Journal of Engineering Science *Vol. XXVII, no. 4 (2020), pp. 103 - 119*
Fascicle *Electronics and Computer Science* *ISSN 2587-3474*
Topic *Computers and Information Technology* *eISSN 2587-3482*

DOI: 10.5281/zenodo.4288297
CZU 004.056(478)

INFORMATICS SECURITY ASSESSMENT IN THE REPUBLIC OF MOLDOVA

Ion Bolun*, ORCID ID: 0000-0003-1961-7310,
Dumitru Ciorbă, ORCID ID: 0000-0002-3157-5072,
Aureliu Zgureanu, ORCID ID: 0000-0003-3301-2457,
Rodica Bulai, Rostislav Călin, Cristina Bodoga

Technical University of Moldova, 168, Stefan cel Mare bd., MD-2004, Chisinau, Republic of Moldova
*Corresponding author: Ion Bolun, *ion.bolun@isa.utm.md*

Received: 10. 05. 2020
Accepted: 11. 16. 2020

Abstract. The topicality of systemic research on informatics (IT) security in the Republic of Moldova is argued. Based on international practices, a set of 24 indicators (aspects) is defined for the incipient assessment of the state of informatics security in enterprises/organizations/institutions (EOIs). Through an online survey, the respective information is collected, EOIs being differentiated into 5 categories according to the number of employees, within each of which are distinguished ICT-EOIs and non-ICT-EOIs. The weighted average value of the percentage of EOIs (%EOI), of the percentage of ICT-EOIs (%ICT-EOIs) and of the percentage of non-ICT-EOIs (%non-ICT-EOIs) on 23 aspects of informatics security are: overall for EOIs - 71.7%, for ICT-EOIs - 73.3%, and for non-ICT-EOIs - 66.1%. The state of IT security of ICT-EOIs is better than that of non-ICT-EOIs. The biggest difference %ICT-EOIs – %non-ICT-EOIs is with reporting the IT security vulnerabilities of the implemented software, with performing the IT security audit of new IT applications/systems before implementation and with the implementing of an internal IT security policy. The dependence of the average value (on 23 aspects) of %EOIs on the number of employees is increasing. Moreover, the percentage of EOIs with 100% IT security performance for EOIs with over 500 employees is about twice as high (91.7%) as that for EOIs with up to 10 employees inclusive (43.8%).

Keywords: *enterprises/organizations/institutions, indicators, informatics security evaluation, informatics space, survey.*

1. Introduction

Information is a strategic resource. Many parts of it are confidential (personal data, commercial secret, state secret). E-commerce is widely used, various online financial transfers take place, etc. Unauthorized access to such information, but also massive, targeted (as the case may be) misinformation of the population, especially through the Internet, leads to considerable losses, slowing down the pace of economic growth and population welfare. Cybersecurity Ventures predicts cybercrime will cost the world in excess

of $6 trillion in 2021 [1] that is approx. 4% of global GDP. If in proportion to the global losses, then in the Republic of Moldova they will constitute, starting with 2021, over 8 billion MDL annually. iFrauds causes losses of 0.5-5% of the total expenditure of public institutions [2]. The survey in the field of informatics security (i-security), conducted in Moldova in 2017 [3], showed that all users who use informatics means need at least general knowledge in IT security.

At the same time, in the period 2005-2014, the share of group organized cyber-attacks increased four times, reaching approx. 80% of the total [4]. Respectively, cyber-attacks are becoming more sophisticated, and counteracting them - increasingly difficult, requiring deep knowledge and related research. Applying local security solutions only temporarily reduces the risks. Moreover, the appropriate solution implemented today may (in a relatively short time) become insufficient. The overall approach to IT security is required with dynamic adaptation to concrete situations.

There are relatively effective theoretical results and practical means of informatics security in the world. But the field is largely confidential, the exchange of information is restricted, often severely restricted, there are many cases of misinformation.

Ensuring i-security is very complex, multidimensional and long-term and requires considerable investment. In the conditions of an acute deficit of financial resources, characteristic to the Republic of Moldova, it is of paramount importance to support and promote the balanced development of areas that will subsequently ensure sufficiently fast (depending on the development phase) and massive (large enough) further actions related to i-security in support of economic growth in the republic.

The paper is intended for the incipient characterization of the informatics security state within some enterprises/organizations/institutions (EOIs) and, tangentially, in the Republic of Moldova as a whole.

2. General considerations regarding the evaluation of informatics security

Monitoring and evaluating the degree of society's i-security or related to it is done by a wide range of approaches and methodologies, which differs on the pursued aim or the ways of achieving it. However, all of these involve the use of a certain set of indicators, which essentially determines the specificity of each of them. At the same time, the quality of the evaluation depends substantially on the veracity of the primary information. That is why both the terms used and the respective indicators must be unequivocally defined.

It would be good if the aspects of i-security assessment were elucidated in detail on different categories of entities: public administration institutions, enterprises, organizations, economic activities and population. But such assessments would require considerable expenses. In conditions of very limited resources, it is reasonable to schedule work in time, starting from the highest priority ones. Of course, defining such priorities is still subjective.

For these reasons, research is currently focused on EOIs. Five categories of EOIs are defined according to the number of employees (very small - up to 10 employees, small - 11-50 employees, small-medium - 51-100 employees, medium - 101-500 employees and large - over 500 employees), and each of them distinguishes between ICT-EOIs (EOIs related to Information and Communication Technologies sector - ICT) and non-ICT-EOIs (EOIs not-related to ICT sector). So, in total there are 10 categories of EOIs.

When defining the respective set of indicators, **international practice in the field** is of great importance. The research of methodologies, related to the monitoring and evaluation of i-security state, highlights a wide diversity of approaches. Each of these methodologies is

aimed at determining or estimating the values of some indicators. Indicators can be primary or synthetic, composite (calculated based on several primary indicators), sometimes called indices. The set of indicators used depends on the purpose pursued. Gradually, with the progress made in advancing to the Information Society, methodologies for assessing information security are proposed, estimating the achievement of established objectives, the degree of coverage with specific technologies and tools of activities in various spheres of society and especially the afferent impact. This is eloquently seen in the eEurope 2002 [5], eEurope 2002+, eEurope 2005 [6], i2010 [7], Horizon 2020 [8] and Digital Europe 2021-2027 [9] programs. The first global index to assess the ability to withstand cyber-attacks and deploy the necessary IT infrastructure is the Cyber Power Index (CPI), proposed by Booz Allen Hamilton in 2011 [10]. The evaluation is based on 39 indicators.

