MEST Journal
DOI 10.12709/mest.09.09.01.13

CYBERSECURITY AS A FUNDAMENTAL ELEMENT OF THE DIGITAL ECONOMY

Alexandru Leahovcenco
ASEM, Department of Applied Informatics in business, Chisinau, Moldova

JEL Category: **M15**

Abstract

The development of the digital economy is inextricably linked to cybersecurity. The article discusses issues related to the definition of cybersecurity, its elements, and examines data on cyber-attacks. The analysis of the tightness of the relationship between the share of the digital economy in GDP and the GCI index using a correlation analysis is carried out in this article. The issues of cybersecurity in the Republic of Moldova are also discussed and ways to improve it are suggested. Currently, there have been significant changes in the structure of cyber threats. These changes are associated with discrete changes in the motives and tactics of cybercriminals. The reasons for enrichment contributed to the emergence of crypto miners. At the same time, there is a shift towards reducing the use of malware and complex infrastructure and moving to low-profile social engineering attacks. This article analyzes the situation in the field of cybersecurity in the Republic of Moldova and provides suggestions for its improvement.

Keywords: *cybersecurity, digital economy, cyber risk, GCI index*

1 INTRODUCTION

The digital economy is an economy, whose formation and development is due to the active use of modern processes of information and communication technologies. The development of the digital economy through the active use of IT requires data protection in cyberspace. In this case, the need to create such a data protection system in cyberspace, which meets the requirements of international standards and will contribute to the further development of the digital economy, must be considered.

The address of the author
Alexandru Leahovcenco
alexandru.leahovcenco@yandex.com

There is currently no unified definition of cybersecurity. As stated in the article 2 "Definitions" of the Regulation (EU) 2019/881 of the European Parliament and the council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and information and communications technology cybersecurity certification and repealing regulation (EU) no 526/2013 (Cybersecurity Act): cybersecurity means the activities necessary to protect network and information systems, users, of such systems and other persons affected by the cyber threat (Council, Regulation (EU) 2019/881, 2019).

Article 4 of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 “Concerning measures for a high common level of security of network and information systems across the Union” defines “security of

network and information systems" as an ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems (Council, Directive (EU) 2016/1148, 2016).

The European Court of auditors in its report challenges for an effective EU cybersecurity policy stated that: "cybersecurity involves preventing or detecting, responding to and recovering from cyber incidents. Incidents can be caused intentionally or unintentionally and cover remarkably diverse situations, for example from accidental disclosure of information to attacks on critical businesses and infrastructures, theft of personal data, and even interference in democratic processes. All these incidents can have far-reaching negative effects on individuals, organizations, and communities. (Europeană, 2019).

Government decision no. 811 of 29.11.2015 "On the national cybersecurity Program of the Republic of Moldova for the years 2016 to 2020" addresses issues of cyber-security as the state of normality resulting from the application of a complex set of proactive and reactive measures, which, in cyberspace, is to ensure the confidentiality, integrity, availability, authenticity, and non-repudiation of information in electronic form, the information systems and resources of the service to the public and the private. Proactive and reactive measures include security policies, concepts, standards and guidelines, risk management, training and awareness activities, implementation of technical solutions to protect cyberinfrastructures, identity management, consequences management (Moldova, 2015).

Kaspersky Lab (an international company operating in the field of information security since 1997) defines cybersecurity, as: "strategic actions aimed at protecting information and communications through a series of advanced tools, policies and processes" (Kaspersky Lab. IT threat evolution Q2 2018. Statistics, n.d.).

The American company Cisco on its website published the following definition: "cybersecurity is the practice of protecting systems, networks, and programs from digital attacks." (Cisco, 2020).

The Guardian determines that cybersecurity refers to all technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cybersecurity can also be called Information Technology Security (Guardian, 2020), Thus, in the author's opinion, cybersecurity is complex of policies, procedures, tools, which include measures to protect various information systems and cyber-attack media, as well as the concept of security on risk management and retaliation.

