ISSN 2076-2429 (print)
ISSN 2223-3814 (online)

INFORMACION TECHNOLOGY. AUTOMATION

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ. АВТОМАТИЗАЦІЯ

UDC 005.8

V. Blintsov[1]**,** DSc, Prof.,
P. Maidaniuk[2]
[1] Admiral Makarov National University of Shipbuilding, 9 Heroes of Ukraine Ave., Mykolaiv, Ukraine, 54025; e-mail: volodymyr.blintsov@nuos.edu.ua
[2] State Service of Special Communications and Information Protection of Ukraine, 32 Spaska Str., Mykolaiv, Ukraine, 54001

CLASSIFICATION OF PROJECTS FOR THE PROTECTION OF MARINE CRITICAL INFRASTRUCTURE FACILITIES

В.С. Блінцов, П.В. Майданюк. **Класифікація проектів захисту об’єктів морської критичної інфраструктури.** Україна є морською державою з активно працюючою інфраструктурою водного транспорту. До її складу входять морські транспортні шляхи у морських територіальних водах держави та внутрішні водні шляхи, морські та річкові порти, суднобудівні та судноремонтні заводи, магістральні морські трубопроводи тощо. Згідно законодавству вказані об’єкти відносяться до об’єктів критичної інфраструктури держави і підлягають захисту. На цей час питання управління проектами розробки і створення систем захисту об’єктів морської критичної інфраструктури від сучасного комплексу загроз їх функціонуванню знаходиться на початковій стадії свого становлення. Це робить актуальним наукове завдання розробки класифікації таких проектів, що створило б теоретичну основу для подальших досліджень у напрямку проектного менеджменту та для побудови високоефективних систем захисту таких об’єктів. У статті запропоновано у якості базових ознак класифікації використовувати приналежність об’єктів морської критичної інфраструктури до точкових, площинних та протяжних, що утворює програму базових проектів захисту таких об’єктів і забезпечує їх уніфікацію на стадіях планування і виконання. Виходячи з реалізації принципів системного підходу щодо комплексного врахування особливостей функціонування матеріальної, енергетичної та інформаційної складових об’єктів, а також з урахуванням людського фактору як складової ефективної експлуатації цих об’єктів, для кожного з проектів програми запропоновано їх класифікацію за видами безпеки. Така класифікація включає основні підпроекти «Фізична безпека», «Енергетична безпека», «Інформаційна безпека» та «Кадрова безпека» й утворює другий класифікаційний рівень. Третій кваліфікаційний рівень, виходячи з принципів системного підходу, охоплює типові роботи менеджера проекту по встановленню властивостей об’єктів захисту та характеру загроз, а також типові роботи з вибору необхідних технологій захисту і практик їх успішного створення. Запропоновані кваліфікаційні рівні сформовано у вигляді множин, відповідно, базових проектів, основних підпроектів і типових робіт менеджера проекту. Отримані множини утворюють генеральну множину робіт програми проектів захисту об’єктів морської критичної інфраструктури. Первинне формулювання робіт генеральної множини створює базу даних шаблонів робіт для однотипних проектів, а виконані типові роботи, основні підпроекти та базові проекти утворюють та постійно доповнюють базу даних артефактних проектів захисту об’єктів морської критичної інфраструктури. Генеральна множина базових проектів, основних підпроектів і типових робіт програми проектів захисту об’єктів морської критичної інфраструктури утворює організаційну основу для ефективної роботи менеджерів проектів безпеки таких об’єктів. Її застосування у практиці управління проектами забезпечить скорочення витрат часу на планування проектів за рахунок використання шаблонів та артефактних проектів, які мають накопичуватись у результаті проектної діяльності команди менеджерів у відповідних базах даних.

Ключові слова: морська критична інфраструктура, класифікація проектів захисту, системний підхід, програма проектів

V. Blintsov, P. Maidaniuk. **Classification of projects for the protection of marine critical infrastructure facilities.** The Ukraine is a seafaring state whose maritime transport infrastructure is actively operated. That infrastructure includes sea transport routes in the territorial maritime belt and inland waterways, sea and river ports, shipbuilding and ship repair yards, off-shore main pipelines and other facilities. According to the law, these facilities classified as the State's critical infrastructure components are subject to protection. Currently, the scope of issues on managing projects for the development and creation of systems aimed onto marine critical infrastructure facilities protecting against the contemporary threats to their functioning is still at the initial elaboration stage. That substantiates the relevance of urgent scientific task to develop such projects classification which would serve in a theoretical basis for further research in the project management field and would be useful for such facilities' most advanced protection systems building. The article proposes to use as the basic classification features the marine critical infrastructure facilities' pertinency to point-, plane-area or extended type, that allows structuring such facilities' protection basic projects program and ensures their unification at the planning and implementation stages. Departing from the systematic approach principles as to the comprehensive account of the material, energy and information components' functioning and considering the