Although evaluation methodologies are ultimately citizen-oriented, both the emphasis and the degree of detail of the set of indicators differ, often considerably. Moreover, sometimes even the sets of indicators used for the same purposes, but taking into account the new realities, are subject to change over time. For example, if for the eEurope2005 Program [5], approved in 2002, the focus was on some indicators, then in the i2010 Program [1], approved in 2005, the focus is largely on other indicators, including the new ones. Some characteristics of the various methodologies for assessing the IT security or directly related to it, approved or recommended by international bodies or related companies/organizations, are systematized in Table 1 [11].

Table 1

Destination and number of indicators used in some programs and methodologies

Index/methodology/ program	Destination	Basing organi-zation/year	Number of indicators
Global Cybersecurity Index (GCI) [12]	Commitment of countries to cybersecurity at a global level	ITU/2013	25
Cyber Readiness Index (CRI) [13]	Assessing countries' maturity and commitment to information security	Hathaway Global Strategies LLC/ 2013	70
National Cyber Security Index (NCSI) [14]	Measures the preparedness of countries to prevent cyber threats and manage cyber incidents	e-Governance Academy/2016	46
Cyber Power Index (CPI) [10]	Ability to withstand cyber-attacks and to deploy the necessary digital infrastructure	Booz Allen Hamilton/2011	39
Information security indicators (ISI) [15]	Assessing security controls level of enforcement and effectiveness	ETSI/2013	97
CIS security metrics [16]	Collection and analysis of data related to the performance and results of security processes	CIS/2010	28
CIS Controls [17]	Identifying and mitigating the consequences of cyber-attacks on computer systems and networks	CIS/2015 (v.6)	171

Continuation Table 1

E-Europe 2005 Programme: Category I [6]	Experience and use by Internet users of computer security means	UE/2002	5
i2010 Programme: Groupe III [7]	Experience and use of computer security means	EU/2005	survey
Digital Agenda for Europe 2020 [18]	Stimulating the digital economy and addressing societal challenges through ICT	EU/2010	
Horizon 2020: Secure Societies Challenge [8]	European attitudes towards cyber security	EU/2013	
Digital Europe 2021-2027: Information Security [9]	Strengthening the security capabilities of networks and information systems	EU/2019	

The paper [11] describes in more detail the indices, methodologies, and programs mentioned in Table 1. In the **Republic of Moldova**, out of the multitude of evaluations regarding the informatization of society, few refer directly to informatics security (Table 2, [11]). It should be noted that, unlike the indicators of the "Electronic Moldova" [19] and "Digital Moldova 2020" strategies [20], the 17 indicators of the "Cyber Security Program" 2016-2020 [21] refer to the monitoring and evaluation of the policy documents in the field of information security implementation and not to the assess of i-security degree achieved as a result of implementing the program actions.

Moreover, according to art. 37 of the Concept of information security of the Republic of Moldova [23], until December 21, 2017 at the national level no complex cyber security audit processes were performed, nor are there any studies or reports that would reflect in detail the situation regarding cybercrime (cyber risks and threats, cyber-attacks and incidents, other events in cyberspace), as well as the number of victims and the amount of its economic damage. The only official sources of statistical data on cybercrime are the Register of Crimes, Criminal Cases, Criminals and Crime Materials, held by the Ministry of Internal Affairs and the Informatics system „Criminal investigation: E-case", managed by the General Prosecutor's Office.

Table 2

About i-security indicators used in some documents in the Republic of Moldova

Index/methodology/program	Destination	Basing organization/year	Number of indicators
National strategy for building the information society „Electronic Moldova" [19]	Assessing the informatics security degree in the Republic of Moldova	Government of the Republic of Moldova/2005	3
National Strategy for developing the information society "Digital Moldova 2020" [20]	Assessing the security and trust degree in the digital space	Government of the Republic of Moldova /2013	4

Continuation Table 2

National cyber security program of the Republic of Moldova for the years 2016-2020 [21]	Monitoring and evaluating the implementation of the policy documents provided by the program	Government of the Republic of Moldova /2015	17
Erasmus+ project LMPI - N°573901-EPP-1-2016-1-IT-EPPKA2-CBHE-JP [3]	Identifying the target professions and training needs in the field of informatics security in Moldova	TUM,BARSU, SUM, AESM/ 2017	23 questions
The information security strategy of the Republic of Moldova for the years 2019-2024 [22]	Strengthening information security in the Republic of Moldova	The Republic of Moldova Parliament /2018	-

The survey (23 questions), realized in 2017 under the Erasmus+ LMPI project [3], was focused on identifying target professions and training needs in the field of information security in Moldova and not on assessing the degree of i-security in the republic.

Also, the annual statistical reports 1-inf (Situation on informatization and Internet connection) and 1-CE (Activity in the field of electronic communications) of the National Bureau of Statistics and the annual reports on the activity and evolution of ICT products and services market of the National Agency for Regulations in Electronic Communications and Information Technology do not contain indicators for assessing the degree of i-security in the republic.

Thus, at the moment, official statistical data that would reflect the degree of informatics security in the republic are not known. At the same time, the Republic of Moldova appears in some international evaluations in the field (Table 3).

Table 3

Republic of Moldova in international i-security rankings

No.	Index name	Total countries in the ranking	The Republic of Moldova place in the ranking
1	Global Cybersecurity Index, GCIv3, y. 2018/2019 [12]	175	53
2	Cyber Readiness Index, CRI 2.0, y. 2015 [13]	125	N/A
3	National Cyber Security Index – NCSI 2018 [14]	100	40
4	National Cyber Security Index – NCSI 2020 [14]	152	52

The data in Table 3 show a slightly more advanced degree of i-security of the Republic of Moldova than the international average.

3. Informatics security assessment indicators

Taking into account the international practice as well as that of the Republic of Moldova and also the fact that the research does not pursue the purpose of general characterization, covering all the aspects related to the IT security of the organization (see s. 2), in evaluations, for the 10 categories of EOIs, as criteria are used 23 aspects of i-

security performance listed in Table 4 and also the indicator 27 - „The time that has passed since the last i-security audit of the EOI informatics space".