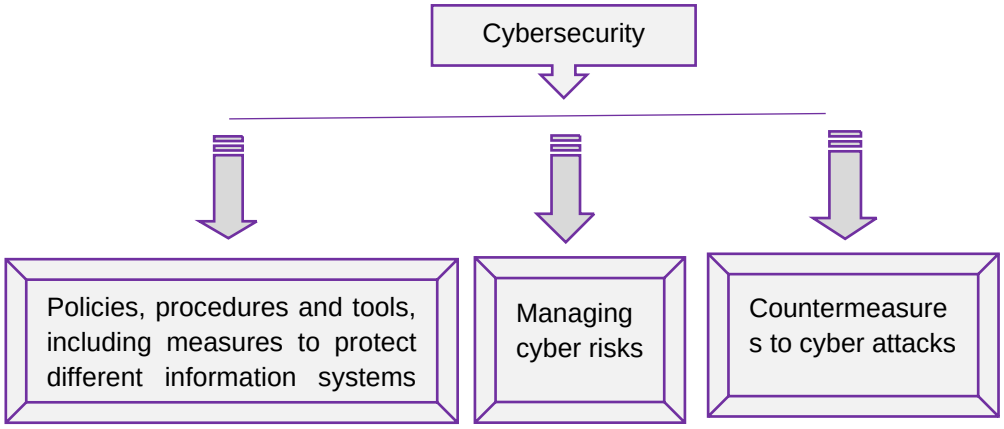

Fig.1 Cybersecurity elements

Analyzing these definitions and emerging from current realities, the author concluded that cybersecurity is not only a protective measure but also aimed at managing cyber risks and acting on response measures. Thus, according to the author, cybersecurity is a complex of policies, procedures, and tools, including measures to protect different information systems and their devices against cyberattacks, as well as security

concepts for risk management and countermeasures to cyberattacks

2 RESEARCH ON THE FIELD OF CYBERSECURITY

In a digital economy, cybersecurity needs to ensure database security, at the state, entity, and individual level.

For effective cybersecurity, an entity must coordinate its efforts across its entire IT system. Cyber elements include:

- application security: applications require constant updates and testing to ensure that they are effective against attacks,
- network security: protecting the network against attacks and intrusions,
- endpoint security is the process of protecting remote access to a company's network,
- data security consists of protecting confidential information about the company and customers,
- identity management is a process of understanding each individual's access to a company,
- database and infrastructure security: the process of protecting devices is equally important,
- cloud security,
- mobile security is the protection of phones and tablets

The most difficult challenge in cybersecurity is that security risks are constantly evolving. Traditionally, companies and governments have focused most of their cybersecurity resources on protecting only the most important components of the system and defending themselves against known treatments. Today, this approach is insufficient, as threats advance and change faster than companies can respond.

Cyber risk assessments should also consider any regulations that influence the way the company collects, stores, and secures data, such as PCI-DSS, HIPAA, SOX, FISMA, and others. One area that is constantly evolving is cybersecurity best practices, which are evolving to adapt to the increasingly sophisticated attacks carried out by attackers. Combining cybersecurity measures with a team of security-educated employees provides the best defense against cyber criminals trying to gain access to confidential company data.

The European Union Agency for Cybersecurity (ENISA) has prepared a report - landscape threats for 2018: Top 15 Cyberthreats and trends. An overview of the current threat landscape in 2018 reveals the first 15 cyber threats (Kaspersky Lab. IT threat evolution Q2 2018. Statistics, n.d.):

