної операції як елемента виробничого процесу. *Східно-Європейський журнал передових технологій*. 1/3 (73), 53-56. DOI: https://doi.org/10.15587/1729-4061.2015.37192.

[25] Харитонов, Ю.Н. (2008). Управление проектами реконструкции на основе артефактных платформ. *Авиационно-космическая техника и технологии*. 8(55), 189–192.

[26] Moo-Hyun Kim,. (2012). *Spar platforms. Technology and analysis methods*. The American Society of Civil Engineers, 240 Pages. URL: https://www.amazon.com/SPAR-Platforms-Technology-Analysis-Methods/dp/078441209X.