Table 4

The names of 23 aspects of 100% EOI i-security performance

No.	Criterion (aspect)
3	EOI has implemented an internal informatics security policy
4	EOI has implemented internal informatics security standards (regulations)
5	EOI has a recovery plan in case of informatics security incidents
6	EOI has a subdivision or authorized person responsible for i-security
7	EOI uses, in sensitive cases, secure dedicated computers (stations)
8	EOI uses dedicated VLANs (virtual local area networks)
9	EOI uses VPNs (virtual private networks)
10	EOI uses firewalls
11	In EOI, non-Web sensitive files, including logs, are secured
12	In EOI, the informatics security audit of the new informatics applications/systems before implementation is provided
13	In EOI, backups of sensitive information on secure servers are automatically created
14	In EOI, IDS/WIDS at all perimeter nodes of the network are used
15	In EOI, IPS/WIPS at all perimeter nodes of the network are used
16	In EOI, access to resources is regulated
17	In EOI, sufficient complexity and regular updating of user account passwords is automatically checked
18,19	All EOI-owned websites are secure (https)
20	In EOI, centrally managed anti-malicious software is used
21	In EOI, the inventory and periodic scanning of the informatics security of network's perimeter nodes is performed
22	In EOI, external and internal penetration are tested to identify vulnerabilities and attack vectors
23	In EOI, the security vulnerabilities of the implemented software are reported
24	In EOI, informatics security incidents are noted
25	In EOI, employees are informed about the implications of informatics security, including possible malicious programs
26	In EOI, the informatics security audit of the informatics space as a whole is performed

4. Organizing and participating in data collection

Evaluation data are collected by sampling. A questionnaire, based on the set of indicators described in s. 3, is used for the survey. The questionnaire contains 28 questions, the last one referring to contact information. There are 4 open questions and 24 questions with only one option to select, of which:

1) 18 questions (in Table 4 numbered 5-13, 16, 17 and 20-26) with 2 options;
2) 5 questions (in Table 4 numbered 3, 4, 14, 15 and (18, 19)) with 3 options;
3) 1 question (indicator 27) with 5 options.

Taking this into account, 23 aspects (criteria) of i-security with two or three answer options (aspects 3-26) and separately aspect 27 are investigated in calculations. In case of the five aspects of i-security performance with the selection of one of three alternatives, the performance may be '0%', 'v100%' (greater than 0% but less than 100%) and '100%'. Namely, for the case of 100% EOIs i-security performance, the names of the 23 aspects are defined in Table 4.

Taking into account the SARS-CoV-2 alert situation in the Republic of Moldova during the reference period, the online collection of information was organized for the survey. For this purpose, the questionnaire was placed on the Internet in Microsoft Forms.

The survey took place between May 25 and June 20, 2020. Totally, representatives of over 600 EOIs, including 12 banks, were contacted to complete the Questionnaire. Of them, 88 respondents completed the questionnaire. The participation in the survey of the EOIs representatives, classified in 10 categories, is given in Table 5.

Table 5

Participation in the survey of EOIs representatives

Number of employees in EOI	ICT-EOIs		Non-ICT-EOIs		Total EOIs			
	nr.	%	nr.	%	nr.	% ÎOI	% TIC	% non-TIC
< 11	14	20.6	1	5.0	15	17.0	93.3	6.7
11.-50	14	20.6	5	25.0	19	21.6	73.7	26.3
51-100	10	14.7	2	10.0	12	13.6	83.3	16.7
101-500	15	22.1	8	40.0	23	26.1	65.2	34.8
> 500	15	22.1	4	20.0	19	21.6	78.9	21.1
Total	**68**	**100**	**20**	**100**	**88**	**100**	**77.3**	**22.7**

According to Table 5, out of the 88 participating EOIs, 68 (77.3%) belong to the ICT sector (economic activity) (ICT-EOIs) and only 20 (22.7%) - to the other economic activities (non-ICT-EOIs). Also, the share of ICT-EOIs of different categories according to the number of employees is from 14.7% to 22.1% (it is of relatively uniform distribution), while for the non-ICT-EOIs the respective share is from 5.0% to 40.0% (it is of strongly uneven distribution). This may be due to more than three times the number of non-ICT-EOIs participating in the survey compared to ICT-EOIs. The biggest discrepancy is for EOIs with up to 10 employees (14 : 1 = 14), followed by EOIs with 51-100 employees (10 : 2 = 5).

5. The EOI informatics security status

Graphs of the dependence of ICT-EOIs (%ICT-EOIs) and non-ICT-EOIs (%non-ICT-EOIs) percentage, at 100% i-security performance, on aspects 3-26 (see Table 4), obtained basing on data from Annexes 9 and 10 of [11], are shown in Figure 1.

From Figure 1 it can be seen that the percentage in question varies from 33.8% to 94.1%. Namely, only at 33.8% of ICT-EOIs is ensured 100% i-security performance in terms of IPS/ WIPS use at all perimeter nodes of the EOI network (total EOIs, aspect 15, - 34.1%) and, likewise, the use of IDS/WIDS at all perimeter nodes of the EOI network (total EOIs, aspect 14, - 35.2%). These two aspects are critical (the least EOIs have 100% i-security performance) for both ICT-EOIs and non-ICT-EOIs. Also, the i-security audit of informatics space is performed only at about 46.6% of the EOIs.

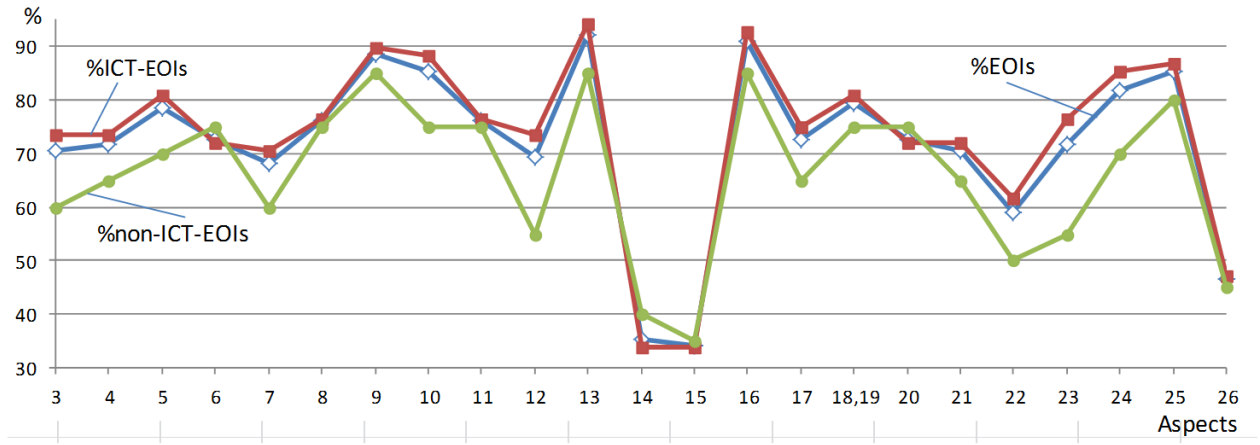

Figure 1. The %EOIs, %ICT-EOIs and %non-ICT-EOIs dependence on aspects 3 – 26 at 100% i-security performance.

A low degree of i-security is also in terms of testing external and internal penetration to identify vulnerabilities and attack vectors on the EOI informatics space (aspect 22 - 59.1%), the use, in sensitive cases, of secure dedicated computers (aspect 7 - 68.2%) and performing the informatics security audit of new informatics applications/systems before implementation (aspect 12 - 69.3%).