1. Malware (malicious software)-software that aims, in one form or another, to harm the computer and its content. Malware is a common name for all kinds of cyber threats such as viruses, trojans, spyware, keyloggers, adware, etc.
2. Web-based Attacks,
3. Phishing is a manipulation of the identity of companies or individuals to obtain financial benefits or confidential information,
4. Spam is unsolicited electronic messages sent using Trojan - infected computers that are part of a botnet. Spam is not a malicious program in itself, but it may include attachments containing such programs,
5. Denial of Service (DoS) is a type of attack on a service that disrupts normal function and prevents other users from accessing it. The most common target for a DoS attack is an online service, such as a website, although attacks can also be launched against networks or even a single program,
6. Ransomware-a type of software designed to extort, block access to a computer system or prevent the reading of data recorded in it (often by encryption methods), and then ask the victim for ransom to restore the original,
7. Botnets – a botnet is several devices connected to the Internet, each of which runs one or more robots. Botnets can be used to perform Distributed Denial-of-Service (DDoS) attacks, steal data, send spam, and allow the attacker to access the device and its connection. The owner can control the botnet using command and control (C&C) software. The word "botnet" is a portmanteau of the words "robot" and " network",
8. Data Breaches is the intentional or unintentional release of private or confidential information in an untrusted environment,
9. Insider threat - is a harmful threat to an organization that comes from individuals within the organization, such as employees,

former employees, entrepreneurs, or business associates, who have internal information about the security practices, data, and information systems of the organization, especially those of the organization.

10. Physical manipulation/damage/theft / loss,
11. Information Leakage occurs when a system that is designed to be shut down, however, discloses some information to unauthorized parties,
12. Identity Theft is the deliberate use of someone else's identity, usually as a method of obtaining a financial advantage or credit and other benefits on behalf of the other person,
13. Cryptojacking is an activity in which an infected device is used to secretly mine for cryptocurrencies,
14. Exploit Kits are automated programs used by attackers to exploit known vulnerabilities in systems or applications. They can be used to secretly launch attacks while victims surf the web to download and execute a type of malware.
15. Cyber Espionage is the act or practice of obtaining secrets and information without the permission and knowledge of the holder of information from persons, rivals, governments for personal, economic, political, or military advantage using methods on the internet, networks, or individual computers using proxy servers, cracking techniques and software, including Trojans and spyware.

According to data presented in the report-landscape threats for 2018: Top 15 Cyberthreats and trends 10 countries were identified according to the share of users attacked by Trojans mobile banking (ENISA, 2020):

According to the data presented by Kaspersky Lab in the table are presented data about unique users attacked by mobile banking Trojans in the country as a percentage of all users of Kaspersky Lab mobile antivirus in this country. They are excluded from the rating with relatively few users of Kaspersky Lab mobile antivirus (under 10,000).

To assess the risk of online damage faced by users in different countries, the information about the percentage of Kaspersky Lab (Web Anti-Virus) users whose computers have been affected is presented. The resulting data indicates the aggressiveness of the environment in which computers operate in different countries. This rating includes only attacks of harmful programs that fall into the Malware class; it does not include anti-Virus web detections of potentially dangerous or unwanted programs such as RiskTool or adware.

Table 1 TOP 10 countries by the share of users attacked by Trojans mobile banking in the 2nd quarter of 2018 (Lab, 2020).

Nr.	Country	%
1	USA	0.79
2	Russia	0.70
3	Poland	0.28
4	China	0.28
5	Tajikistan	0.27
6	Uzbekistan	0.23
7	Ukraine	0.18
8	Singapore	0.16
9	Moldova	0.14
10	Kazakhstan	0.13

The Center for Strategic and International research tracks cyber-attacks on government institutions, defense, and high-tech companies, or economic crimes with losses of more than one million dollars. Over the past decade, they have tracked 490 significant cyber incidents.

Below is the data on the number of consumer complaints about internet crimes that were obtained by the Federal Bureau of Investigation (FBI, 2020) between 2009 and 2019.

Currently, there have been significant changes in the structure of cyber threats. These changes are associated with discrete changes in the motives and tactics of cybercriminals. The reasons for enrichment contributed to the emergence of crypto miners. At the same time, there is a shift towards reducing the use of malware and complex infrastructure and moving to low-profile social engineering attacks. Threatening actors are expected to adapt their activities to these changes, thus impacting the cyber threat landscape in the coming years.

The emergence of IoT environments will continue to be a concern due to the lack of security mechanisms in cheap IoT devices. The need for generic IoT security architectures will remain urgent.