DOI: 10.15276/opu.3.59.2019.11

human factor as these facilities efficient operation component, the classification by security type has been proposed for each of the programme projects. Such classification includes the main subprojects “Physical security”, “Power-related security”, “Information security” and “Personnel security” thus forming the second classification level. The third classification level, based on the system approach principles, covers typical work of the project manager to identify the security objects' properties and the nature of threats, as well as typical works on selecting the necessary security technologies and practices for their successful implementation. The proposed qualification levels are accordingly presented as the sets formed by arrays that include basic projects, main subprojects, and typical works of the project manager. The obtained sets form the entire pattern of works integral to the marine critical infrastructure facilities protection projects program. At the issue of that Works general pattern initial formulation both a database of work templates for similar projects is created; thus the completed standard works, main subprojects, and basic projects do form and constantly contribute to the database of artifacts as to marine critical infrastructure objects protection projects. The entire set or totality of basic projects, main subprojects, and standard works under marine critical infrastructure facilities protection projects program provides an organizational basis for efficient professional activity of such facilities security project managers. Its application in project management practice will reduce the time spent on project planning through use of templates and artifact project accumulated in the corresponding databases as a result of managers’ team project activities.

Keywords: marine critical infrastructure, protection projects classification, system approach, projects program

Introduction. Currently the Ukraine's marine transport infrastructure includes 13 continental ports and 16 river ports and terminals [1]. Sea transport routes making part to the international maritime traffic ways pass through the marine belt of Ukraine [2]. According to the decision taken by the Cabinet of Ministers of Ukraine, all ports belong to the State's critical infrastructure subject to protection in order to guarantee the State functions both in peacetime and when a special period [3].

Analysis of global trends in marine transport activity evidences an increase in the terrorist threats level, an increase in the number and complexity of attacks on marine infrastructure facilities as well as of cyber attacks on their information resources. Considering those trends and damage to infrastructure facilities in the Eastern and Southern regions of Ukraine, the Cabinet of Ministers of Ukraine approved the “Concept on creating the national system to protect the critical infrastructure” [4].That concept identifies the main directions, mechanisms and terms for a comprehensive legal arrangement as to the issues of critical infrastructure protection, including the marine critical infrastructure (MCI) facilities, as well as for the creation of a governmental control system in the field of critical infrastructure protection.

The significance in the international scale of Ukrainian MCI facilities protection is confirmed by the European program for critical infrastructure protection (EPCIP) and the European information network for critical infrastructure threat prevention (European Critical Infrastructure Warning information network, CIWIN) [5, 6].

These and other documents do immediately point to the need for creating an unified system of MCI facilities protection as a component of the European water transport safety. At the same time, the main tasks of each European state include work on creating its own, national system for MCI facilities protection, all those systems integrating as components into an united pan-European system and easily integrating for joint actions.

Given the current geopolitical realities, the Ukrainian water transport system can be considered by European and transatlantic partners as a critical infrastructure of pan-European significance. This imposes as required the implementation of a project approach to building the national MCI protection component, which would ensure the creation of a highly efficient protection system providing for a close partnership with the EU countries.

Analysis of recent publications and problem statement. The task of marine critical infrastructure facilities (MCI) protecting (NCIS) has always been a central point the Ukrainian government and domestic scientists [7 – 9] focused their attention onto. Thus, the Order issued by the Ministry of Infrastructure of Ukraine [7] lays the foundations to a sea port security concept principally new for Ukraine, that defines the main tasks as “implementing a totality of organizational, administrative, regime-related and technical measures to prevent, detect and suppress acts of piracy, terrorism and illegal interference in the port or port facility activities”. Still that document being this one of general organizational character it considers security measures for only one MCI facilities type (sea port). In particular, the issues of ensuring ports' energy and information security are not highlighted therein.

The publication [8] exposes the experience of working out the concept of critical infrastructure protection in Ukraine and suggests priority directions for such concept implementing in the national security system of Ukraine. In particular, the tasks of providing scientific and technological, methodological and personnel support for the critical infrastructure protection are set. However, the features of MCI facilities security organization are not considered in this work.

In [9], the issues of building a secured information system for sea area monitoring are considered, but other important components of the MCI facilities protection system such as material, power, and personnel have not been covered therein.

Among the foreign sources the most extensive study of issues on marine infrastructure protection is given in the strategic documents of world's leading seafaring countries: Great Britain, USA and France [10 – 12]. For example, [10] presents the UK's national maritime security strategy, that provides for a set of measures aimed to organize a three-level system for protecting the state's waters. The source [11] outlines the U.S. national maritime security strategy, based on the global Maritime intelligence integration plan, the Operational threat response plan, the international Information awareness and coordination strategy, the Maritime transport system security plan, and the Maritime trade security plan. The source [12] exposes the national maritime security strategy of France, which main implementation areas refer to the water environment control, ships protection, combating the illegal sea trade channels practice, national economic interests protection at sea and the the state's maritime borders protection.

These documents contain a complete list of tasks relevant for any seafaring state in the world. However, these tasks implementation requires to elaborate a detailed implementation plan that would take into account national interests and peculiarities of MCI facilities' functioning in each specific country.

In addition, a large number of publications are devoted to the world's main sea transport corridors study and principles of their security organization. For example, in [13] discussed are the activities of the Combined Maritime Forces (CMF) international organization to ensure the safety of navigation through the Gulf of Aden, the Bab El-Mandeb Strait, the Red Sea and in the related waters. In particular, considered is the creation of a new organizational structure, the Maritime Security Transit Corridor (MSTC). The source [14] deals with the organization of maritime security in the Indian ocean. The author focuses on the characteristics of maritime security and threats (including military aspects, lines for communication at sea, maritime piracy, port security, ocean resources security, smuggling and human trafficking, non-state threats and security outsourcing), as well as on the organisational problems as to the sub-regional and multinational cooperation.

