The European Proceedings of
Social and Behavioural Sciences
EpSBS
www.europeanproceedings.com
e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2020.12.80

TIES 2020
International conference «Trends and innovations in economic studies»

PROBLEMS OF FORMATION OF THE ENTERPRISE DIGITAL SECURITY SYSTEM

Maxim Yu. Tantsyura (a)*, Gennadii A. Shtofer (b), Elvina E. Shamileva (c), Galina V. Olkhovaya (d)
*Corresponding author

(a) Crimean Vernadsky Federal University, 4, Acad. Vernadsky ave, Simferopol, Russia, smt@bk.ru
(b) Crimean Vernadsky Federal University, 4, Acad. Vernadsky ave, Simferopol, Russia, cgena@mail.ru
(c) Crimean Vernadsky Federal University, 4, Acad. Vernadsky ave, Simferopol, Russia, elya_shamileva@mail.ru
(d) Crimean Vernadsky Federal University, 4, Acad. Vernadsky ave, Simferopol, Russia, galinaboyko2006@yandex.ru

Abstract

The article is devoted to the problems of creating an enterprise digital security system. The main objectives of the study: to consider modern approaches to the definition of the concept of "security system" and highlight its main features; identify the problems of the formation of the digital security system of the enterprise; to offer quantitative indicators of the integrated assessment of the formed digital security system of the enterprise. To study approaches to the definition of the concept of "security system" and highlight its main features, a comparative analysis is used. To assess the level of security and the effectiveness of the security system, a coefficient method is proposed. A formal logical approach is used to calculate an effective level of security. The main problems of the formation of the enterprise's digital security system include: creating a subsystem for managing the enterprise's digital security system; selection of physical and virtual means, methods and measures designed to ensure digital security; categorization of digital assets of an enterprise by the criterion of value; identification and assessment of digital risks. The following indicators are proposed for a quantitative assessment of the adequacy of the formed security system: the level of security that characterizes the adequacy of the enterprise's digital security system to existing external and internal risks, and the effectiveness of the security system, which characterizes the rationality of spending money on the enterprise's digital security system.

Keywords: Problems, system formation, security system, digital security, enterprise.

https://doi.org/10.15405/epsbs.2020.12.80
Corresponding Author: Maxim Yu. Tantsyura
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

The active development of the digital economy now poses new challenges for the activities of enterprises of all types and forms of ownership. The speed and level of adaptation to ongoing changes is becoming a prerequisite for the survival of the enterprise in the market and its competitiveness (Keyun, 2019). Moreover, there is a steady trend towards the further development and deepening of the digitalization process. In the near future, the fifth generation 5G wireless network deployment process will have the most significant impact on the market. This will further accelerate the digitalization process and lead to new opportunities and new threats for enterprises (Gunter, 2017).

2. Problem Statement

The emergence of the digital economy, in addition to the obvious advantages, has also brought a number of negative phenomena that can cause damage to a particular enterprise. We are talking about digital risks as a special kind of economic risks. One of the main digital risks of global importance is the digital divide. The essence of this problem is that individual entities and their groups have disproportionate access to digital resources (Weise, 2018). Moreover, this problem is not only economic, but also political in nature, since it violates the democratic principles of the structure of society and can lead to the emergence of a digital dictatorship. To illustrate the scale of this problem, we present Table 1.

Table 01. Rating of leading countries in the computing power of supercomputers (The TOP500 project, 2019)

Country	Count	System Share (%)	Rmax (TFlops)	Rpeak (TFlops)	Cores
China	228	45,6	531,833	1,132,046	30,463,860
United States	117	23,4	611,063	861,974	17,224,104
Japan	29	5,8	109,503	174,575	3,977,228
France	18	3,6	68,889	105,646	2,122,784
Germany	16	3,2	66,894	98,394	1,732,022
Netherlands	15	3	24,737	31,795	864,000
Ireland	14	2,8	23,088	29,676	806,400
United Kingdom	11	2,2	32,143	39,455	1,189,608
Canada	9	1,8	16,147	29,802	505,088
Italy	5	1	30,099	47,844	794,032

As can be seen from table 1, only 10 countries from 195 independent states of the world possess the main computing potential of supercomputers, that is, about 5 %. Moreover, even among these ten countries there is a monstrous imbalance. If we compare the number of supercomputers with the leader of this rating – China and the "outsider" – Italy, we get: 228/5 = 45.6, that is, the difference is almost 50 times. Based on the above calculations, the current situation can be called critical.