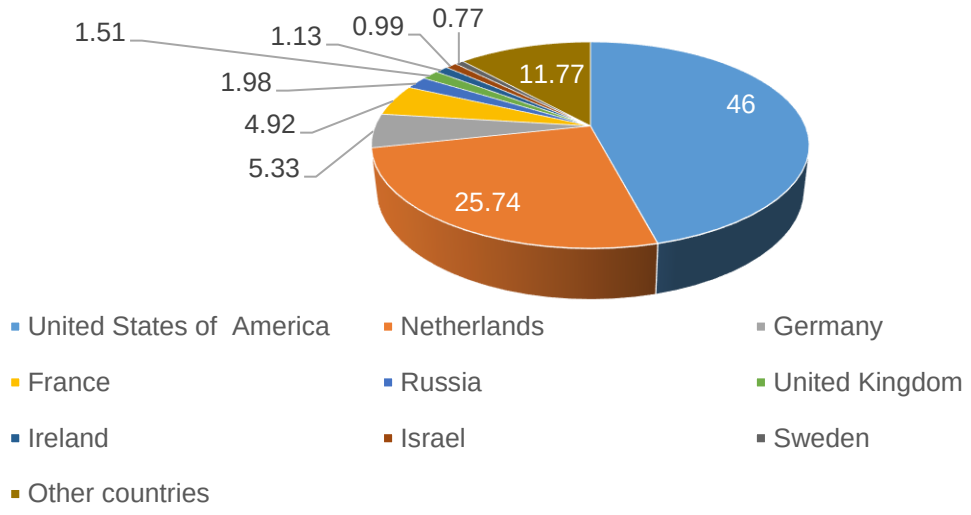

Fig. 2 Distribution of web attack sources by country, 2nd quarter of 2018 (Lab, 2020)

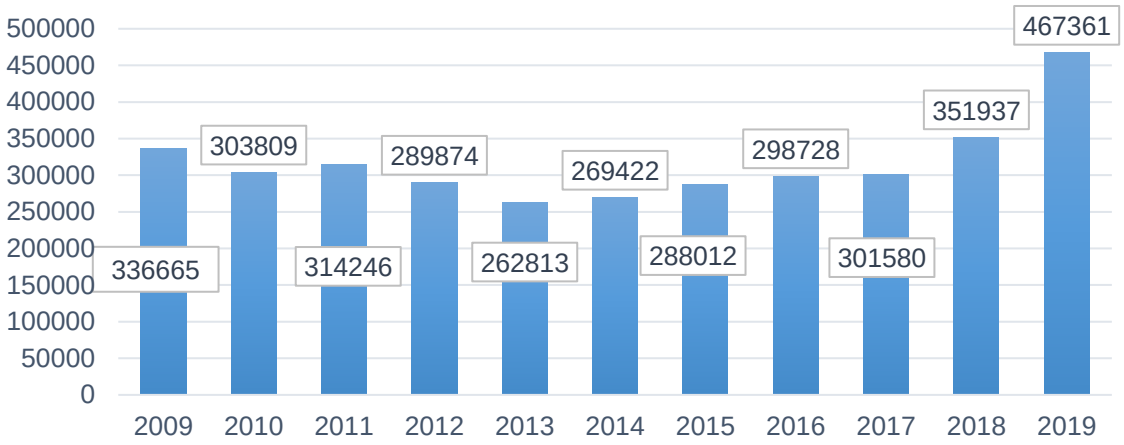

Fig.3 (Number of cases of economic crimes through cyberattacks with losses of more that one million US dollars, 2020)

Using intelligence to prevent cyber threats (AI) should become commonplace for many stakeholders, with a focus on those without technical knowledge.

The security software industry needs to research and develop solutions using automation and knowledge engineering to help end-users and organizations mitigate the slightest lower-level cyber threats with minimal human intervention. AI knowledge management should be the subject of standardization efforts. Of particular importance is the development of standard cybersecurity dictionaries, standard attack repositories, automatic methods of information collection, and knowledge management processes.