At the same time, the best situation regarding i-security is with the automatic creation of backups of sensitive information on secure servers (aspect 13 - 92.0%). A relatively high degree of i-security is also in terms of regulating access to resources (aspect 16 - 90.0%), the use of VPN (aspect 9 - 88.6%), the use of firewalls (aspect 10 - 85.2%) and informing employees about the implications of informatics security, including possible malicious software (aspect 25 - 85.2%).

Also, the unweighted average value of %EOI, %ICT-EOIs and %non-ICT-EOIs on the 23 i-security aspects constitutes:

- for EOI - 71.7%;
- for ICT-EOIs - 73.3%;
- for non-ICT-EOIs - 66.1%.

Of course, the 23 i-security aspects are, as a rule, of different importance - importance that may vary at different EOIs even in terms of one and the same aspect. At the same time, in comparative research, the unweighted use of the values of researched indicators puts in relatively equal situations the compared EOIs categories. Thus, the average degree of EOIs i-security (based on the 23 aspects) is about 71.7%; that is, in 71.7% of cases regarding the 23 aspects, the 100% i-security performance is ensured. Respectively, for ICT-EOIs it is about 73.3% of cases, and for non-ICT-EOIs - of 66.1%.

For a more detailed comparison, in Figure 2 is given the graph of the difference %ICT-EOIs – %non-ICT-EOIs dependence, at the 100% i-security performance, on aspects 3-26. As expected, from Figures 1 and 2 it can be seen that the state of i-security in ICT-EOIs is better than in the non-ICT-EOIs. The biggest difference %ICT-EOIs – %non-ICT-EOIs is with the reporting of i-security vulnerabilities of the implemented software (aspect 23), performing i-security audit of new informatics applications/systems before implementation (aspect 12) and the implementation of an internal i-security policy (aspect 3). The unweighted average value of the difference %ICT-EOIs – %non-ICT-EOIs on the 23 i-security aspects is 7.3%.

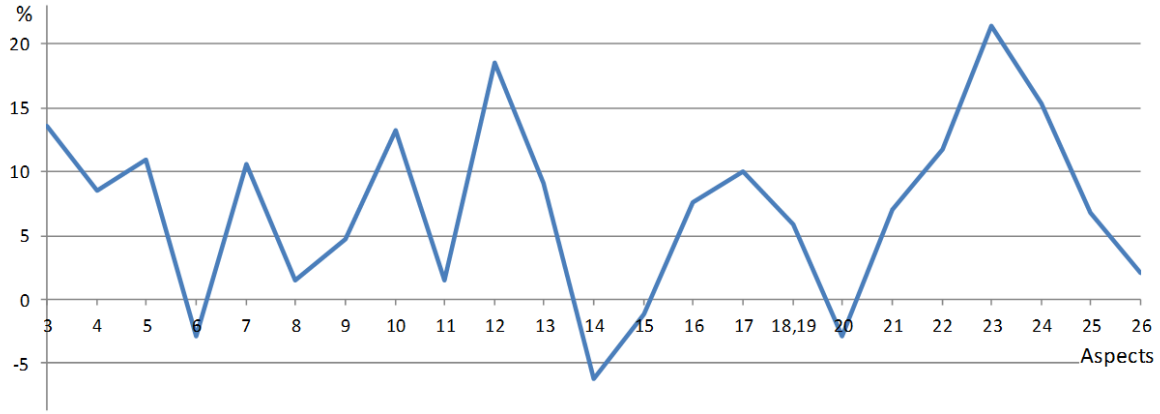

Figure 2. Difference %ICT-EOIs - %non - ICT-EOIs dependence on aspects 3 – 26 at 100% i-security performance.

Moreover, it can be stated with certainty that the situation with i-security at non-ICT-EOIs is weaker than that shown in Figures 1 and 2, that is on average the difference in question is greater than 7.3%. As arguments for such a statement could be:

1) the small number of non-ICT-EOIs that responded to the request to participate in the survey (only 20 non-ICT-EOIs), compared to the number of EOIs that the survey organizers addressed. Possibly, in some non-ICT-EOIs there was no one to fill in the questionnaire form knowingly;
2) participation in the survey of only one non-ICT-EOIs with a number of up to 11 employees (out of the 20, that is 5%), while ICT-EOIs with a number of up to 11 employees participated 14 (out of the 68, that is 20.6%). It is known (see also Figure 3) that the situation with i-security at EOIs with a small number of employees is weaker than at EOIs with a large number of employees;
3) participation in the survey of the National Bank of Moldova (non-ICT-EOI), whose informatics space is of a high level of i-security.

In order to identify the discrepancy of i-security performance between large EOIs (with more employees) and small EOIs (with fewer employees), the graph of %EOIs average value, on aspects 3 - 26, dependence on the number of employees (at 100% i-security performance) is constructed (see Figure 3).

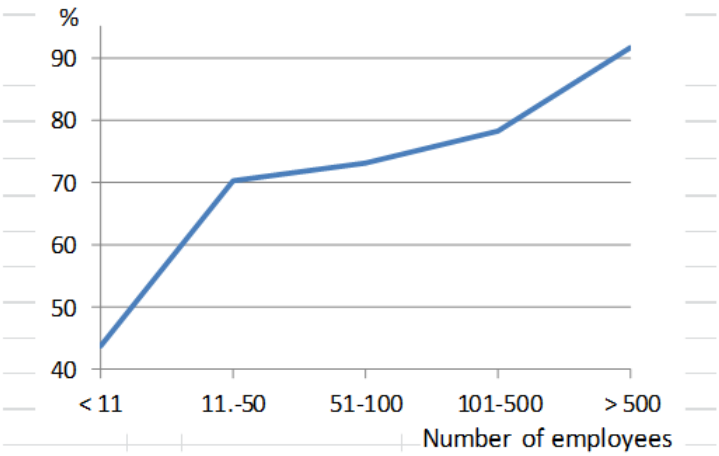

Figure 3. The %EOIs average value (on aspects 3 - 26) dependence on the number of employees at 100% i-security performance.

It can be seen that the %EOIs average value dependence, at i-security performance of 100%, on the number of employees is increasing. Moreover, the percentage of EOIs with 100% i-security performance for EOIs with over 500 employees is about twice as high (91.7%) as for EOIs with up to 10 employees (43.8%).

Of interest is the dependence on aspects 3 - 26 of %EOIs (at 100% i-security performance) by categories according to the number of employees. The respective graph is presented in Figure 4. It clearly shows the big difference between the i-security status of large EOIs (over 500 employees) and of the small ones (up to 10 employees inclusive) for each of the 23 aspects.