In these and other foreign authors' publications the problems of sea transport routes security are studied mainly from the position of armed countering to the unauthorized entrance aboard attempts in order to capture ships taking possession of material resources. However, none source considers the issues of international MCI facilities complex protection based on the principles of a systematic approach with the account of energy, communication and personnel components.

For Ukraine, currently, one of the state's general strategy establishing documents is this one published by the National Institute for strategic studies [15], setting out the basic principles on building a system for critical infrastructure protection, based on its role in ensuring the national security of a modern state. According to this document, the critical infrastructure does mean the totality of "systems and resources, physical or virtual so vital to the country that their functional incapacity or destruction undermines the national security, national economy, public health or population security, either results in any combination of the above."

Considering the Ukrainian MCI facilities, the issues of building systems that render protection against “threats from the sea” are currently at the initial stage of development. The main task of project management for such facilities today is to develop a general theoretical framework that allowed a use of the system approach general principles to form a scientific basis for building those facilities high-performance protection systems.

Well known is that in project management a system approach embodies a comprehensive study of the whole phenomenon or process from the system analysis standpoint, aimed at clarifying the complex problem with its rearrangement into series of tasks that can be resolved using organizational and economic-mathematical methods, finding criteria for the solution and detailing those tasks' goals, therefore a synthesis of effective organizational structure to achieve those goals [16].

The project manager's priority task is to develop a generalized project management structure for the MCI facilities' protection which would include systematic information about the main projects and works required for their implementation.

This study purpose and objectives. This article purpose is to develop a classification of projects for the marine critical infrastructure facilities protection as a theoretical basis for managing those facilities protection processes based on a systematic approach, taking into account the protected objects' properties, existing threats to their functioning, and protection technologies.

This goal achievement requires to solve the following scientific problems:

– creating, on the basis of the seafaring state typical MCI facilities analysis, the basic project program aimed onto such objects safety ensuring, and offering, on the system approach basis, the main subprojects which implementation will provide effective protection of the said facilities;

– offering a variety of typical project manager works, that will ensure both construction and successful operation of MCI facilities protection system;

– getting a general pattern, totalizing projects, subprojects and works of MCI facilities protection project program in the form of a three-dimensional matrix that helps the Manager in carrying out high-quality planning of MCI facilities protection projects with works systematisation using databases of similar projects templates and databases of MCI facilities protection artifact projects.

Development of general pattern for basic projects, main subprojects, and standard works under MCI facilities protection projects program. The challenging worldwide, and particularly in Ukraine, security situation on water transport, caused by the intensification of terrorism, piracy and military aggression acts, requires to adopt appropriate measures (both preventive and response ones) in relation to MCI facilities, which list, first of all, includes the following:

– water transport (WT) – sea, river, lake;

– water transport routes (WTR) – sea transport corridors, anchorages, river fairways and channels, shipping routes on water reservoirs and lakes;

– sea and river ports and transshipment complexes (PRT);

– offshore fixed platforms, underwater pipelines and other fixed structures located on the sea shelf (SLF);

– shipbuilding and ship repair yards (YRD);

– naval bases (NVB).

In general case, such objects set can be expanded through:

– consideration of certain types of main MCI facilities as above (for example, for stationary structures (SLF) located on the offshore shelf, here the list can be extended with offshore fixed platforms (Slf1), underwater pipelines (Slf2), etc;

– adding to this security system other facilities of special importance (berthing facilities for special cargo $P_{\mathrm{PRT\ SLF}}$, undersea communications cables $P_{\mathrm{HM\_FCT}}$, floating ship-repair workshops P_{WRSH}, floating docks P_{DOCK} and the like).

Accordingly, the security projects of these MCI types as an aggregate can be presented in the form of a PP_{MCI} projects program integral to L projects (the indexes correspond to the above abbreviations):

$$PP_{\mathrm{MCI}} = \{P_{\mathrm{WT}};\ P_{\mathrm{WTR}};\ P_{\mathrm{PRT}};\ P_{\mathrm{SLF}};\ P_{\mathrm{YRD}};\ P_{\mathrm{NVB}};\ P_{\mathrm{PRT\ SLF}};\ P_{\mathrm{HM\_FCT}};\ P_{\mathrm{WRSH}};\ P_{\mathrm{DOCK}};\ \ldots\ P_l;\ \ldots;\ P_L\}. \quad (1)$$

Proposed is to develop a national system MCI facilities protection based on the systematic approach principles in combination with the best practices of project management [17,18].

It is known that the system approach to new technology objects creating implies a comprehensive account of such objects' material, energy and information components functioning, as well as taking into account the human factor as their effective operation component. From the project management theory it follows that this approach corresponds to the research direction “Project and program management processes” [19].

