Проаналізовано інформаційну складову системи моніторингу акваторій морських та приморських об'єктів. Визначено загрози для інформації, яка циркулює в різних середовищах функціонування систем моніторингу. Створено систему кількісних показників інформаційної безпеки об'єкту морської інфраструктури. Вона є основою для визначення рівня захищеності та ефективності заходів із захисту інформації в системі моніторингу морської акваторії

Ключові слова: захист інформації, моніторинг морської акваторії, мережа передачі даних, телекомунікаційна система

Проанализирована информационная составляющая системы мониторинга акваторий морских и приморских объектов. Определены угрозы для информации, которая циркулирует в различных средах функционирования систем мониторинга. Создана система количественных показателей информационной безопасности объекта морской инфраструктуры. Она является основой для определения уровня защищенности и эффективности мероприятий по защите информации в системе мониторинга морской акватории

Ключевые слова: защита информации, мониторинг морской акватории, сеть передачи данных, телекоммуникационная система

UDC 004.056: 654.9
DOI: 10.15587/1729-4061.2017.118851

DEVELOPMENT OF INFORMATIONALLY-PROTECTED SYSTEM OF MARINE WATER AREA MONITORING

O. Blintsov
Doctor of Tehcnical Sciences,
Associate Professor
Department of Electrical Equipment of
Ships and Information Security
Admiral Makarov National
University of Shipbuilding
Heroiv Ukrainy ave., 9, Mykolaiv, Ukraine, 54025
E-mail: alex_blintsov@ukr.net

P. Maidaniuk
State Service of Special Communication and
Information Protection of
Ukraine in Mykolaiv region
Spaska str., 32, Mykolaiv, Ukraine, 54001
E-mail: pashamaydanuk@gmail.com

1. Introduction

Ukraine is the country with a developed sea infrastructure with active economic activity. Modern terrorist threats require creation of a unified system of monitoring over over-water, underwater and air situation in marine waters of the state, which should be based on unmanned marine systems [1]. Such a system consists of remotely or software-driven underwater, over-water and air apparatus-robots that in real time provide information about the situation in the territorial waters of the state to the coastal center. A system of information security that circulates between the components of the monitoring system should be an integral part of the created new facilities of the marine infrastructure of informational character.

2. Literature review and problem statement

General issues in the field of information security were published in [2–5]. Works on the theory of State and law address exploration of the problems of legal provision of information security [6, 7]. These results are the basis for development of the systems, which provide for informational protection, however, the problems of information security in monitoring marine water areas require further research.

Paper [8] focuses on development and testing of autonomous over-water and underwater apparatus for problems of monitoring of marine waters. The results of application of autonomous underwater apparatus such as "glider" for monitoring the waters in the polar region are presented in [9]. The emphasis in these papers is placed on the use of specialized sensors, whereas the problems of data protection are not considered in these papers.

Analysis of the structures of unmanned over-water apparatus, designed for monitoring of the marine environment was made in [10]. However, the proposed structures do not contain a component, designed for information protection.

In [11], a new system of monitoring and prior notification of the environment for the Black Sea was developed. It includes five sea observatories and the coastal measuring station. The work contains a description of the composition of observatories and their operation procedure. Such a system provides for information exchange between distant elements, but the issue of information security is not tackled in this paper.

The issue of conceptualization of maritime security for energy transfer systems is explored in [12]. The composite index of maritime security with the equivalent weight indicator for calculation of vulnerability of marine security for 17 major marine routes was proposed. But application of unmanned marine systems in the problems of provision of maritime security was not explored in this research.

Research [13] is devoted to consideration of possibilities of unmanned air systems to fulfill the tasks of marine monitoring. Article [14] describes the areas of application of

unmanned air systems for execution of maritime operations. Paper [15] presents the "SEAGULL" project. Its purpose is to develop the intellectual system for monitoring marine environment based on unmanned flying vehicles. But application only of flying vehicles is insufficient for monitoring of underwater situation.

Analysis of the literature data showed that the theoretical issues of application of unmanned marine systems for monitoring of marine situation, as well as of information security have not been sufficiently developed so far. In particular, the presented results are focused either on monitoring of separate components of the environment, or on peculiarities of application of specialized sensors. The issue of monitoring of marine water areas with protection of information, which is generated, processed, transmitted and used in them, is not considered in complex statement.