There are various indices to determine the level of cybersecurity. The Global Cybersecurity Index (GCI) is an initiative of the International Telecommunication Union (ITU) involving experts from different fields and organizations. The Global Cybersecurity Index (GCI) is a composite index produced, analyzed, and published by the International Telecommunication Union (ITU) to measure countries ' commitment to cybersecurity to raise cybersecurity awareness. The GCI is rooted in the ITU Global Cyber Security Agenda (GCA) launched in 2007 and reflects its five pillars: legal, technical, organizational, capacity building, and cooperation.

The GCI combines 25 indicators in a benchmark measure to monitor the cybersecurity commitment of 193 ITU member states and the state of Palestine to the five pillars endorsed by global cybersecurity. The index uses data collected through an online survey. Questions were developed for each pillar to assess commitment. Through consultation with an expert group, questions are weighted to generate an overall GCI score.

The main objectives of the GCI are to measure:

- the type, level, and evolution over time of Cybersecurity Engagement in countries and compared to that of other countries.
- progress in the global cybersecurity commitment of all countries.
- progress in the cybersecurity commitment from a regional perspective.
- the division of the cybersecurity commitment (i. e. the difference between countries in terms of their level of involvement in cybersecurity initiatives.

Let us analyze the tightness of the relationship between the share of the digital economy in GDP and the GCI index using correlation analysis.

Table 2 Determination of the tightness of the relationship between indicators through a correlation analysis for 2017

States	Share of the digital economy in GDP (X)	Index GCI (Y)	X^2	XY	Y^2
United Kingdom	6.27	0.78	39.31	4.91	0.61
France	4.96	0.82	24.60	4.06	0.67
Litonia	4.84	0.50	23.43	2.44	0.25
Germany	6.03	0.68	36.36	4.09	0.46
Poland	5.13	0.62	26.32	3.19	0.39
Romania	4.10	0.59	16.81	2.40	0.34
total	31.33	3.99	166.83	21.09	2.73

The calculation is carried out according to the following formula, $\begin{cases} na + b\sum x = \sum y \\ a\sum x + b\sum x^2 = \sum xy \end{cases}$, with n-the number of countries is 6. Substituting the indicators in the formula, we come to the following calculation: $\begin{cases} 6a + 31.33b = 3.99 \\ 31.33a + 166.83b = 21.09 \end{cases}$ thus

$$r = \frac{\sum xy - \frac{\sum x \sum y}{n}}{\sqrt{\left[\sum x^2 - \frac{(\sum x)^2}{n}\right]} \times \sqrt{\left[\sum y^2 - \frac{(\sum y)^2}{n}\right]}}$$

b=0.07, the number is positive, indicating a direct relationship. To determine the tightness of the relationship between the indicators, we use the correlation coefficient according to the formula:

Performing the calculations

$$\frac{21.09-(31.33 \times 3.99)/6}{\sqrt{([166.83-(166.83)/6)] \times \sqrt{[2.73-(2.73)/6]}}}$$

we get indicator 0.014.

The correlation coefficient is less than 0.7, which indicates the presence of a weak relationship. Analyzing the indicators in the table above, it can be stated that the higher the share of the digital economy in GDP, the higher the GCI index, for example, in the United Kingdom, the share of the digital economy in GDP in 2017 was 6.27, and the GCI index was 0.78; Germany, 6.03 and 0.68 respectively; in Poland, respectively 5.13 and 0.62; in Romania, respectively 4.10, respectively 0.59.

According to the information disclosed in the "Register of forensic and criminological information", presented by the Ministry of Internal Affairs, starting in 2015 and until December 2019 inclusive, 105 computer crimes were registered on art. 259-2611 and art. 2081 of the Criminal Code of the Republic of Moldova.

The following figure shows data on cybercrime in the Republic of Moldova.