With regard to the MCI facilities protection, the following set of main subprojects UP_{MCI} is proposed for each of the program (1) projects, whose implementation is managed on the basis of a systematic approach to security types classification:

$$UP_{\mathrm{MCI}}=\{UP_{\mathrm{PH\_SEC}};\ UP_{\mathrm{EN\_SEC}};\ UP_{\mathrm{IN\_SEC}};\ UP_{\mathrm{PER\_SEC}}\}, \qquad (2)$$

where $UP_{\mathrm{PH\_SEC}}$ – “Physical security” subproject which includes measures to prevent unauthorized physical access to MCI facilities and their information resources;

$UP_{\mathrm{EN\_SEC}}$ – “Energy security”, subproject which includes measures for guaranteed energy supply of MCI facilities in peacetime and when a special regime period;

$UP_{\mathrm{IN\_SEC}}$ – “Information security” subproject which includes measures to protect communication systems and document flow at MCI facilities;

$UP_{\mathrm{PER\_SEC}}$ – “personnel security” subproject, which includes measures to manage the development and implementation of personnel policy at MCI facilities.

In some cases, this set can be expanded by additional subprojects of a special direction – financial security $UP_{\mathrm{FIN\_SEC}}$,, procurement security $UP_{\mathrm{PROC\_SUP}}$, regulatory support for projects $UP_{\mathrm{LEG\_SUP}}$ etc Then denoting the total number of main subprojects with M, we write the expression (2) in the form:

$$UP_{\mathrm{MCI}}=\{UP_{\mathrm{PH\_SEC}};\ UP_{\mathrm{EN\_SEC}};\ UP_{\mathrm{IN\_SEC}};\ UP_{\mathrm{HM\_FCT}};\ UP_{\mathrm{FIN\_SEC}};$$
$$UP_{\mathrm{PROC\_SUP}};\ UP_{\mathrm{LEG\_SUP}};\ \ldots;\ UP_{\mathrm{TECH\_SUP}};\ \ldots;\ UP_{M}\}. \qquad (3)$$

It is also proposed to introduce for each of these main subprojects, a set of project manager's standard works J_{MCI} which should cover the full range of measures for creating a security system; so such program implementation management will ensure the MCI facilities protection. Based on the principles of a systematic approach to the process of creating the MCI protection system, such works set shall cover:

$$J_{\mathrm{MCI}}=\{J_{\mathrm{X}};\ J_{\mathrm{OFFEND}};\ J_{\mathrm{WTYRD}};\ J_{\mathrm{PRTp}}\}, \qquad (4)$$

where J_{X} – works on determining the list of all significant characteristics of MCI facilities subject to protection (material values, energy, information and personnel support of MCI facilities);

J_{OFFEND} – work to identify the likely offenders characteristics to prevent from the protection system shall be built (for sub-project $UP_{\mathrm{PH\_SEC}}$ – terrorists, unauthorized visitors and their technical equipment; for subproject $UP_{\mathrm{EN\_SEC}}$ – characteristics of the threats to the energy system of MCI facility; for subproject $UP_{\mathrm{IN\_SEC}}$ – hackers and unauthorized users; for subproject $UP_{\mathrm{PER\_SEC}}$ – characteristics of MCI personnel constituting threats to the facility operation physical, energy and information components, at the same time posing risks related to intellectual capacity of the personnel and labor relations);

J_{WTYRD} – works to determine the protection technologies required to prevent the offender's illegal actions (information, technical and power related);

J_{PRTp} – organisational works for practical implementation of MCI facilities protection projects (design, construction, commissioning and maintenance of operation).

It should be noted that at separate projects the above list of typical activities can if necessary be supplemented with other activities (organization and management of MCI facilities protection new techniques development and creation processes J_{NEW}, organization and control of MCI facilities protection new equipment and technologies tests J_{TESTS} and the like).

It is obvious that the proposed set of standard works J_{MCI} is also based on a systematic approach to creating a MCI protection system, since it covers work on identifying the security objects' properties and the nature of threats, as well as work on selecting the necessary protection technologies and practices for their creation and embodiment.

