UDC 656.614

DEVELOPMENT OF THE CONCEPT OF INFORMATION SECURITY ON VESSELS AND IN SEA TRANSPORT COMPANIES

Petrov I.M., D.Sc., professor, deep-sea Captain (NU "OMA")

It is known that a typical modern vessel uses a distributed network of connected and interacting electronic and computer devices that have access to the internet and provide settlement, navigation and repair operations, as well as data exchange with the external environment [1]. Examples of ship systems that are monitored and controlled through the use of information technology are: steering devices and propulsion, navigation aids, SPP service systems, ballast and fire protection systems. The processed results of measurement of parameters (rate, speed, temperature, pressure, consumption and quality of fuel and lubricants, etc.) are sent to storages and databases, and then transferred to shore services.

But at the same time, forms of unwanted, advertising and malicious software (SW) are being worked out and developed all over the world, which are integrated into the functioning of systems in order to intercept, steal and destroy valuable technical, economic and personal information. The most dangerous of these are the Trojan virus, publicity and disguise programs [2]. Examples include hacking attacks on Maersk systems in 2019, which resulted in a loss of about 300 million USA dollars. The company said that the NotPetya virus, which affected multinational companies, caused system interruptions that resulted in "significant business interruption" and prevented the processing of documentation for several days [3]. Also, there is a well-known incident with the hacking of data of the State Shipping Company of the Islamic Republic of Iran (IRISL) in 2011, in which the organization lost the available geolocation data for all 170 vessels, which also emphasizes the importance of the organization of information security (IS) [4].

Along with the development of harmful SW, new technologies are being created to organize the protection of confidential data. The most popular solutions in this area include data leakage prevention systems (DLP) and various methods of quantum cryptography. Work is underway in both the technical and legal segments, which is reflected in the improvement of domestic and foreign regulatory grounds. In particular, a number of legislative acts are being formed (Law of Ukraine of 05.10.2017 № 2163-VIII "On Basic Principles of Cyber Security of Ukraine", materials of the 40th session of the Committee FAL 39/WP.8, FAL 40/9, FAL 40/9/1, FAL 40/INF.5 and Resolution A.1098) on various aspects of the protection of sea transport networks from cyber threats. As an example of standardization of targeted and organizational measures to ensure IS, it should be noted the creation of BIMCO and ICS Union to combat cybercrime [5]. However, these solutions have a number of significant drawbacks. They are not universal and do not allow to take into account the specifics of various existing systems.

The analysis of the peculiarities of the data usage on vessels and in shore companies, as well as the existing precedents of hacking confirms the urgency of the problem of providing IS and developing new methods and models of secure access to these information resources.

It should be noted that the growing demands for IS form a stable trend, which consists of the systematic development of models for assessing the risks of hacking systems and requires those who make management decisions, develop and use the following actions to ensure information security:

- counteraction to threats of penetration into control units and modules of systems;
- organization of secure use of electronic information exchange subsystems;
- preventive assessment of the level of threats to the integrity, confidentiality and preservation of information used;
- encryption of transmitted data over open and closed communication channels.

The paper considers the analysis of IS threats to the service ergatic systems (SES), whose feasibility is eliminated with the help of a formalized discrete Harrison-Ruzzo-Ullmann (HRUA)

model. It is justified due to its simplicity, clarity and flexibility. This model was adapted to the specific conditions of SES operation and a concept was developed, which includes separate stages, including: preventive identification and formalization of the most critical and vulnerable components of systems, assessment and analysis of system hazard risks, development of threat and attack models, integration of data protection, adaptation and improvement of existing intelligent methods of cybersecurity to the specifics of a particular SES, the formation of an integrated indicator of the level of IS SES.