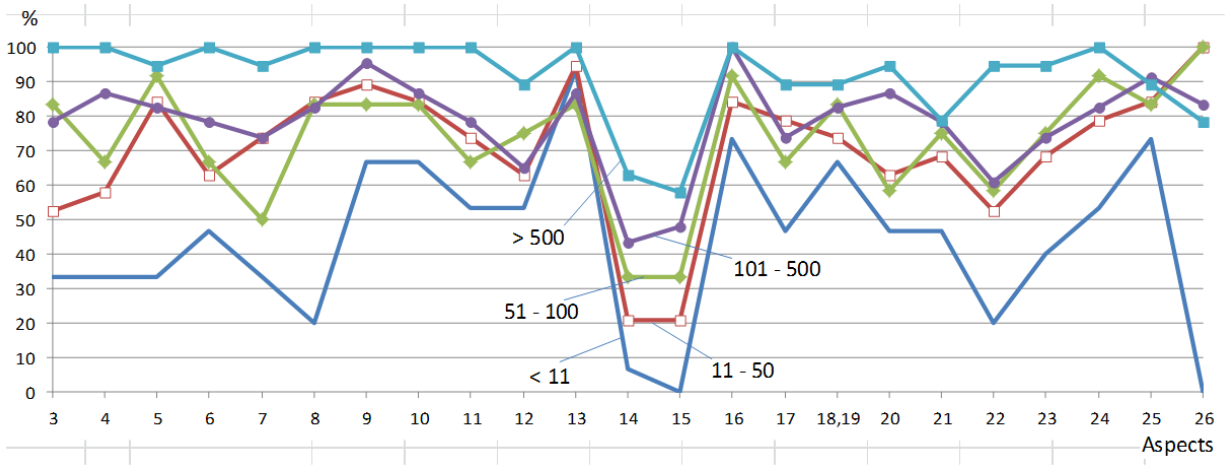

Figure 4. Dependence of %EOIs (at 100% i- security performance), by categories according to the number of employees, on aspects 3 – 26.

It should be noted that in case of EOIs with up to 10 employees, IPS/WIPS at all perimeter nodes of the corporate network are not used (aspect 15) nor is the i-security audit of the informatics space performed (aspect 26) in any EOI. Among these, the number of EOIs using IDS/WIDS at all perimeter nodes of the corporate network (aspect 14), using dedicated VLANs (aspect 8) and testing external and internal penetration to identify vulnerabilities and attack vectors (aspect 22) is also reduced. Moreover, few such EOIs have implemented an internal i-security policy (aspect 3), have implemented internal i-security regulations (aspect 4) and have a recovery plan in case of i-security incidents (aspect 5).

Significantly better than at EOIs with up to 10 employees, is the state of i-security at EOIs with 11 to 50 employees.

However, only 20% of them use IDS/WIDS (aspect 14) and IPS/WIPS (aspect 15) at all perimeter nodes of the corporate network and only 52.6% of them have implemented an internal i-security policy (aspect 3) and tests external and internal penetration to identify vulnerabilities and attack vectors (aspect 22).

On the other hand, all EOIs with over 500 employees have 100% i-security performance in 10 aspects: 3, 4, 6, 8-11, 13, 16 and 24. But also in this category of EOIs, only 57.9 % EOIs use IPS/WIPS (aspect 15) and 63.2% EOIs use IDS/WIDS at all perimeter nodes of the network (aspect 14).

Also, about 78.6% of EOIs perform the i-security audit of the informatics space as a whole (aspect 26) and 78.9% of EOIs perform the periodic inventory and scan on i-security of the perimeter nodes of the network (aspect 21).

In the process of improvement is the state of i-security on aspects with three alternative answers, namely: 3, 4, 14, 15 and (18, 19).

That information can be found in Tables A10.3, A10.4, A10.14, A10.15 and A10.(18,19) of [11].

The results, obtained by adding the calculations for the alternative of full compliance with the i-security requirement (100%) and those for the alternative of partial compliance with the i-security requirement (greater than 0% but less than 100%) at each of these aspects, with the respective reformulations, are systemized in Tables 6 and 7.

In Table 6 EOIs are differentiated in ICT-EOIs and non-ICT-EOIs categories, and in Table 7 the EOIs are differentiated in categories according to the number of employees.

Table 6

Features of aspects with three alternative answers (EOIs, ICT-EOIs and non-ICT-EOIs)

No.	iSecurity aspect	Total EOIs		Total ICT-EOIs		Total non-ICT-EOIs	
		Answers	%	Answers	%	Answers	%
3	EOI has implemented or is implementing an internal i-security policy	78	88.6	60	88.2	18	90.0
4	EOI has implemented or is implementing internal i-security regulations	78	88.6	61	89.7	17	85.0
14	In EOI, IDS/WIDS are used on all or part of the perimeter nodes of the network	63	71.6	48	70.6	15	75.0
15	In EOI, IPS/WIPS are used on all or part of the perimeter nodes of the network	60	68.2	48	70.6	12	60.0
18,19	All or part of the EOI-owned websites are secure (https)	82	93.2	65	95.6	17	85.0

Using, for aspects 3, 4, 14, 15 and (18, 19), the data from Table 6 and, respectively, those from Table 7, and for the other aspects - the same data as those used to build the graphs in Figures 1 - 4, the dependencies shown in Figures 5-8 are obtained.

The direct comparison, in pairs, of the information in Figure 1 with that in Figure 5, in Figure 2 with that in Figure 6, in Figure 3 with that in Figure 7 and in Figure 4 with that in Figure 8 would not be correct. Figures 1-4 do not take into account the information regarding the partial observance of some i-security requirements, and in Figures 5 - 8 the v100% i-security performance is considered and not the 100% one.

However, the use of the information in Figures 5 - 8 (and in tables on which these figures are built) allows a broader characterization of the degree of EOIs i-security.

Table 7

Features of aspects with three alternative answers, EOIs by categories according to the number of employees

No.	iSecurity aspect	%EOI				
		< 11	11-50	51-100	101-500	> 500
3	EOI has implemented or is implementing an internal i-security policy	61.9	84.2	91.7	95.7	100.0
4	EOI has implemented or is implementing internal i-security regulations	66.7	78.9	91.7	100.0	100.0
14	In EOI, IDS/WIDS are used on all or part of the perimeter nodes of the network	33.3	63.2	58.3	87.0	100.0
15	In EOI, IPS/WIPS are used on all or part of the perimeter nodes of the network	33.3	68.4	58.3	73.9	94.7
18,19	All or part of the EOI-owned websites are secure (https)	86.7	89.5	100.0	95.7	94.7

Comparing Figure 5 with Figure 1, one can see a possible gradual improvement of the situation regarding the internal i-security policy (aspect 3), the use of IDS/WIDS at all perimeter nodes of EOI network (aspect 14) and the use of IPS/WIPS at all perimeter nodes of EOI network (aspect 15) - these are implemented in several EOIs. Moreover, in many EOIs some of the websites are, however, secure (aspect (18, 19)).