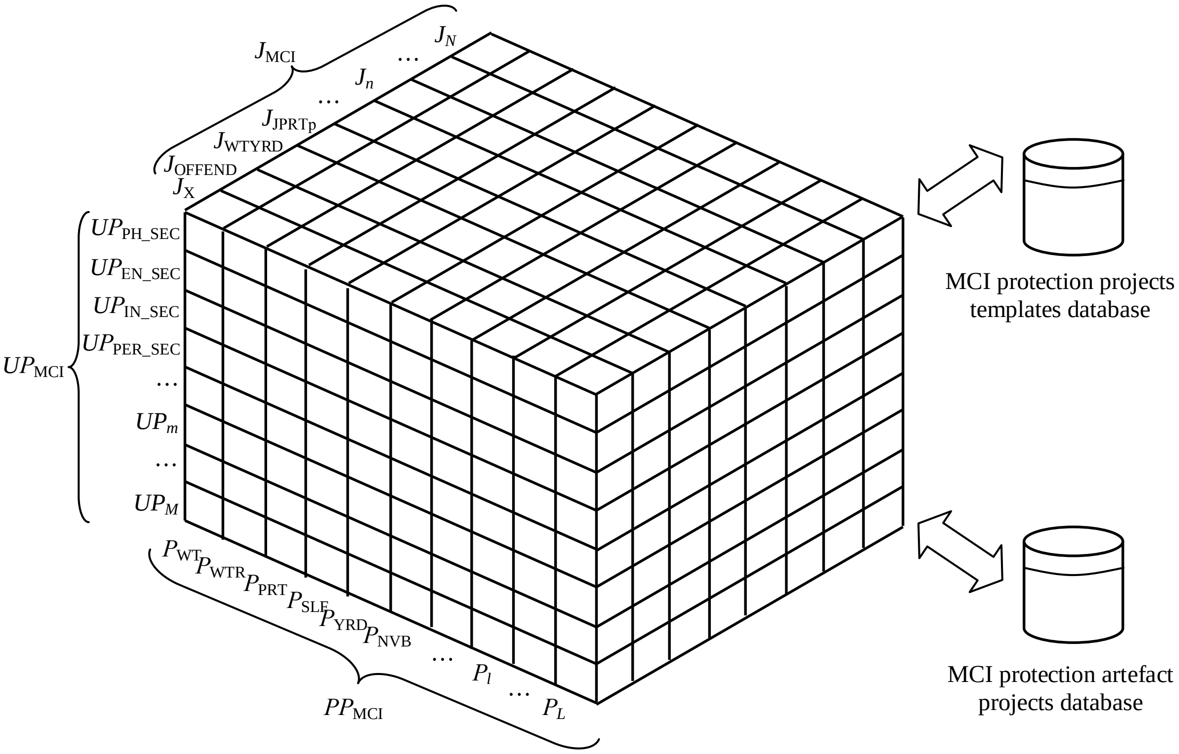
Denoting the total number of typical works with N, we write this set as:

$$J_{\mathrm{MCI}}=\{J_{\mathrm{X}};\ J_{\mathrm{OFFEND}};\ J_{\mathrm{WTYRD}};\ J_{\mathrm{PRTp}};\ J_{\mathrm{NEW}};\ J_{\mathrm{TESTS}};\ \ldots\ J_{n};\ \ldots;\ J_{N}\}. \qquad (5)$$

According to (1), (3) and (5) we build the entire assembly $Q_{\mathrm{MCI}}=\{PP_{\mathrm{MCI}};\ UP_{\mathrm{MCI}};\ J_{\mathrm{MCI}}\}$ of MCI facilities protection program PP_{MCI} projects, subprojects and works, where each element $q_{l,m,n}\in Q_{\mathrm{MCI}}$ represents a single n-th job which execution control will protect the MCI l-th facility protection in respect of *m*-th threat type criterion. The resulting entire assembly Q_{MCI} embodies a classification of basic projects, main subprojects and typical works at MCI facilities protection program projects.

From a mathematical viewpoint, the Q_{MCI} set is a three-dimensional matrix (a three-dimensional array of MCI protection project manager works) $Q_{\text{MKI}} = (q_{l,m,n})_{L,M,N}$, which initial filling creates templates for similar projects. This matrix allows an efficient work with databases of artifact projects, using them when planning projects for MCI facilities protection and enlarging those databases with new projects and works.

A graphical representation of entire set of projects and works Q_{MCI} shaped as the "Parallelepiped of management tasks for MCI facilities protection projects" is shown in Figure.



Program "Parallelepiped of project management tasks for marine critical infrastructure facilities protection"

As seen in Figure, the entire set Q_{MCI} allows us to systematize the processes of templates database creation.

Thus, the obtained entire projects and works set Q_{MCI} components renders possible to systematize the project manager work on managing the MCI facilities protection projects program PP_{MCI} at all phases of their existence.

It is obvious that in real practice the project manager shall build an individual "Parallelepiped of protection projects management" $Q_{\text{MCI}in\_sec}$ for each component of the security projects array (1) for each *i*-th basic project of projects PP_{MCI} program.

An example of a practical construction for a portion from the entire projects and works set Q_{MCI}. As an example, let's consider a fragment of the initial implementation for one of the projects making part to the projects PP_{MCI} program, namely the P_{SLF1} project. ensuring the marine stationary platform safety ($P_{\text{SLF1}} \in P_{\text{SLF}}$). We examine sequentially the features of managing subprojects in accordance with (3) on the example of $UP_{\text{SLF1-PH\_SEC}}$ "Physical security" subproject for which a fully developed security subproject is not yet available.

Both from the printed sources [18] and the long-term experience accumulated by the Admiral Makarov National University of Shipbuilding on surveying the marine stationary platforms (MSPs) on the Black sea well known is that the main task of the “Physical security” $UP_{\mathrm{SLF1\text{-}PH\_SEC}}$ subproject is to manage the processes of preventing an unauthorized physical access to MSPs. Such subprojects usually require taking into account the particular given MSP's geographical location $J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}X}\Gamma}$, its design features from the facility access viewpoint $J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}XHM\_FCT}}$ and determining the significant characteristics of this MSP as an object of material value $J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}XPROC\_SUP}}$.