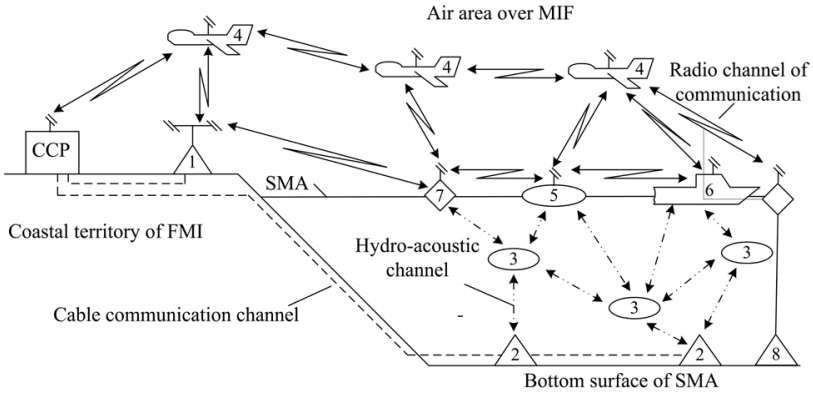

Fig. 1. Complex of hardware facilities for monitoring over-water, underwater and air situation of secure marine area: 1 — stationary ground-based monitoring facilities; 2 — stationary bottom-based monitoring facilities; 3 — unmanned underwater equipment; 4 — unmanned aerial vehicles; 5 — unmanned over-water equipment; 6 — crew-controlled ships; 7 — drifting buoys; 8 — stationary bottom-based monitoring facilities with radio channel

3. The aim and objectives of the study

The aim of present research is to develop a secure system for monitoring of the over-water, underwater and air situation at the facilities of marine infrastructure.

To accomplish the set goal, the following tasks were set:

– development of the structure and composition of the monitoring system;

– identification of threats and potential intruders for information, circulating in the system;

– statement of requirements for the methods and facilities of provision of information security for a monitoring system.

4. Materials and methods for development of a secure system of marine waters monitoring

4. 1. Structure and composition of informationally-protected system of marine waters monitoring

Interference into the processes of functioning of facilities of marine infrastructure (FMI) can lead to losses in the field of vital interests of an individual, society and the state, as well as to negative effect on the processes of natural or technogenic nature. Implementation of the threats is possible because of trespassing on a secure marine area (SMA), facilities, located on it, interception of information that circulates on FMI and (or) information about operation of facilities.

For monitoring marine, air and ground situation, it is proposed to use a complex of hardware facilities, presented in Fig. 1, at SMA and FMI.

The specified technical facilities are carriers of search and measuring equipment. They independently patrol the water area and the shore territory of the facility along previously planned routes, perform real-time radio-technical, radar, hydro-acoustic, magnet-metric and visually-optical monitoring of underwater, surface and air situation. Monitoring results are transmitted over secure channels to the waters' central control point (CCP).

The proposed FMI monitoring system is a distributed network, which includes the following components:

– access control sub-system (ACS) (electronic locks, turnstiles for provision of the regime of access to premises and land territories; booms barrages, electronic-optical, magnet-metric, seismic, radar, hydro-acoustic devices for water areas);

– subsystem of security alarm systems and video surveillance (CCTV, DVR, burglar alarm sensors for monitoring people staying within protected zone (inner perimeter of facilities), and within the controlled zone (water area and neighboring area);

– cable network (cables of communication and data transmission, power supply cables, grounding cables);

– network of wireless communication channels (Wi-Fi, radio relay stations, reception/transmission equipment);

– switching and routing data (switches, hubs, routers);

– automated workplaces (AWP) of system control, from which management, control, and tuning of the monitoring system are performed;

– AWP of databases (servers) to store (to archive) the data on operation of the monitoring system;

– hardware components of the system (unmanned submarine, surface, flying vehicles, stationary ground-based and underwater equipment).

An integral component of a secure monitoring system is the information-telecommunication network with the implemented complex information security system.

The proposed scheme of information-telecommunication network of the system of monitoring SMA and FMI is shown in Fig. 2.

In the proposed schematics for data transfer, it is possible to identify the following functional modules:

– module of information collection and processing – unmanned submarine, surface, flying vehicles, stationary ground- and underwater-based equipment ("subscribers");

– module of system control and data storage – AWP of system and the databases control that are located at the command point;

– module of communication – cable network, a system of wireless communication channels (radio channel, hydro-acoustic channel).