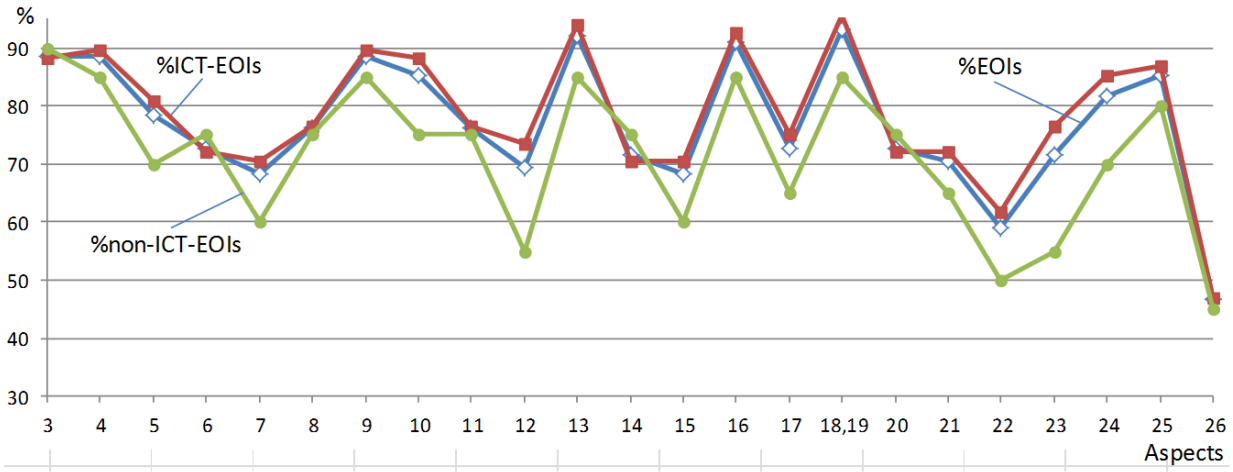

Figure 5. The %EOIs, % ICT-EOIs and %non-ICT-EOIs dependence on aspects 3 – 26 at v100% i-security performance.

Also, in the case of v100% i-security performance, the unweighted average value of %EOIs, %ICT-EOIs and %non-ICT-EOIs on the 23 aspects of i-security constitute:

- for EOIs - 76.9%, compared to 71.7% in the case of 100% performance;
- for ICT-EOIs - 78.5%, compared to 73,3% in the case of 100% performance;
- for ÎOI-non-TIC - 71.3%, compared to 66.1% in the case of 100% performance.

Thus, in 76.9% of cases regarding the 23 aspects, the v100% i-security performance is ensured. Respectively, for ICT-EOIs it is about 78.5% of cases, and for non-ICT-EOIs - 71.3% of cases.

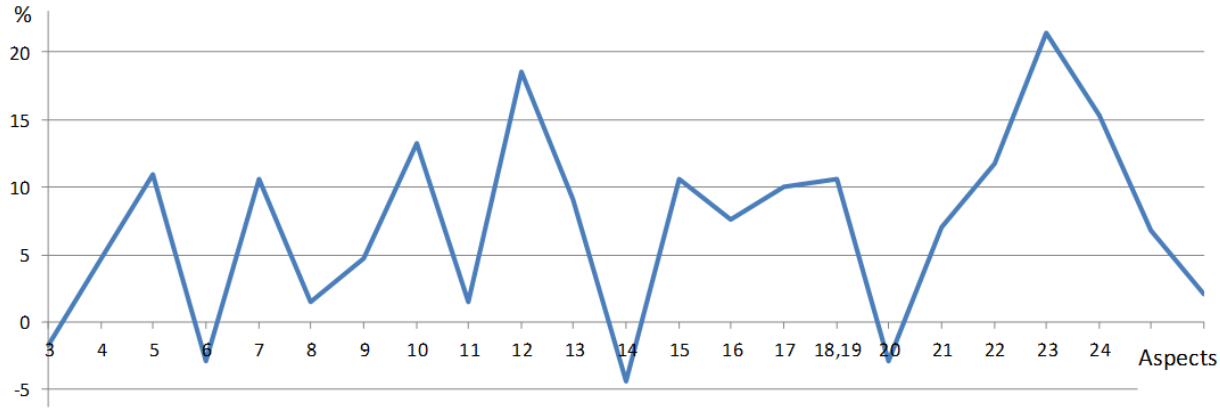

Figure 6. Difference „%ICT-EOIs – %non-ICT-EOIs dependence on aspects 3 – 26 at v100% i-security performance.

Figures 2 and 6 show a comparative improvement of non-ICT-EOIs i-security compared to that of ICT-EOIs on aspects 3 (EOI has implemented or is implementing an internal i-security policy) and 4 (IOI has implemented or is implementing internal i-security standards/regulations) and, conversely, a comparative improvement of ICT-EOIs i-security compared to that of non-ICT-EOIs in terms of aspects 14 (IDS/WIDS are used in all or part of the perimeter nodes of the EOI network) and 15 (IPS/WIPS are used in all or part of the perimeter nodes of the EOI network) and (18,19) - all or part of the EOI-owned websites are secure (https). However, the weighted average value of the difference %ICT-EOIs – %non-ICT-EOIs on the 23 aspects at v100% i-security performance is 7.2% that is approximately the same as at 100% i-security performance.

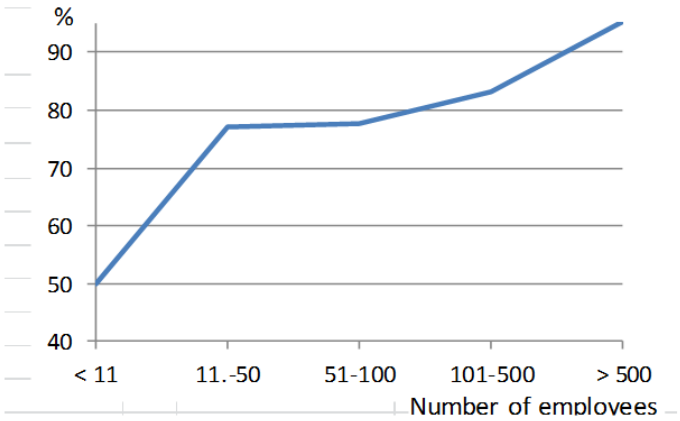

Figure 7. The %EOIs average value (on aspects 3 - 26) dependence on the number of employees at v100% i-security performance.