Another obvious problem is a sharp increase in the global volume of information and its traffic (see table 2). This leads to increased requirements for the computing power of devices and their memory. In addition, information processing algorithms are becoming more complicated.

Table 02. Dynamics of global Internet traffic (Digital Economy Report UNCTAD, 2019)

Year	2002	2007	2017	2022
Internet-traffic volume, GB/sec	100	2000	46000	150700

Based on the data in table 2, we calculate the level of average annual increase in global Internet traffic (GI) in the periods indicated in the table:

$$GI_{2002-2007} = \frac{2000-100}{2007-2002} = 380(GB/sec) \quad (1)$$

$$GI_{2007-2017} = \frac{46000-2000}{2017-2007} = 4400(GB/sec) \quad (2)$$

$$GI_{2017-2022} = \frac{150700-46000}{2022-2017} = 20940(GB/sec) \quad (3)$$

As can be seen from the above calculations, the rate of average annual growth in global Internet traffic is constantly increasing.

The problems discussed determine the need for the formation of a digital security system at all enterprises that intend to continue and develop their activities in the market and be competitive. But this process is not typical and standardized in full, it requires taking into account the characteristics of each particular enterprise and the conditions for their functioning.

3. Research Questions

The main objectives of the study: to consider modern approaches to the definition of the concept of "security system" and highlight its main features; identify the problems of the formation of the digital security system of the enterprise; to offer quantitative indicators of the integrated assessment of the formed digital security system of the enterprise.

4. Purpose of the Study

The purpose of the study is to identify the problems of forming a digital security system of an enterprise. This will allow us to formulate a methodology for creating an enterprise’s digital security system in further research on this issue, which would be an excellent reference point for each enterprise that is aware of the existence of digital risks and the consequences of their implementation.

5. Research Methods

To study approaches to the definition of the concept of "security system" and highlight its main features, a comparative analysis is used. To assess the level of security and the effectiveness of the security system, a coefficient method is proposed. A formal logical approach is used to calculate an effective level of security.

6. Findings

First of all, it is necessary to define the concept of “security system” for this; we will consider the various approaches presented in table 3.

Table 03. Approaches to the definition of the concept of "security system" (SB)

An approach	Definition
(Amoroso, 2019)	SS – a hardware system that prevents unauthorised intrusion into a premises, and reports such attempts or a similar software system that prevents unauthorised access
(Hi-news.ru, 2019)	SB is a generic name for systems that protect access to private information or the inviolability of private property. The security system can be quite physical – in the form of alarms, video cameras, a security call console, security too – or completely virtual – a firewall, antivirus, passwords, encrypted connection and other protection
(Dialog Group of Companies, 2019)	SB is a set of interrelated organizational measures (measures, methods) and technical means, combined by communication channels, and ensuring the maintenance of a safe condition of the object, detection and elimination of the most complete list (complex) of threats to life, health, the environment, property and information and having common means of collecting and processing information and management.
(Retail-loyalty, 2019)	SB is a combination of means and methods of maintaining the safe state of an object, preventing, detecting and eliminating threats to life, health and the environment, property and information.

Summarizing the approaches presented in table 3, we can conclude that the concept of "security system" can be considered both in a broad sense and in a narrow one. In a narrow sense, a security system is a software and / or hardware complex that performs one or more tasks of protecting an enterprise. In a broad sense, the security system has the following main features:

- value orientation: the main function of the security system is the protection of objects of value to the enterprise;
- anti-risk nature: the features of the security system are due to the presence of risks in the external and internal environment of the enterprise;
- the variability of the forms of the security system: the use of physical and / or virtual forms;
- instrumentality of the security system: the availability of a set of means, methods and security measures;
- integrity of the security system: the presence of interconnections between the elements of the security system;
- security system focus: the main purpose of the security system is to ensure the safe state of the protected object;
- manageability of the security system: the availability of a system for collecting information from the management of the security system.

Based on the selected features, the following author’s definition can be formulated: a security system is a managed combination of interconnected physical and virtual means, methods and measures designed to ensure the safety of valuable objects in the presence of external and internal risks.