Then, according to (5) the subproject P_{SLF1} implies a necessary control as to following works making part to J_{X} subset for determining its significant characteristics list:

$$J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}X}}=\{J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}X}\Gamma};\ J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}XHM\_FCT}};\ J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}XPROC\_SUP}}\}. \qquad (6)$$

Management of works attributed to J_{OFFEND} subset on determining the likely offenders' characteristics for which prevention the protection system shall be built can be divided into:

– managing the $J_{\mathrm{SLF1\text{-}OFFEND\text{-}WT\ DOCK}}$ works to identify characteristics and develop the alleged terrorists and saboteurs behavioral models that may pose a threat of unauthorized entry to the territory of MSPs by surface, underwater and air routes;

– managing the $J_{\mathrm{SLF1\text{-}OFFEND\text{-}NEW\ OFFEND}}$ works to identify characteristics and develop behavioral models of unauthorized visitors who intend an unauthorized entry to MSPs territory for the material gain purpose;

– managing the $J_{\mathrm{SLF1\text{-}OFFEND\text{-}WT\ YRD}}$ works to identify characteristics and developing models of technical equipment operation (on water surface, underwater and airborne) that can be used to penetrate the protected MSP water area for the purpose of transporting offenders or equipment intended for unauthorized data retrieval or destructive damage.

Thus, according to (5) for P_{SLF1} subproject, the project manager must organize managerial control over following works making part to the J_{OFFEND} subset for determining the likely offenders' characteristics:

$$J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}OFFEND}}=\{J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}WT\ DOCK}};\ J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}NEW\ OFFEND}};\ J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}WT\ YRD}}\}. \qquad (7)$$

Managing the works referred to the J_{WTYRD} subset for determining the security technologies required to prevent the offenders' illegal actions usually involves creating a multi-level system of MSOs protection which can be summarized as the following measures aggregate:

$$J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}WT\ YRD}}=\{J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}HM\_FCT\ SLF}};\ J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}HM\_FCT\ PRT}};$$
$$J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}HM\_FCTDock}};\ J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}HM\_FCT\ tests}}\}, \qquad (8)$$

where $J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}HM\_FCT\ SLF}}$ is a set of measures for managing the processes of intruder detecting, his actions monitoring, and evaluation of risks associated with those actions;

$J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}HM\_FCT\ PRT}}$ is a set of measures for managing such intruder warning that he is detected and about the need to stop unauthorized activities;

$J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}HM\_FCT\ Dock}}$ is a set of measures to manage the forceful counteraction to the intruder, aimed to motivate him for unauthorized activities abandoning;

$J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}HM\_FCT\ tests}}$ is a set of measures to manage the forceful counteraction to the offender, purposed to force him for stopping the illegal actions.

Managing works from the J_{PRTp} subset on organization of MCI facilities protection projects practical implementation usually includes four main groups jobs:

$$J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}WT\ YRD}}=\{J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}PRTp1}};\ J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}PRTp2}};\ J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}PRTp3}};\ J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}PRTp4}}\}, \qquad (9)$$

where $J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}PRTp1}}$ is work on managing the development and design of a system securing MSPs against the identified threats;

$J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}PRTp2}}$ refers to the management of works on organizing the MSP protection system building;

$J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}PRTp3}}$ is the management of works on the organization of MSP protection system acceptance tests and commissioning;

$J_{\mathrm{SLF1\text{-}PH\_SEC\text{-}PRTp4}}$ refers to the management of works to organize the MSP protection system operation.

Thus, dependencies (6) – (9) allow the MSP security project manager to schedule a list of typical activities for managing the $UP_{\text{SLF1-PH\_SEC}}$ “Physical security” subproject as an integral part of the marine stationary platform security project P_{SLF1} within entire PP_{MCI} projects program.

Similarly, taking into account the operation specific features and special requirements for the protection system, jobs arrays are composed as sets relevant to other subprojects of P_{SLF1} project and other components of PP_{MCI} projects program.

To mention is that the complexity of project managers work will decrease by the measure of project templates database and the artifact projects database accumulation (Figure).

Discussion of elaborated classification of MCI facilities protection projects. Since in Ukraine the task of managing the MCI facilities protection projects is at an early elaboration stage, those projects successful completion greatly depends onto development of such projects classification features based on a systematic approach. This approach provides for a comprehensive consideration of all factors contributing the MCI facilities safety. These factors include:

– coverage by security measures of all basic MCI facilities, which failure will lead to losses on a national scale; such facilities are subdivided into point objects (water transport, stationary facilities of marine infrastructure), plane area-laid (ports, shipyards) and longitudinally-extended (water transport routes) facilities;

– taking into account the peculiarities of functioning and protection as to MCI facilities' main system components which include the protection of material, energy and information resources as well as safeguarding against threats posed by unreliable or incompetent personnel;

– planning a set of works to build the MCI facilities protection system that provides answers to project manager's key questions: “what shall we protect?”, “from whom shall it be protected?”, “how should it be protected?” and “how shall we arrange such a protection system?”.

The classification of MCI facilities protection projects here above proposed is built based on just these factors. It represents a “Parallelepiped of project management tasks for MCI facilities protection”, built on the basis of three sets: the program of respectively, PP_{MCI} projects, UP_{MCI} subprojects and J_{MCI} jobs. The proposed classification is systemically complete and provides the scientific and organizational basis assisting the project manager's work at the MCI facilities protection project planning phase.

The general pattern or Q_{MCI} totality of basic projects, main subprojects, and standard works of MCI facilities protection projects program lays the procedural structure serving in basis to organize effectively the MCI facilities protection projects managers,' activity since it allows reducing the time they spend on project planning, using templates and project artifacts accumulated in the corresponding databases throughout the management team project activities.