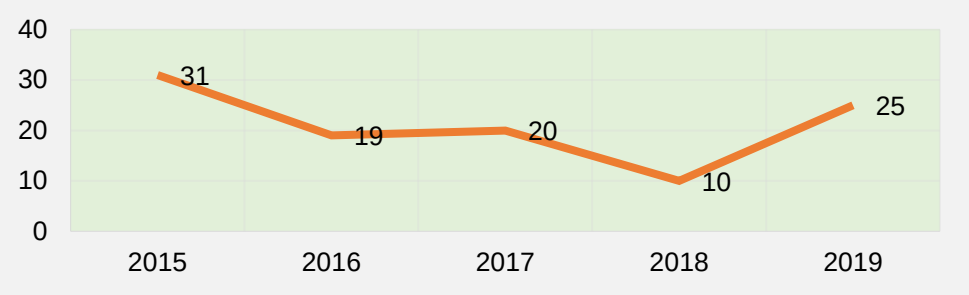

Fig.4 (Dynamics of the number of computer crimes in the Republic of Moldova registered in the "Register of forensic and criminological information" of the Republic of Moldova , 2020).

At the same time, as mentioned in the Government Decision no. 811 of 29.11.2015 "On the National Cyber Security Program of the Republic of Moldova for the years 2016-2020": " that the data in the Register of forensic and criminological information are not yet complete and do not reflect all classes of crimes and contraventions within the meaning of the Budapest Council of Europe Convention on cybercrime, it can be seen that the number of crimes and misdemeanors is increasing." (ENISA, 2020).

In the decision of the Government of Moldova no.811 it was found, that for the effective development of the cybersecurity system, it is necessary to create a cybersecurity management system. At the same time, cybersecurity management is necessary for:

- cybersecurity system planning,
- conduct an annual cybersecurity audit to identify risks,
- effective protection of information systems against cyber-attacks,
- develop and implement policies on preventive measures against cyber-attacks.

3 CONCLUSIONS

A management system in the field of cybersecurity is necessary both at the state level and at the company level, while it must penetrate all areas of activity: economic, political, social. Many problems related to ensuring cybersecurity in Moldova should be noted:

1. At the state level, there is no complete safety when processing, accessing and storing public data.
2. The security of computer networks and services is not adjusted to the standards and recommendations of the European Union according to the provisions of the association agreement between the Republic of Moldova and the European Union.
3. There are no satisfactory capacities to prevent cyber-attacks at the national level, given the intermittent nature of cyber-attacks.
4. The national regulatory framework should be revised following the provisions of the Council of Europe Convention on cybercrime.
5. Curricula in the field of cybersecurity must be constantly modified according to the changing situation in the digital economy and cybersecurity.
6. Lack of sufficient international interaction to identify risks and other events occurring in global cyberspace.

Analyzing this situation, the author concluded that cybersecurity management at the state level should consist of the following components:

1. State strategy on Cyber Security Management, which would be approved for one year,
2. State center, which would be responsible for public policy in the field of cybersecurity and Prevention of cyber threats,
3. Annual audit of the cybersecurity system at the level of the state and its institutions,
4. Help Center for business and citizens regarding cybersecurity management,
5. Educational institutions and the availability of advanced programs in the field of cybersecurity, updated in line with changes in cyberspace and the digital economy.

Analyzing this situation, the author concluded that cybersecurity management at the state level should consist of the following components:

1. State strategy on Cyber Security Management, which would be approved for one year,
2. State center, which would be responsible for public policy in the field of cybersecurity and Prevention of cyber threats,
3. Annual audit of the cybersecurity system at the level of the state and its institutions,
4. Help Center for business and citizens regarding cybersecurity management,
5. Educational institutions and the availability of advanced programs in the field of cybersecurity, updated in line with changes in cyberspace and the digital economy.

It should be noted that by the provisions of the Government Decision No. 482 of 08.07.2020 ”On approval of necessary measures to ensure cybersecurity at government level and modification of government decision no. 414/2018 "has been designated I. P." Information Technology and Cyber Security Service "as government cybersecurity incident response center (CERT Gov).