Based on the author's definition proposed above, the following problems of forming the enterprise's digital security system can be distinguished:

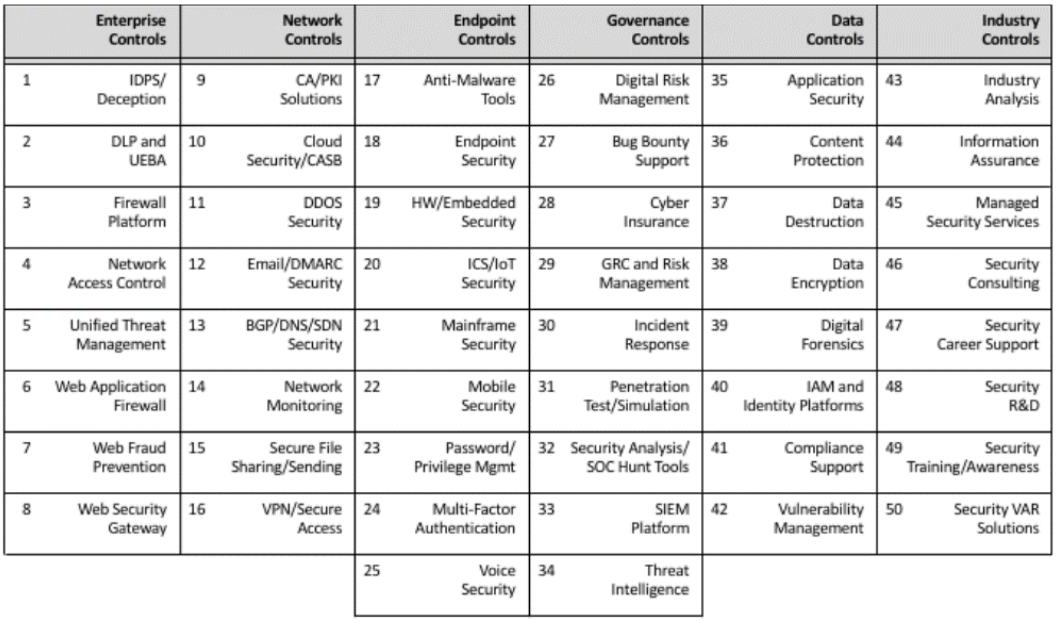
1) creation of a subsystem for managing the enterprise's digital security system;

2) the choice of physical and virtual means, methods and measures designed to ensure digital security;

3) categorization of digital assets of the enterprise by the criterion of value;

4) identification and assessment of digital risks.

The enterprise digital security management system subsystem should include the elements shown in Figure 1.



Enterprise Controls	Network Controls	Endpoint Controls	Governance Controls	Data Controls	Industry Controls
1 IDPS/ Deception	9 CA/PKI Solutions	17 Anti-Malware Tools	26 Digital Risk Management	35 Application Security	43 Industry Analysis
2 DLP and UEBA	10 Cloud Security/CASB	18 Endpoint Security	27 Bug Bounty Support	36 Content Protection	44 Information Assurance
3 Firewall Platform	11 DDOS Security	19 HW/Embedded Security	28 Cyber Insurance	37 Data Destruction	45 Managed Security Services
4 Network Access Control	12 Email/DMARC Security	20 ICS/IoT Security	29 GRC and Risk Management	38 Data Encryption	46 Security Consulting
5 Unified Threat Management	13 BGP/DNS/SDN Security	21 Mainframe Security	30 Incident Response	39 Digital Forensics	47 Security Career Support
6 Web Application Firewall	14 Network Monitoring	22 Mobile Security	31 Penetration Test/Simulation	40 IAM and Identity Platforms	48 Security R&D
7 Web Fraud Prevention	15 Secure File Sharing/Sending	23 Password/ Privilege Mgmt	32 Security Analysis/ SOC Hunt Tools	41 Compliance Support	49 Security Training/Awareness
8 Web Security Gateway	16 VPN/Secure Access	24 Multi-Factor Authentication	33 SIEM Platform	42 Vulnerability Management	50 Security VAR Solutions
		25 Voice Security	34 Threat Intelligence		

Figure 01. Elements of the enterprise digital security management system subsystem (Amoroso, 2019)

The abundance of elements of the control subsystem of the digital security system of the enterprise, as well as their specificity, raises the problem of the impossibility of applying traditional management methods. Moreover, the implementation of such a subsystem requires the active introduction of automated planning, organization, control, etc. In addition, there is no possibility of typing the management subsystem, since each enterprise needs an individual security system architecture based on the resources it has and those conditions in which it operates.