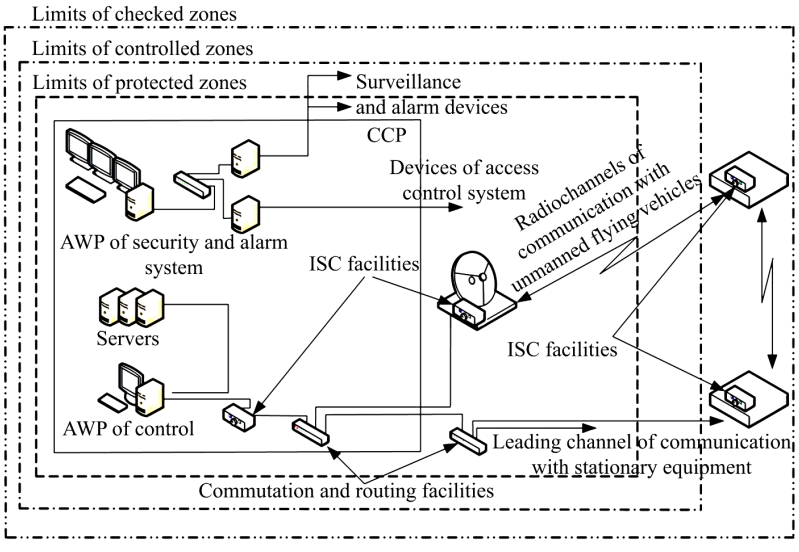

Fig. 2. Schematic of information-telecommunication network of monitoring system for marine infrastructure facilities

Telecommunication network of the system of SMA and FMI monitoring consists of interconnected cable and wireless communication channels, so in the process of data transmission, signals of messages are subject to different transformations during passing through different environments [2].

4. 2. Information security

The basis of information security in the system of SMA and FMI monitoring is a set of methods and facilities that provide integrity, confidentiality and availability of information that circulates in it.

Creation of a secure monitoring system (SMS) of marine situation with an implemented complex information security system allows solving the following problems, in particular:

– protection of information from leaking through technical channels;

– protection of information from unauthorized actions and unauthorized access;

– protection from special influence on information.

Accomplishment of the set goal implies solution of the following problems:

– determining of possible threats to information that circulates at SMA and FMI;

– development of the security system for information that circulates at SMA and FMI.

4. 3. Threats to information that circulates in a monitoring system

In the information and telecommunications systems (ITS) of monitoring of marine situation, there circulates the following information, which is subject to protection:

– data and program codes in the form of files of different formats that contain information that is subject to protection (information on results of monitoring of underwater, above-water and air environment);

– information about the state of the alarm system, video, hydro-acoustic and magnetometric surveillance and access control systems; algorithms and modes of operation of unmanned vehicles;

– orders of control of technical facilities and of the system and hardware facilities of monitoring and control;

– technological information which is used for provision of functioning of the system;

– files of the complex of information security facilities (crypto-algorithms, key data, system debugging parameters).

Threats to information that is processed in ITS depend on ITS characteristics, complexity of a system, the type of applied technical facilities, physical environment, staff, and other factors that may be of objective or subjective nature.

The main kinds of threats to information security that may occur in the ITS are:

– a change in conditions of physical environment (storm and seismic disturbances, smoke pollution of the atmosphere over SMA, changes in water transparency and its hydro-acoustic characteristics or other random events);

– faults and failures in operation of hardware facilities of monitoring system;

– errors of staff during operation of the monitoring system;

– intentional actions of potential intruders (information leakage due to: channels of outside electromagnetic radiation and guidance, unauthorized access, use of embedded devices, interception of information during transmission through communication channels, application of destructive software).

4. 4. Model of a intruder

For SMA and FMI, located on it, there are threat sources that can be caused by internal or external intruders in relation to the informationally secure monitoring system.

Internal intruders are the individuals who have the right of permanent access within the limit of the controlled zone of the water area (facilities), where the components of the monitoring system are located:

– technical staff that serves buildings, premises on the territory (water area), in which components of the system are located;

– the staff that serves technical facilities of the system (technicians, engineers);

– users (operators) of the monitoring system;

– officers of information security service in the system (administrators);

– heads of different levels of service hierarchy.

External intruders are individuals, who do not have the right of permanent access within the controlled zone of facilities, where components of the monitoring system are located:

– individuals, who are outside the controlled zone of facilities;

– visitors to facilities;

– representatives of organizations that interact on the issues of technical support;

– staff of foreign services or individuals acting on their tasks.