To adapt the formalized discretionary model HRUA for SES, we introduce the following notation:

- W_{sb} – many entities (sea agents, technicians, guest users) that provide access to SES;
- O_{ob} – a set of all possible objects to which the user of SES gets access, and each object with W_{sb} is a part of O_{ob};
- $A = \{A_1,\ldots, A_n\}$ – set of all possible access rights to SES (read – rd, write – wr, execution – ez, delete – del, save – sw, change – mod, create – cr, export – ex , search – sr);
- $S_{cn} = W_{sb} \times O_{ob} \times A$ – integral space of admissible states of SES;
- M_r – matrix of access rights, which allows you to display the ratio of current access rights of all eligible SES entities to its objects. The rows of the matrix correspond to the subjects, and the columns correspond to the objects;
- $M [w_{sb}, o_{ob}]$ – cell of the matrix of access rights to the SES, which contains a set of possible access rights of the selected subject of the SES to its object;
- $C = (W_{sb}, O_{ob}, M_r)$ – current state of the system.

The behavior of the system over time is expressed by transitions between all its possible states, which are carried out by adjusting the values of the matrix M_r by using commands of the conditional-production type:

The command ξ ($p_1,\ldots, p_k$) {If "A_1 is in the cell" $M [w_{sb1}, o_{ob1}]$) & (A_2 "is in the cell" $M [w_{sb2}, o_{ob2}]$) &… & An "is in the cell" $M [w_{sbn}, o_{obn}]$, then "execute" ($elp_1, elp_2,\ldots elp_n$), "fix state" ($T_{log}$),

where ξ is the name of the command used from the allowable set of size m, defined by the semantics of the system $S = \{\xi_1 (x_1, ..., x_k), \xi_2 (x_1, ..., x_k),\ldots, \xi_m (x_1, .. ., x_k)\}$.

p – input parameters of the command, which are unique identifiers of subjects and objects of SES.

elp – valid elementary operations:

- cns, <creation of a new subject W_{sb}>;
- cno, <create new object O_{ob}>;
- adso, <adding the subject W_{sb} rights in relation to the object O_{ob}>;
- chso, <change of the subject W_{sb} of the right in relation to the object O_{ob}>;
- dso, <removal of the right from the subject W_{sb} in relation to the object O_{ob}>;
- ds, <delete existing subject W_{sb}>;
- do, <delete existing subject O_{ob}>.

T_{log} – operation of creating an entry in the log pool of SES states in the format: "date-time-number-performed operations-current memory state-number of running processes". Braces are symbols of the beginning and end of the logical content of the command ξ.

Elementary operations elp_1 ... elp_n are implemented only if the entire list of conditions in the production unit <If ... Then>.

When describing the allowable elementary operations as a result of their implementation SES goes from state $C = (W_{sb}, O_{ob}, M_r)$ to state $C^{/} = (W^{/}_{sb}, O^{/}_{ob}, M^{/}_r)$. In fact, the adapted model taking into account the specifics of SES is based on the aggregation of subsets of triplets of the form {"subject"-"operation"-"object"}.

The behavior of the system over time is considered as a sequence of sets of states {C}, each subsequent state is the result of applying some command to the previous one: $C_{n+1} = S_n (C_n)$.

As an example of constructing an access matrix according to the adapted discretionary model of HRUA, we give the following example. Suppose a typical SES has 4 different entities:

1. W_{sb1} – SES administrator, has full-featured access rights to all objects of the system;

2. W_{sb2} – sea agent, which has the right to create, read, write, delete and modify data in a number of functional forms;

3. W_{sb3} – a technical specialist who has the right to read, change and write data only to the forms of assessment of technical condition in the operation of sea vehicles;

4. W_{sb4} – shipowner who has the right to read, search and export data in all forms.

Let there be 6 different objects of the system:

1. O_{ob1} – graphical form of accounting for financial and production applications;

2. O_{ob2} – window of information retrieval and reference support of the stages of agency maintenance of the vessel;

3. O_{ob3} – window for the formation and management of document flow;

4. Oo_{b4} – graphical form of display of current and normative operational technical characteristics of vessel systems components;

5. O_{ob5} – a form of viewing logs of user interaction with the system in command form;

6. O_{ob6} – a graphical form of viewing, searching and exporting data according to selected criteria for a specified period of time.