The problem of the choice of methods for ensuring digital security gives rise to the need for careful study of the principles of their classification, assessment and the possibility of combination. The complexity is also the fact that the methods for ensuring digital security of an enterprise are heterogeneous, they are divided into two groups:

1) internal – methods that are developed by the enterprise;

2) external – methods that are developed outside the enterprise:

a) outsourcing methods – methods that are developed by third parties by order of this company;

b) collective methods – methods that are developed by a business combination;

c) legislative methods:

- legislation on information;
- legislation on state, professional and commercial secrets;
- legislation on personal data;
- legislation on electronic digital signature.

The problem of categorizing digital assets is the need to develop clear criteria and an assessment methodology. In addition, it is necessary to standardize the concept of “digital asset” for its uniform application and full coverage of all manifestations of this concept. Existing approaches to the definition of “digital assets” are presented in table 4.

Table 04. Approaches to the definition of the concept of " digital asset " (SB)

An approach	Column Heading
(Wikipedia, 2019)	digital assets - this is what exists in digital form within the digital environment and with established digital rights that determine the procedure for the formation, distribution and use of this type of asset
(Aryamov, Grachova, Chuchaev, & Malikov, 2019)	digital asset is an asset that exists on a digital medium (digitally processed and containing digitized information)
(Kud, 2019)	Digital asset is an information resource derivative of the right to a value and circulating in the distributed ledger in the form of a unique identifier.
(Digital Asset Working Group, 2019)	digital assets is a ledger-based asset, either: • assets native to Distributed Ledger (“DL”), in which the ledger is the account of record (including cryptocurrencies), or • assets immobilized, dematerialized, and/or held off chain, but represented on DL.

Based on the definitions presented in table 4, you can select the following types of digital assets:

1) digital data (content);

2) digital goods;

3) digital services;

4) digital technology;

5) digital platforms.

The problems of identifying and assessing digital risks are associated primarily with the fact that they are global in nature and can hardly be localized. In addition, the realization of many digital risks may not be noticeable. For example, an attacker illegally copied data from a digital document, but the document itself was not deleted or corrupted. In this case, in the absence of a special security system, this violation cannot be detected. Digital risks can be classified according to the following criteria:

1) by source of occurrence:

a) natural – arise due to the action of the forces of nature;

b) man-made – arise for technical reasons;

c) anthropogenic – arise due to the action of the human factor;

2) by object:

a) the risks of digital data;

b) the risks of digital infrastructure;

c) risks of digital processes:

- risks of data generation;
- communication risks;
- data processing risks;
- risks of data storage.

The solution to the above problems will allow a particular company to create its own digital security system. However, like any utilitarian system, it requires a quantitative and qualitative assessment, which would allow to determine the result of the formation and reasonably make management decisions in the field of functioning and development of the digital security system. We propose the use of the following quantitative indicators of assessment:

`1) security level (SL) – characterizes the adequacy of the enterprise's digital security system to existing external and internal risks:

$$SL = \left(1 - \frac{RD}{PD}\right) * 100\%,$$

$$RD = MaD + MoD + PhD,$$

$$PD = D * R,$$

where RD is the real damage received by the enterprise, monetary units; PD – potential damage, monetary units; MaD – the amount of material damage that has occurred, monetary units; MoD – the amount of moral damages, monetary units; PhD – the amount of physical damage that has occurred, monetary units; D – the amount of possible future damage, monetary units; R – risk level (probability of damage), fractions of a unit.

2) the effectiveness of the security system (SE) – characterizes the rationality of spending money on the digital security system of the enterprise:

$$SE = \left(1 - \frac{SSE}{PD-RD}\right),$$

where SSE – security system costs, monetary units.

Combining the two indicators proposed above, we obtain an integrated indicator for assessing the enterprise's digital security system: effective security level (ES):

$$ES = \frac{SL * SE}{100} = \frac{1}{100} * \left(1 - \frac{RD}{PD}\right) * 100\% * \left(1 - \frac{SSE}{PD - RD}\right) * 100\% =$$

$$= \left[1 - \frac{SSE}{PD - RD} - \frac{RD}{PD} + \frac{RD * SSE}{PD * (PD - RD)}\right] * 100\% =$$

$$= \left[1 - \frac{SSE * PD + RD * (PD - RD)}{PD * (PD - RD)} + \frac{RD * SSE}{PD * (PD - RD)}\right] * 100\% =$$

$$= \left[1 + \frac{-SSE * PD - RD * PD + RD^2 + RD * SSE}{PD * (PD - RD)}\right] * 100\% =$$

$$= \left[1 + \frac{-SSE * (PD - RD) - RD * (PD - RD)}{PD * (PD - RD)}\right] * 100\% = \left(1 - \frac{SSE + RD}{PD}\right) * 100\%$$

For a qualitative assessment of the enterprise's digital security system, we suggest qualifying it with the help of the Security System Quadrant (see table 5).