For each category of intruders, it is possible to distinguish five different specifications with definition of the level of potential threats (LT):

– by motives (irresponsibility (LT-1); insufficient professional qualification (LT 2); self-assertion (LT-3) self-serving interest (LT-4));

– by qualification level (knows functional features of the system, basic principles for collection, processing, storage and transmission of data in the system, has the skills of using standard facilities of the system (LT-1); has a high level of knowledge and practical skills for working with technical equipment of the system and its maintenance (LT-2); has a high level of knowledge in the field of programming and computer technology, design and operation of systems for data collection and transmission (LT-3); knows the structure, functions and mechanisms of operation of system security facilities and their shortcomings (LT-4));

– by the possibility to use facilities and methods for overcoming the protection system (uses only agent methods for obtaining information (LT-1); uses passive facilities (technical facilities of receiving information without modifying the system's components) (LT-2); uses only standard features and shortcomings of the security system for its overcoming (unauthorized actions using allowed facilities), as well as compact magnetic information carriers, which can be hidden from security guards (LT-3); applies methods and facilities of remote implementation of software bugs and special collection programs (LT-4));

– by duration of operation (before implementation of the monitoring system or its separate components (LT-1); during inactivity of the components of a system (during scheduled breaks in operation, interruptions for maintenance and repair, etc.) (LT-2) during operation of a monitoring system (LT-3); both during operation of a system and during maintenance of the components of a system (LT-4));

– by the place of operation (without access to the territory, buildings, structures, and facilities where components of a system are located (LT-1) on territories inside premises and buildings, where are the components of a system are located, but without access to the hardware of a system (LT-2), from workplaces of users (operators) of a system with access to databases and/or archives (LT-3); from workplaces of users (operators) with access to control of facilities for providing system's security (LT-4)).

Here, "LT" is a determined level of a threat, relative assessment of possible losses that may be caused by a intruder if there are relevant characteristics. The threat level is characterized by the following categories: 1 – insignificant, 2 – significant, but mostly permissible, 3 – medium, 4 – very significant.

Using designations of specification and threat levels, it is possible to determine the profiles of intruders (P) of different categories regarding effectiveness of realization of threats to a monitoring system at facilities of marine infrastructure, from the formula:

$$P_i = \frac{m + k + z + t + s}{5}, \quad (1)$$

where i is the category of an intruder; m is the LT value by specification "motive"; k is the LT values by the "level of qualification" specification; z is the LT level by specification "possibility of using facilities and methods of overcoming a security system"; t is the LT value by specification "duration of operation"; s is the LT value by specification "operation place".

Assessment is performed by the conditional scale from 1 to 4:

– 1 – threat realization is impossible;

– from 1 to – probability of threat realization is insignificant; its consequences can be neglected;

– from 2 to 3 – threat realization is possible, assessment of its consequences is necessary;

– from 3 to 4 – probability of threat realization and possible consequences are significant, additional measures regarding threat blocking are required

4. 5. Methods of protection of information that circulates in ITS of SMA and FMI monitoring

To protect information leakage through channels of outside electromagnetic radiation and guidance around the components of ITS of SMA and FMI, it is necessary to provide a controlled zone (CZ). The value of CZ should be obtained according to the results of instrumental check of electric and magnetic fields of scattering signals that carry information (dangerous signals) that emerge around the technical information processing facilities (IPF). In case of impossibility to provide the specified controlled zone (wires of a cable network, electric supply system, AWP of control and databases, stationary hardware and ground-based systems, transformation substations of power supply, grounding elements) around IPF and communication lines, it is necessary to use additional technical protection measures:

– active protection facilities (generators of electromagnetic interference, generators of artificial interference of electric supply lines, etc.);

– implementation of hardware components of an information system in a secure form (shielded cables and hardware cases, screened premises, shrouds, etc.).

For protection against unauthorized access (UAA) to the components of a system, organizational and security measures at SMA and FMI must be taken. To protect the system from implementation of special software and hardware facilities, allowing implementation of UAA and introduction of special software or hardware mechanisms that violate the structure and functions of the system, the policy of information security in the ITS, which is a complex of security measures, is implemented.