Data in Figure 7 show that the dependence of %EOIs average value, on aspects 3-26, to the number of employees at v100% i-security performance is increasing, as in the case of 100% i-security performance (see Figure 3), but the difference between the categories of EOIs with 11-50 employees and with 51-100 employees has been considerably reduced - this is only 0.4%.

Also, the %EOIs by categories (according to the number of employees) dependence on aspects 3-26 at v100% i-security performance has usually become closer between different categories. This is also explained by the fact that the possible improvement of i-security is limited from above by the 100% maximum possible. Thus, the difference

between the average of EOIs category with over 500 employees and that of EOIs category with up to 10 employees is of 48.0% according to Figure 3 and of 45.2% according to Figure 7. This situation is also observed when comparing data of Figure 4 with those of Figure 8.

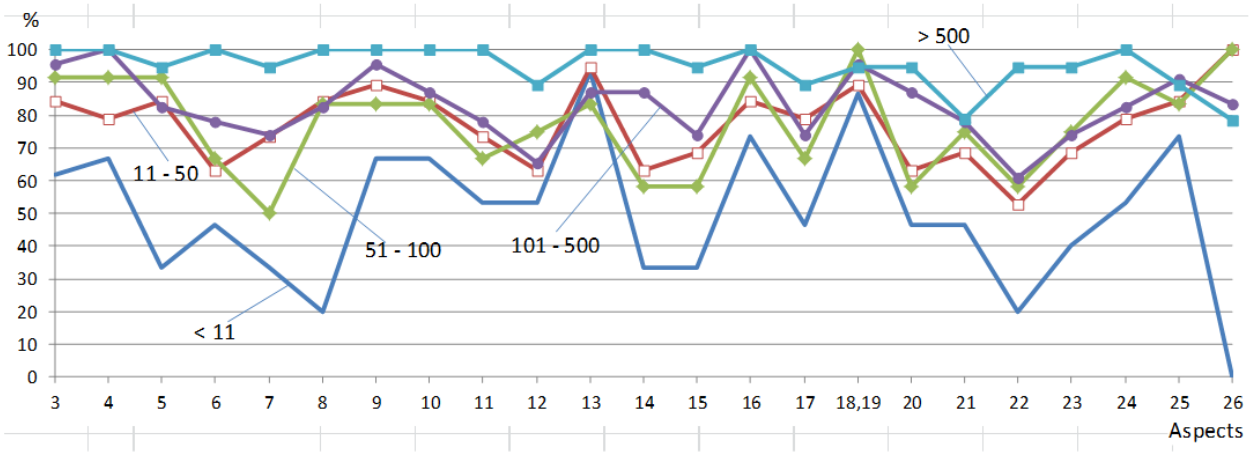

Figure 8. Dependence of % EOIs (at v100% i-security performance), by categories according to the number of employees, on aspects 3 – 26.

In the case of v100% i-security performance, things seem to be improving, but according to Figures 4 and 8 there is still a big difference for 21 of the 23 aspects of i-security between EOIs with up to 10 employees and that of EOIs of other categories. However, some EOIs with up to 10 employees are in a position to implement the internal i-security policy (aspect 3) and the internal i-security standards (regulations) (aspect 4) and also IDS/WIDS (aspect 14) and IPS/WIPS (aspect 15) are implemented at a part of corporate network perimeter nodes. Nevertheless, none of such EOIs performs the IT security audit of their own informatics space (issue 26).

It should also be noted that to the 10 aspects, to which EOIs with over 500 employees have a 100% i-security performance (3, 4, 6, 8 - 11, 13, 16 and 24), the aspect 14 is added, to which such EOIs have v100% i-security performance.

Regarding the i-security criterion 27 (time elapsed since the last IT security audit) - the representatives of 41 EOIs, where the i-security audit of the informatics space was done, marked it. The calculation results for this criterion are given in the Table 8.

Table 8

Time elapsed since the last i-security audit of EOIs informatics space

No. of employees	ICT-EOIs				Non-ICT-EOIs				Total EOIs			
	⩽ 1 year		> 1 year		⩽ 1 year		> 1 year		⩽ 1 year		> 1 year	
	no.	%	no.	%	no.	%	no.	%	no.	%	no.	%
< 11	0	0	1	100	0	0	0	0	0	0	1	100
11-50	5	100	0	0	4	100	0	0	9	100	0	0
51-100	5	100	0	0	0	0	0	0	5	100	0	0
101-500	8	80.0	2	20.0	2	100	0	0	10	83.3	2	16.7
> 500	8	72.7	3	27.3	3	100	0	0	11	78.6	3	21.4
Total	26	81.3	6	18.8	9	100	0	0.0	35	85.4	6	14.6

Of the 41 EOIs, where the informatics space i-security audit took place, 32 are ICT-EOIs and 9 are non-ICT-EOIs. Thus, the ratio between ICT-EOIs and non-ICT-EOIs for these

41 EOIs is approximately the same as in the case of the all 88 EOIs: 32 : 9 = 3.(5) and 68 : 20 = 3.4.

At the same time, if in the case of non-ICT-EOIs for all of them the time elapsed since the last i-security audit of the informatics space does not exceed 1 year, then in the case of ICT-EOIs the time in question does not exceed 1 year for only 26 EOIs (81.3%). So, non-ICT-EOIs, having, on average, a lower degree of i-security than ICT-EOIs, take a greater care in conducting the i-security audit.

At the same time, small ICT-EOIs may often be able to assess the security of their own informatics space without a dedicated audit.

6. Conclusions

At the national level, several laws and decisions of the Parliament and decisions of the Government of the Republic of Moldova, some of which are listed in Annex 9 of [11], provide the legal and normative framework in the field of informatics security. Within them are approved the "National Cyber Security Program of the Republic of Moldova for the years 2016-2020" [21], the Information Security Strategy of the Republic of Moldova for the years 2019–2024 [22] and others.

Also, as standards for the Republic of Moldova, 214 international and European standards on data processing, storage, secure access, security of informatics systems, electronic communications systems, etc. were adopted, including 22 ISO standards and 15 ETSI standards related to "Cyber security".

Regarding the monitoring of informatics security at national level, the situation is less gratifying: few of the many assessments conducted on the informatization of society in the republic relate directly to informatics security. At present, official statistics that would reflect the degree of computer security at the national level are not known.

At the same time, the Republic of Moldova appears in some international assessments in the field, which show a degree of its i-security a little more advanced than the world average.

Based on an online survey, some features of i-security state within EOIs are determined. For the case of 100% i-security performance, the average degree of EOIs i-security is about 71.7%; that is, within 71.7% of the EOIs, the 100% i-security performance is ensured regarding the 23 aspects. Respectively, for ICT-EOIs it is about 73.3% of cases, and for non-ICT-EOIs - of 66.1% of cases. The average degree of EOIs i-security is increasing compared to their size (number of employees), being, for example, 43.8% for EOIs with up to 10 employees and of 91.7% for IOIs with more than 500 employees.