The formed matrix of access to SES according to the HRUA model is given in table. 1.

Table 1. The formed matrix of access to SES according to the HRUA

	Objects						
Subjects		O_{ob1}	O_{ob2}	O_{ob3}	O_{ob4}	O_{ob5}	O_{ob6}
	W_{sb1}	rd, wr, ez, del, sw, mod, cr, ex, sr	rd, wr, ez, del, sw, mod, cr, ex, sr	rd, wr, ez, del, sw, mod, cr, ex, sr	rd, wr, ez, del, sw, mod, cr, ex, sr	rd, wr, ez, del, sw, mod, cr, ex, sr	rd, wr, ez, del, sw, mod, cr, ex, sr
	W_{sb2}	rd, wr, sw, del, mod, sr, cr	rd, sr, sw, del	rd, wr, sw, del, mod, sr, cr			rd, sr, cr
	W_{sb3}				rd, mod, wr,		
	W_{sb4}	rd, sr, ex	rd, sr, ex	rd, sr, ex	rd, sr, ex	rd, sr, ex	rd, sr, ex

For a given SES, the initial state $C_0 = \{W_{sb0}, O_{ob0}, M_{r0}\}$ is safe with respect to the right A, if there is no sequence of commands applicable to C_0, as a result of which the right A will be entered in the cell of the matrix M, in which it was not in state C_0.

If the right A is found in the cell of the matrix M_r, in which it was originally absent, this is a clear sign of the leakage of the right A. This is a criterion for assessing the safety of SES in this adapted model of HRUA.

Due to the fact that SES implements the concept of "man-technical system", where the role of man is given the main place, to ensure a comprehensive approach to the analysis of the level of information security of the system it is necessary to assess the human factor. One of the promising areas of development of the proposed method is the development of unified mathematical models of threats that allow to take into account sets of heterogeneous factors and perform numerical assessment of key characteristics of IS SES (analysis and assessment of information risks, information security, effectiveness of preventive measures and others) [6, 7].

The developed concept of IS SES can be used as a basis for various information systems to support the functional activities of specialists not only in maritime agency of ships, but also in any segment of service activities in maritime transport.

REFERENCES

1. Kiberprestupnost v sudohodstve [Elektronnyiy resurs]. – Rezhim dostupa: http://interlegal.com.ua/ru/publikacii/kiberprestupnost_v_sudohodstve_i_ torgovlee _ mail_podpricelom/
2. Starovoytov A. V. Kiberbezopasnost kak aktualnaya problema sovremennosti / A.V. Starovoytov // Informatizatsiya i svyaz. – 2011. – № 6. – S. 4-7.
3. Informatsionnaya bezopasnost [Elektronnyiy resurs]. – Rezhim dostupa: https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/ printsip-raboty-dlp-sistemy/
4. Torskiy G.V. Kiberataki stoyat dorogo / V.G. Torskiy // Mezhdunarodnyiy morskoy zhurnal “Sea Review”.
5. Sokolov S.S. Tekhnycheskye y pravovyie aspektyi yspolzovanyia elektronno-tsyfrovoi podpysy y elektronnoho dokumentooborota s tseliu optymyzatsyy y povyishenyia effektyvnosty byznes-protsessov / S.S. Sokolov, A.S. Karpyna A.S. // Nauchnoe soobshchestvo XXI stoletyia. Tekhnycheskye nauky: sb. statei po materyalam XIX mezhd. nauch.-prakt. konf. − Novosybyrsk: SybAK. – 2014. – № 4 (19). – S. 50-56.
6. Shybanov H.P. Kolychestvennaia otsenka deiatelnosty cheloveka v systemakh chelovek-tekhnyka / H.P. Shybanov. − M.: Mashynostroenye, 1983. – 263.
7. Zyhel A. Modely hruppovoho povedenyia v systeme «chelovek-mashyna» / A. Zyhel, D. Volf. − M.: Myr, 1973. − 261 s.