At the same time, when developing cybersecurity management, it is necessary to use the provisions:

ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements,

ISO / IEC 27002: 2013 Information technology — Security techniques — Code of practice for information security controls.

WORKS CITED

Council, E. P. (2016, July 6). *Directive (EU) 2016/1148.* Retrieved from eur-lex.europa.eu: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016L1148&from=EN

Council, E. P. (2019, April 7). *Regulation (EU) 2019/881.* Retrieved from eur-lex.europa.eu: https://eur-lex.europa.eu/eli/reg/2019/881/oj

Dynamics of the number of computer crimes in the Republic of Moldova registered in the "Register of forensic and criminological information" of the Republic of Moldova . (2020). Retrieved from https://www.mai.gov.md/ro/date-statistice

ENISA. (2020). *ENISA Threat Landscape Report 2018 15 Top Cyberthreats and Trends*. Retrieved from https://www.enisa.europa.eu: https://www.enisa.europa.eu/publications/ecsm

Europeană, C. d. (2019). *Raportul Provocări pentru o politică eficace a UE în domeniul securității cibernetice.* Bruxelles: Curtea de conturi Europeană.

FBI. (2020). *Number of cases of economic crimes through cyber attacks with losses of more than one million US dollars (according to addresses to the FBI)*. Retrieved from https://sectigostore.com/: https://sectigostore.com/blog/42-cyber-attack-statistics-by-year-a-look-at-the-last-decade

Guardian, T. (2020). *The Guardian.* Retrieved from The Guardian: https://support.theguardian.com/int/subscribe/digital?gclid=CjwKCAjwsO_4BRBBEiwAyagRTTyL4R6i3yXpC-pzfPMZvdLINu_pbj5OHJDogH2qV1wfFvD07-XnuBoCG2gQAvD_BwE

Kaspersky Lab. IT threat evolution Q2 2018. Statistics. (n.d.). Retrieved from Kaspersky Lab: https://securelist.com/it-threat-evolution-q2-2018-statistics/87170/

Lab, K. (2020). *Kaspersky Lab.* Retrieved from Kaspersky Lab: https://www.kaspersky.ru/resource-center/preemptive-safety/cyber-security-basics

Moldova, G. R. (2015). *Government decision no. 811, On the national cyber security Programme of the Republic of Moldova for the years 2016 to 2020.* Chisinau: Guvernul Republiicii Moldova.

Number of cases of economic crimes throgh cyber attacks with losses of more thatn one million US dollars. (2020). Retrieved from https://sectigostore.com.

Cisco. (2020). *What Is Cybersecurity?* Retrieved from Cisco: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Received for publication: 05.09.2020
Revision received: 22.09.2020
Accepted for publication: 30.12.2020

How to cite this article?

Style – **APA** *Sixth Edition:*

Leahovcenco, A. (2021, January 15). Cybersecurity as a fundamental element of the digital economy. (Z. Cekerevac, Ed.) *MEST Journal, 9*(1), 97-105. doi:10.12709/mest.09.09.01.13

Style – **Chicago** *Sixteenth Edition:*

Leahovcenco, Alexandru. 2021. "Cybersecurity as a fundamental element of the digital economy." Edited by Zoran Cekerevac. *MEST Journal* (MESTE) 9 (1): 97-105. doi:10.12709/mest.09.09.01.13.

Style – **GOST** *Name Sort:*

Leahovcenco Alexandru Cybersecurity as a fundamental element of the digital economy [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto : MESTE, January 15, 2021. - 1 : Vol. 9. - pp. 97-105.

Style – **Harvard** *Anglia:*

Leahovcenco, A., 2021. Cybersecurity as a fundamental element of the digital economy. *MEST Journal,* 15 January, 9(1), pp. 97-105.

Style – **ISO 690** *Numerical Reference:*

Cybersecurity as a fundamental element of the digital economy. **Leahovcenco, Alexandru.** [ed.] Zoran Cekerevac. 1, Belgrade – Toronto : MESTE, January 15, 2021, MEST Journal, Vol. 9, pp. 97-105.