To protect information from leaking through communication channels, it is proposed to provide the controlled communication zone around communications in order to prevent unauthorized access to them and to take measures regarding information protection from leakage through technical channels:

– for the key channels of communication: using anti-interference filters, minimizing or excluding the common run of cables of the data transmission network with the lines that are going beyond CZ, application of shielded cables in a communication system; of communication;

– for the radio channels of communication: decreasing power of radio electronic facilities (REF), introduction of territorial, spatial, and time limitations for REF operation, application of modes of short-term radiation, creation of interferences, creation of false signals;

– for hydro-acoustic channels of communication: the use of natural and industrial hydro-acoustic interference, provision of the necessary level of disguise of hydro-acoustic interference, introduction of territorial, spatial, and time limitations on operation of facilities of hydro-acoustic radiation.

In addition to the use of organizational and technical security measures during transmission of information via communication channels, it is necessary to implement a system of cryptographic protection of information. It is essential to install the facilities of cryptographic transformation of information (facilities of through encryption of

traffic) of the appropriate access limit level, in hardware component of ITS (SPM control of the system and databases, unmanned submarine, over-water and flying vehicles, stationary ground-based and undersea-based equipment, monitoring and control facilities).

4. 7. Control over effectiveness of information security

Determining of efficiency of security of information that circulates on SMA and FMI is based on qualitative research into metrics that characterize the state of information security in different environments of its circulation. This will make it possible to determine the potential threats of information leakage, to carry out an assessment of effectiveness of information security by using calculation of the integral index of the state of information security at SMA and FMI.

The level of the state of information security at SMA and FMI is determined by assessing its major processes (stages) depending on the indicators of their metrics regarding determining of methods and measures to counteract certain threats. It will also help with determining of sufficiency of technical and organizational support, state and control over implementation of necessary measures, etc.

Formation of lists of information security metrics is based on selection of indicators that best characterize the state of information security at SMA and FMI, taking into account experience of evaluation of the state of technical and cryptographic information protection.

Normalization of information security metrics is carried out using a linear function so that characteristic values of indicators fall in the intervals, comparable by magnitude. Transition from absolute to normalized values of indicators allows measuring indicators by the scale from 0 to 1, or as a percentage, where 0 corresponds to 0 %, and 1 is 100 %.

Thus, the resulting normalized value of the indicator characterizes by its magnitude a degree of approximation to the highest value of 1.

By weight coefficient of the metrics, we imply the coefficient, defined by the method of expert estimations, which describes the amount of contribution of a specific security indicator into the integral index of the state of information security.

Calculation of integral indices of the state of information security is carried out separately for each environment of functioning of ITS components of the marine infrastructure facilities at all stages of the life cycle. After calculations of integral indices, the level of information security on the whole at SMA and FMI is calculated.

An example of formation of a set of security indicators (metrics), normalized values and weigh coefficients is shown in Table 1.

Calculation of the integral index of the state of information security of SMA and FMI is carried out based of the data obtained during the execution of works on development and implementation of information security measures.

Table 1

Example of creation of security indicators and weight coefficients

No.	Processes of information security control	Metrics (i)	Value of security metrics (n) 0...1	Weight coefficient of indicator (k)
1	Staff	Appointment of people in charge of organization of security measures	–	0.015
		.....		.....
		Personnel training (theoretical, practical trainings)	–	0.025
2	Planning	Identification of crucial information	–	0.02
		.....		.....
		Formulation of security requirements	–	0.04
3	Development	Determining of threat counteraction methods	–	0.03
		.....		.....
		Development of costs estimation documentation	–	0.015
4	Technical provision	Provision of necessary security facilities	–	0.1
		.....		.....
		Provision of necessary cryptographic facilities of information security	–	0.1
5	Organization provision	Security procedures are regulated by organizational and normative documents	–	0.04
		.....		.....
		The staff is acquainted with normative documents	–	0.05
6	State of implementation	Security measures are taken timely and fully	–	0.06
		.....		.....
		Cryptographic security measures are taken	–	0.06
7	Expert assessment	Effectiveness is proved by appropriate procedure	–	0.03
8	Internal audit	Control over security effectiveness is organized and permanently exercised	–	0.05

After introduction of the information security system, the integral index of the state of information security in each environment of components of information-telecommunication systems of SMA and FMI is calculated from the following formula:

$$Y_m = \sum_i n_{im} k_{im}, \quad (2)$$

where Y_m is the integral index of security state of the m-th operation environment; n_{im} is the normalized value of the i-th indicator of security of the m-th operation environment; k_{im} is the weight coefficient, determined by the method of expert assessment, which characterizes the amount of contribution of the i-th security indicator to the integral index of security state of the m-th operation environment.