Of the 23 aspects of i-security, the automatic creation of backups of sensitive information on secure servers is the best situation (92.0%).

A relatively high degree of i-security is also in terms of regulating access to resources (90.9%), the use of VPN (88.6%), the use of firewalls (85.2%) and informing employees about the implications of i-security, including possible malicious programs (aspect 25 - 85.2%).

At the same time, the use of IPS/WIPS and the use of IDS/WIDS at all perimeter nodes of the EOIs corporate network are in the worst situation (34.1% and 35.2% respectively). A low degree of i-security is also in terms of EOIs informatics space IT security auditing (46.6%), testing external and internal penetration to identify vulnerabilities and attack vectors on EOIs informatics space (59.1%), the use in sensitive cases of dedicated

secure computers (68.2%) and the performing of i-security audit of new applications/informatics systems before implementation (69.3%).

Regarding the case of v100% i-security performance, the average degree of EOIs i-security is about 76.9%, of ICT-EOIs - 78.5% and of non-ICT-EOIs - 71.3%. In reality, the average degree of non-ICT-EOIs i-security is probably much lower, intuiting that a large part of them, especially the small ones, did not participate in the survey, due to a low i-security.

Although the values of the v100% i-security performance indicators mean some improvement (present or expected in the not too far future) of the EOIs i-security, compared to those of the 100% i-security performance indicators, the overall state of i-security cannot be considered sufficient for the most of EOIs, including for reasons such as:

1) the 23 investigated i-security aspects do not cover a large part of the aspects i-security usually considered internationally (see, for example, Annexes 5 and 7 of [11]);
2) for a good part of the 23 aspects of i-security the degree of i-security is low;
3) cyber-attacks are intensifying and becoming more complex and aggressive; more and more often they are organized by groups of specialists [4], and sometimes even by state services [24].

References

1. 2019 Official Annual Cybercrime Report. Cybersecurity Ventures, 2019. https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf (accessed 24.04.2020).
2. Guide to Understanding the Total Impact of Fraud, February 2020. International Public Sector Fraud Forum. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866608/2377_The_Impact_of_Fraud_AW__4_.pdf (accessed 12.02.2020).
3. Bolun I., Beșliu V., Rusu G., Negară C. Sondaj de identificare a profesiilor țintă și a nevoilor de instruire în domeniul securității informatice în Moldova. Chișinău, 2017. https://www.lmpi-erasmus.net/en/project.aspx (accessed 24.05.2020). (Romanian)
4. Ablon L., Libicki M.C., Galay. A. Markets for Cybercrime Tools and Stolen Information: Hackers' Bazaar. Rand Corporation. 2014.
5. eEurope 2002-An Information Society for All. Council of the European Union and European Commssion, June 2000.
6. E-Europe 2005: An information society for all. Brussels, 28.5.2002, COM(2002) 263 final. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2002:0263:FIN:EN:PDF ((accessed 24.04.2020).
7. i2010. The User Challenge Benchmarking The Supply Of Online Public Services. 7th Measurement. European Commission. Directorate General Information Society and Media, September 2007.
8. Horizon2020 - The EU Framework Programme for Research and Innovation. European Commission, 2013. https://trimis.ec.europa.eu/programme/horizon2020-eu-framework-programme-research-and-innovation (accessed 24.02.2020).
9. Digital Europe 2021-2027. European Commission, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A434%3AFIN (accesed 26.02.2020).
10. Cyber Power Index: Findings and Methodology. Booz Allen Hamilton, 2011. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf (accessed 12.03.2020).
11. Bolun, I., Ciorbă, D., Zgureanu, A., Bulai, R., Călin, R., Bodoga, C. Starea, necesitățile și prioritățile securității informatice în Republica Moldova. Chișinău: UTM, 2020. (Romanian)
12. Global Cybersecurity Index 2018. ITU, 2019. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (accessed 15.02.2020).
13. Hathaway, Melisa; Demchak, Chris, Kerben, Jason et all. Cyber Readiness Index 2.0. Potomac Institute for Policy Studies, 2015. https://www.potomacinstitute.org/images/ CRIndex2.0.pdf (accessed 16.02.2020).

14. National Cyber Security Index. Tallin: eGovernance Academy, 2019. ahttps://ncsi.ega.ee/ methodology/ (accessed 14.02.2020).
15. ETSI GS ISI 001-1 V1.1.1 (2013-04) Information Security Indicators. ETSI, 2013. https://www.etsi.org/deliver/etsi_gs/ISI/001_099/00101/01.01.01_60/gs_isi00101v010101p.pdf (accessed 21.02.2020).
16. CIS security metricks. Center for Internet Security, 2010. http://www.itsecure.hu/library/image/CIS_Security_Metrics-Quick_Start_Guide_v1.0.0.pdf (accessed 23.02.2020).
17. CIS Controls v. 7.1 Measures and Metrics. Center for Internet Security, 2019. https://www.cisecurity.org/white-papers/cis-controls-v7-measures-metrics/ (accessed 24.02.2020).
18. Digital Agenda for Europe 2020. https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52010DC0245 (accessed 24.04.2020).
19. Strategia Naţională pentru Edificarea societăţii informaţionale – „Moldova electronică", aprobată prin Hotărârea Guvernului nr.255 din 09.03.2005. Monitorul Oficial Nr. 46-50 din 25.03.2005. (Romanian)
20. Strategia Naţională de dezvoltare a societăţii informaţionale „Moldova digitală 2020", aprobată prin Hotărârea Guvernului nr.857 din 31.10.2013. Monitorul Oficial Nr. 252-257 din 08.11.2013. (Romanian)
21. Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, aprobat prin Hotărârea Guvernului nr.811 din 29.11.2015. Monitorul Oficial Nr. 306-310 din 13.11.2015. (Romanian)
22. Strategia securității informaționale a Republicii Moldova pentru anii 2019-2024, aprobată prin Hotărârea Parlamentului nr.257 din 22.11.2018. Monitorul Oficial Nr. 13-21 din 18-01-2019. (Romanian)
23. Concepţia securităţii informaţionale a Republicii Moldova, aprobată de Parlamentul prin Legea ordinară nr.299 din 21.12.2017. Monitorul Oficial Nr. 48-57 din 16-02-2018. (Romanian)
24. Shaimaa Khalil, Australia cyber attacks: PM Morrison warns of 'sophisticated' state hack. BBC News Australia, 19 June, 2020. https://www.bbc.com/news/world-australia-46096768 (accessed 20.06.2020).