The considered example of a practical activities' plotting for a portion from projects and works entire set, namely “Physical security of a marine stationary platform” subproject clearly demonstrates the content of the project manager's activity in planning typical works for such kind of critical marine infrastructure facilities.

Conclusions

The article proposes a classification of marine critical infrastructure facilities protection projects based on the systematic approach principles and considering the protected facilities with regard to four main threats types: threats to those facilities' physical, energy, information and personnel security. The developed classification also takes into account the protected objects' features, existing threats to their functioning and the technological opportunities to render them secured.

The study served to formulate a program of basic projects purposed to ensure such facilities' safety the protected objects being subcategorised into main point, plane area and extended marine critical infrastructure facilities.

Created is the project manager's working tool embodied with a set of typical works which successive implementation management will contribute to both rational creation and efficient operation of the marine critical infrastructure facilities protection system.

At the issue of research carried out, an entire set of the marine critical infrastructure facilities protection system Program's projects, subprojects, and works has been built in the form of a three-dimensional matrix (a three-dimensional array of project manager's jobs), that matrix initial filling creates templates for similar projects.

The resulting matrix gives the theoretical basis for marine critical infrastructure facilities protection system projects qualitative planning and formalizes the processes of those projects' new work templates databases creating, as well as contributes to the systematic use of existing templates on work and artifact projects for the marine critical infrastructure facilities protection projects.

Література

1. Інформація про водний транспорт України. Міністерство інфраструктури України. 2019. URL: https://mtu.gov.ua/content/informaciya-pro-vodniy-transport-ukraini.html. (дата звернення 02.12.2019).
2. Транспорт України. Міжнародні транспортні коридори на території України. 2017. URL: https://mozok.click/182-transport-ukrayini-mzhnarodn-transportn-koridori-na-teritoryi-ukrayini.html. (дата звернення 02.12.2019)
3. Перелік об'єктів державної власності, що мають стратегічне значення для економіки і безпеки держави: Постанова Кабінету Міністрів України від 04.03.2015 №83. URL: http://www.spfu.gov.ua/userfiles/files/postanova83.pdf. (дата звернення 02.12.2019).
4. Концепція створення державної системи захисту критичної інфраструктури. Схвалено розпорядженням Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80. (дата звернення 02.12.2019).
5. Council Directive 2008/114/EC “On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection”. 2008. URL: http://eur-lex.europa.eu/.
6. Critical Infrastructure Warning Information Network – CIWIN. 2008. URL: http://ccpic.mai.gov.ro/ciwin_en.html.
7. Про затвердження Типового положення про службу морської безпеки порту: Наказ Мінінфраструктури України від 25 серпня 2011 р., № 339. URL: https://zakon.rada.gov.ua/laws/show/z1233-11. (дата звернення 02.12.2019).
8. Бірюков Д.С. Захист критичної інфраструктури в Україні: від наукового осмислення до розробки засад політики. *Науково-інформаційний вісник Академії національної безпеки.* 2015. 3–4 (7–8). С. 155–170.
9. Blintsov O., Maidaniuk P. Development of informationally-protected System of Marine Water Area Monitoring. *Eastern-European Journal of Enterprise Technologies.* 2017. №6/9(90). P. 10–16. DOI: 10.15587/1729-4061.2017.1188514.
10. The UK National Strategy for Maritime Security. 2014. 53 p. URL: https://assets. publishi.-g.service.gov.uk/government/uploads/system/uploads/attachment_data/file/322813/20140623-40221_ national-maritime-strat-Cm_8829_accessible.pdf.
11. The National Strategy for Maritime Security. 2005. URL: https://georgewbush-whitehouse.archives.gov/homeland/maritime-security.html. (дата звернення 02.12.2019).
12. National strategy for the security of maritime areas. 2015. 58 p. URL: https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2016/01/strategie_nationale_de_surete_des_espaces_maritimes_ en_national_strategy_for_the_security_of_maritime_areas.pdf.
13. Maritime Security Transit Corridor (MSTC). URL: https://combinedmaritimeforces.com/maritime-security-transit-corridor-mstc/. (дата звернення 02.12.2019).
14. Thean Potgieter. Maritime security in the Indian Ocean: strategic setting and features. Institute for Security Studies, 2012. №236. 21 P. URL: https://www.africaportal.org/publications/maritime-security-in-the-indian-ocean-strategic-setting-and-features/.
15. Зелена книга з питань захисту критичної інфраструктури в Україні (друга версія проекту документа). Національний інститут стратегічних досліджень. 2014. 31 с. URL: http://old2.niss.gov.ua/public/File/2014_table/1125_zelknuga.pdf.
16. Joseph Devine. Project Management - A Systemic Approach. 2008. URL: http://pdf2.hegoa.efaber.net/entry/content/966/Project_Management_-_A_Systemic_Approach.pdf.
17. Blintsov V., Hrytsaienko M. Improvement of the management of material and technical resources of water cleaning projects from explosive objects. *Technology Audit and Production Reserves.* 2016. № 6/2(32). P. 51–56. URL: http://journals.uran.ua/tarp/article/view/86810/83010.
18. Dan Secrieru, Gheorghe Oaie, Vlad Radulescu, Cristina Voicaru. The Black Sea Security System – A New Early Warning and Environmental Monitoring System. 2015. URL: https://www. springerprofessional.de/en/the-black-sea-security-system-a-new-early-warning-and-environmen/2276828.
19. Бушуєв С.Д., Гогунський В.Д., Кошкін К.В. Напрями дисертаційних наукових досліджень зі спеціальності «Управління проектами та програмами». *Управління розвитком складних систем.* 2012. 12. С. 5–7. URL: http://nbuv.gov.ua/UJRN/Urss_2012_12_3.