Generalizing integral index of security state of ITS of SMA and FMI is calculated from the following formula:

$$Y = \sum_m \frac{Y_m}{m}, \quad (3)$$

where m is the number of operation environments

The level of information security state is determined by comparison of numeric values, derived with the help of calculation of summarizing integral index of information security state and characteristic values that diagnose the level of security state.

A range of values that diagnose the level of information security can be divided into the following intervals:

$$[Y_0, Y_{\text{unsat}}); [Y_{\text{unsat}}, Y_{\text{insec}}); \\ [Y_{\text{insec}}, Y_{\text{crit}}); [Y_{\text{crit}}, Y_{\text{sat}}); [Y_{\text{sat}}, Y_{\text{opt}}], \quad (4)$$

where Y_0 is the value of the integral index that characterizes absolutely insecure level of information security state – 0 % or 0; Y_{unsat} is the value that characterizes unsatisfactory level of information security state at the rate of 20 % or 0.2 of the optimal value; Y_{insec} is the value that characterizes insecure level of information security state at the rate of 40 % or 0.4 of the optimum value; Y_{crit} is the value that characterizes critical (minimal) level of information security state at the rate of 60 % or 0.6 of the optimal value; Y_{sat} is the value that characterizes satisfactory level of information security state at the rate of 80 % or 0.8 of the optimal value; Y_{opt} is the value that characterizes optimal level of information security state (100 % or 1).

6. Discussion of results of research into secure monitoring system

Implementation of secure systems for monitoring of marine, air and ground environment at the marine and coastal facilities will enable prevention of possible illegal (unwanted) actions of any nature. This is achieved by combining a complex of hardware facilities of environment monitoring into a single information and telecommunication system with a central control point.

A special feature of the developed system for SMA monitoring is protection of information that circulates in it. This significantly complicates any outside interference in functioning of the system's components and enhances reliability of a monitoring system as far as failures and false information imposition are concerned. Secure information and telecommunication networks of monitoring systems are promising for transmission of information with restricted access between correspondents within facilities or within SMA. In addition, universality of monitoring systems makes it possible to construct the system of facilities monitoring without substantial structural changes, regardless of the geographical features of SMA and FMI type. It offers the prospects for their wide application.

The advantage of the proposed secure monitoring system is the possibility of its application at industrial, transport, scientific research marine and coastal facilities and other FMI. It may be used by units of the border guard service and the armed forces of Ukraine as part of the border control system, for protection of military facilities, etc. In addition, proposed generalizing index of security state and the method of its calculation makes it possible to quantitatively assess the information security level in a monitoring system.

High cost of the hardware part of the system, in particular, unmanned submarine and flying vehicles can be mentioned as a drawback of this system. This disadvantage can be eliminated by organizing their mass production with wide implementation. In addition, quantitative assessment of security level is based on weight coefficients of indicators that are selected on the basis of expert evaluation. Development of a formal procedure for obtaining of these data would be desirable.

Development of the results, presented in this study, may involve step by step design (from the outline project to mass production) of a secure monitoring system for SMA or FMI with certain parameters. But at each stage, there possibly may arise the need to conduct analysis of threats and to refine the model of a intruder. It is proposed to adjust a technical task between the stages based on quantitative assessment of information security level in the monitoring system.

7. Conclusions

1. Based on analysis of conditions of functioning of the search and measuring equipment, the structure of the monitoring system for facilities of the marine infrastructure was proposed. Its specific feature is incorporation of a complex of hardware facilities of environment monitoring into a single information and telecommunication system with a central control point. Hardware monitoring facilities include unmanned underwater, over-water and aerial flying vehicles that provide monitoring of correspondent parts of the environment.

2. Based on analysis of the structure of a monitoring system, information that is processed and transmitted in it via communication channels, signals' distribution environment, the models of a intruder and threats for information circulating in the system were constructed.

3. Based on the results of assessment of information leakage channels and capacities of intruders, the methods for provision of information security of a monitoring system were selected. Their application provides protection against leakage through channels of outside electromagnetic radiation, from unauthorized access, leakage via communication channels, as well as cryptographic transformation of information. For quantitative estimation of the security level, a system of quantitative indicators (metrics) and the technique for calculation of generalizing index of security state was developed. Quantitative indicators are numerical characteristic of security state of separate individual information processes in the system, and the generalizing index allows us to determine (control) the level of information security provision.