Table 05. Approaches to the definition of the concept of "security system" (SB)

Security level	**Security Efficiency**	
	Low	**High**
Low	Minimum security system	Deficit security system
High	Costly security system	Optimal security system

Source: compiled by the authors

Based on the categorization of the digital security system by Quadrant, an enterprise can choose a strategy for the further development of this system:

1) with a minimum security system – a strategy for reforming the system;

2) in case of a deficient security system – a strategy for improving the risk management system;

3) with an expensive security system – restructuring the costs of the system;

4) with an optimal security system – adaptation of the system to future changes in the external environment.

7. Conclusion

Thus, a security system is understood as a manageable combination of interconnected physical and virtual means, methods and measures designed to ensure the safety of valuable objects in the presence of external and internal risks. The main problems of creating a digital security system of an enterprise are: the creation of a subsystem for managing a digital security system of an enterprise; selection of physical and virtual means, methods and measures designed to ensure digital security; categorization of digital assets of an enterprise by the criterion of value; Identification and assessment of digital risks. The following indicators are used to quantify the adequacy of the formed security system: the security level, which characterizes the adequacy of the enterprise's digital security system to existing external and internal risks, and the effectiveness of the security system, which characterizes the rationality of spending money on the enterprise's digital security system. An effective level of security can be used as an integral indicator of evaluating an enterprise's digital security system.

References

Amoroso, G. (2019). Outlook for fifty cyber security control. *TAG Cyber Security Annual, 1.* Retrieved from: https://www.tag-cyber.com/annuals/Volume_1_- _2019_TAG_Cyber_Security_Annual.pdf

Aryamov, A., Grachova, V., Chuchaev, I., & Malikov, V. (2019). Digital asset as an object legal regulation. *Ekonomika, Journal for Economical Theory and Practice and Soc.ial Issues, 65(2*), 1–11. https://doi.org/ 10.5937/ekonomika1902001A

Dialog Group of Companies. (2019). *Security system*. Retrieved from: http://dialog-e.ru/solutions/security-system/

Digital Asset Working Group. (2019). *Digital Asset Working Group Report June 2019*. Retrieved from: https://www.r3.com/wp-content/uploads/2019/07/DigitAssetWorkingGroupReport.June2019.pdf

Digital Economy Report, UNCTAD. (2019). Retrieved from: https://unctad.org/en/PublicationsLibrary/der2019_overview_en.pdf

Gunter, S. (2017). Digitally Secure Transformation. *ITNOW, Oxford University Press, 59(2),* 12–13. https://doi.org/ 10.1093/itnow/bwx036

Hi-news.ru. (2019). *Security system*. Retrieved from: https://hi-news.ru/tag/sistema-bezopasnosti

Keyun, R. (2019). Digital Assets as Economic Goods. *Digital Asset Valuation and Cyber Risk Management* (pp. 1–28). Academic Press. https://doi.org/10.1016/B978-0-12-812158-0.00001-6

Kud, A. A. (2019). Substantiation of the Term “Digital Asset”: Economic and Legal Aspects. *International Journal of Educational and Science, 2*, 1. https://doi.org/10.26697/ijes

Retail-loyalty. (2019). *Security system*. Retrieved from: https://www.retail-loyalty.org/journal_retail_loyalty/about/

The TOP500 project. (2019). *The top 500 List of the 500 most powerful commercially available computer systems*. Retrieved from: https://www.top500.org/lists/2019/11/highs

Weise, A. (2018). Digital Security – Wie Unternehmen den Sicherheitsrisiken des digitalen Wandels trotzen. In: Lars Fend, Jürgen Hofmann (eds.) *Digitalisierung in Industrie-, Handels- und Dienstleistungsunternehmen* (pp. 243–262). https://doi.org/10.1007/978-3-658-26964-7_13

Wikipedia. (2019). *Digital asset*. Retrieved from: https://en.wikipedia.org/wiki/Digital_asset