References

1. Ministry of Infrastructure of Ukraine. (2019). *Information reference about water transport in Ukraine.* Retrieved from: https://mtu.gov.ua/content/informaciya-pro-vodniy-transport-ukraini.html.
2. *Transport of Ukraine. International transport corridors on the territory of Ukraine.* (2017). Retrieved from: https://mozok.click/182-transport-ukrayini-mzhnarodn-transportn-koridori-na-territory-ukrayini.html.
3. Cabinet of Ministers of Ukraine. (2015). *List of state property facilities of strategic importance for the national economy and security.* Resolution of the Cabinet of Ministers of Ukraine No 83, dated of 04.03.2015. Retrieved from: http://www.spfu.gov.ua/userfiles/files/postanova83.pdf.
4. Cabinet of Ministers of Ukraine. (2017). *Concept of creating the national system for critical infrastructure protecting.* Approved by the order of the Cabinet of Ministers of Ukraine No. 1009-p as of December 6, 2017. Retrieved from: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80.
5. Council Directive 2008/114/EC. (2008). *On the identification and designation of european critical infrastructures and the assessment of the need to improve their protection***.** Retrieved from: http://eur-lex.europa.eu/.
6. Critical Infrastructure Warning Information network – CIWIN. (2008). Retrieved from: http://ccpic.mai.gov.ro/ciwin_en.html.
7. Ministry of Infrastructure of Ukraine. (2011). *On approval of the Standard regulations on the Port's maritime security service.* Order of the Ministry of Infrastructure of Ukraine No. 339 dated August 25, 2011. Retrieved from : https://zakon.rada.gov.ua/laws/show/z1233-11.
8. Biryukov, D.S. (2015). Critical infrastructure protection of in Ukraine: from scientific understanding to the policy development. *Scientific and information Bulletin of the National Security Academy, 3-4 (7-8),* 155–170.
9. Blintsov, O. & Maidaniuk, P. (2017). Development of informationally-protected System of Marine Water Area Monitoring. *Eastern-European Journal of Enterprise Technologies*, 6/9(90), 10–16. DOI: 10.15587/1729-4061. 2017. 1188514.
10. *UK National Strategy for Maritime security.* (2014). 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.
11. *National Strategy for Maritime Security*. (2005). Retrieved from: https://georgewbush-whitehouse.archives.gov/homeland/maritime-security.html.
12. *National strategy for the security of maritime areas*. (2015). Retrieved from: https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2016/01/strategie_nationale_de_surete_des_espaces_maritimes_en_national_strategy_for_the_security_of_maritime_areas.pdf.
13. Combined Maritime Forces. (2019). Maritime Security Transit Corridor (MSTC). Retrieved from: https://combinedmaritimeforces.com/maritime-security-transit-corridor-mstc.
14. Thean Potgieter. (2012). *Maritime security in the Indian Ocean: strategic setting and features.* Institute for Security Studies, 236, 21 p. Retrieved from: https://www.africaportal.org/publications/maritime-security-in-the-indian-ocean-strategic-setting-and-features.
15. National Institute for strategic studies. (2014). *Green book on critical infrastructure protection in Ukraine (second version of the draft document*). Retrieved from: http://old2.niss.gov.ua/public/File/2014_table/1125_zelknuga.pdf.
16. Joseph Devine. (2008). *Project Management - A Systemic Approach.* Retrieved from: http://pdf2.hegoa.efaber.net/entry/content/966/Project_Management_-_A_Systemic_Approach.pdf.
17. Blintsov, V., & Hrytsaienko, M. (2016). Improvement of the management of material and technical resources of water cleaning projects from explosive objects. *Technology Audit and Production Reserves, 6/2 (32),* 51–56. Retrieved from: http://journals.uran.ua/tarp/article/view/86810/83010.
18. Dan Secrieru, Gheorghe Oaie, Vlad Radulescu, & Cristina Voicaru. (2015). *The Black Sea Security System – A New Early Warning and Environmental Monitoring system.* Retrieved from: https://www.springerprofessional.de/en/the-black-sea-security-system-a-new-early-warning-and-environmen/2276828.
19. Bushuev, S.D., Gogunsky, V.D., & Koshkin, K.V. (2012). Directions of dissertation research in the specialty "Project and program management". *Managing the development of complex systems. 12,* 5–7. Retrieved from: http://nbuv.gov.ua/UJRN/Urss_2012_12_3.

Блинцов Владимир Степанович; Blintsov Volodymyr, ORCID: https://orcid.org/0000-0002-3912-2174
Майданюк Павло Володимирович; Maidaniuk Pavlo, ORCID: http://orcid.org/0000-0002-1289-019X

Received October 29, 2019

Accepted November 28, 2019