References

1. Blintsov, V. S. Bezekipazhna viyskovo-morska tekhnika – stan ta osnashchennia VMS ZS Ukrainy [Text] / V. S. Blintsov, O. M. Kyryziuk, O. V. Krasnykh, S. V. Yakymiak // Nauka i oborona. – 2012. – Issue 4. – P. 61–64.
2. Lipkan, V. A. Informatsiyna bezpeka yak skladova natsionalnoi bezpeky Ukrainy [Text] / V. A. Lipkan // Informatsiyni tekhnolohiy v ekonomitsi, menedzhmenti i biznesi: Problemy nauky, praktyky i osvity. Zb. nauk. prats VIII Mizhnar. nauk.-prakt. konf. – Kyiv: Vyd-vo Yevrop. un-tu, 2003. – P. 443–453.
3. Pocheptsov, G. G. Kommunikativnye tekhnologii dvadtsatogo veka [Text] / G. G. Pocheptsov. – Moscow: Refl-buk; Kyiv: Vakler, 2000. – 352 p.
4. Kormych, V. A. Informatsiyna bezpeka Ukrainy: orhanizatsiyno-pravovi osnovy [Text]: navch. pos. / V. A. Kormych. – Kyiv: Kondor, 2004. – 384 p.
5. Dergausov, M. M. Ukraina – derzhava morskaya [Text] / M. M. Dergausov. – Donetsk: Izd-vo «Donechchina», 2000. – 269 p.
6. Rabynovych, P. M. Osnovy zahalnoi teoriy prava i derzhavy [Text]: pos. / P. M. Rabynovych. – Kyiv, 1994. – 236 p.
7. Kolodiy, A. M. Teoriya derzhavy ta prava [Text]: navch. pos. / A. M. Kolodiy, V. V. Kopeichykov, S. L. Lysenkov et. al.; S. L. Lysenkov, V. V. Kopeichykov (Eds.). – Kyiv: Yurinkom Inter, 2003. – 368 p.
8. Anderson, B. Autonomous Surface Vehicles for Arctic Data Collection [Text] / B. Anderson, A. Kleiner // OTC Arctic Technology Conference. – 2014. doi: 10.4043/24556-ms
9. Field, M. Barents Sea monitoring with a SEA EXPLORER glider [Text] / M. Field, L. Beguery, L. Oziel, J. C. Gascard // OCEANS 2015 – Genova. – 2015. doi: 10.1109/oceans-genova.2015.7271540
10. Heo, J. Analysis of Design Directions for Unmanned Surface Vehicles (USVs) [Text] / J. Heo, J. Kim, Y. Kwon // Journal of Computer and Communications. – 2017. – Vol. 05, Issue 07. – P. 92–100. doi: 10.4236/jcc.2017.57010
11. Secrieru, D. The Black Sea Security System – A New Early Warning and Environmental Monitoring System [Text] / D. Secrieru, G. Oaie, V. Radulescu, C. Voicaru // Sustainable Development of Sea-Corridors and Coastal Waters. – 2015. – P. 109–115. doi: 10.1007/978-3-319-11385-2_12
12. Kosai, S. Conceptualizing maritime security for energy transportation security [Text] / S. Kosai, H. Unesaki // Journal of Transportation Security. – 2016. – Vol. 9, Issue 3-4. – P. 175–190. doi: 10.1007/s12198-016-0173-2
13. Klimkowska, A. Possibilities of UAS for maritime monitoring [Text] / A. Klimkowska, I. Lee, K. Choi // ISPRS – International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences. – 2016. – Vol. XLI-B1. – P. 885–891. doi: 10.5194/isprsarchives-xli-b1-885-2016
14. De Sousa J. B. Unmanned Aircraft Systems for Maritime Operations [Text] / J. B. de Sousa, P. McGuillivary, J. Vicente, M. N. Bento, J. A. P. Morgado, M. M. Matos et. al. // Handbook of Unmanned Aerial Vehicles. – 2014. – P. 2787–2811. doi: 10.1007/978-90-481-9707-1_75
15. Marques, M. M. Unmanned aircraft systems in maritime operations: Challenges addressed in the scope of the SEAGULL project [Text] / M. M. Marques, P. Dias, N. P. Santos, V. Lobo, R. Batista, D. Salgueiro et. al. // OCEANS 2015 – Genova. – 2015. doi: 10.1109/oceans-genova.2015.7271427