Kuzmenko, O., Cyburt, A., Yarovenko, H., Yesh, V., & Humenna, Y. (2021). Modeling of "information bubbles" in the global information space. *Journal of International Studies, 14*(4), 270-285. doi:10.14254/2071-8330.2021/14-4/18

Journal
of International
Studies

Scientific Papers

Modeling of "information bubbles" in the global information space

Olha Kuzmenko
Department of Economic Cybernetics,
Sumy State University, Ukraine
o.kuzmenko@biem.sumdu.edu.ua
ORCID 0000-0001-8520-2266

Agnieszka Cyburt
Pope John Paul II State School of Higher Education in Biała
Podlaska, Poland
a.cyburt@dydaktyka.pswbp.pl
ORCID 0000-0002-7084-6066

Hanna Yarovenko
Department of Economic Cybernetics,
Sumy State University, Ukraine
h.yarovenko@biem.sumdu.edu.ua
ORCID 0000-0002-8760-6835

Valeryia Yersh
Faculty of Economics and Management, Lazarski University,
Warsaw, Poland
valeryia.yersh@gmail.com
ORCID: 0000-0002-5794-4198

Yuliia Humenna
Department of Financial Technologies and Entrepreneurship,
Sumy State University, Ukraine
y.gumenna@finance.sumdu.edu.ua
ORCID 0000-0001-5309-6016

Abstract. The article uses the Sedov-Taylor function to model "information bubbles" formed in the global information space due to information attacks. The authors identify the most relevant determinants that describe information activities related to cyber threats and reactions of economic agents in the global digital economic space. The article hypothesizes about the emergence of "information bubbles" due to increases in information activities and their rupture due to

Received:
February, 2021
1st Revision:
October, 2021
Accepted:
December, 2021

information intrusion, leading to appropriate reactions of economic agents and their subsequent stabilization over time. The empirical data from global web statistics indicates, that four large-scale information overloads were caused by cyberattacks during the study period, which led to the rupture of "information bubbles". Application of autocorrelation functions allows us to determine that the period during which misinformation spreads is, on average, seven days. Solution of the Sedov-Taylor optimization problem and calculations of differential equations, as well as their derivatives, suggest several indicators. Namely, a breakpoint of the second kind, corresponds to the rupture of the "information bubble" with a subsequent adaptation of the system; the inflection point of the function identifies the levels of information activities related to cyber threats, which will change the consequences of the "information bubble" rupture; the minimum possible level of the reactions of economic agents in the global digital economic space.

DOI:
10.14254/2071-8330.2021/14-4/18

Keywords: cyber threat, digital economy, information activity, information bubble, information injection, information security, information space.

JEL Classification: C02, C22, H56.

1. INTRODUCTION

The fourth industrial revolution has brought on the rapid development of cyber-physical systems, which has led to the mass introduction of computer technologies in various sectors in the last decade. At the same time, these processes have been accompanied by an increase in cybercrime, the main purpose of which is to seize information or disrupt information systems through illegal access to them. The World Economic Forum (2021) has identified cybercrime as the fifth expecting risk to increase in the world after economic confrontations, domestic political polarization, extreme heat waves, destruction of natural ecosystems. According to the University of Maryland statistics, every two minutes three cyberattacks happen globally (Cvetićanin, 2020). Their most common forms are phishing, ransomware attacks, data leaks, DDoS attacks, etc. Among all these violations, 23% are cyber warfare acts, which increased by 440% from 2009 to 2018 (Cvetićanin, 2020). This is primarily due to the fact that governments use information or cyber warfare against each other as the most powerful weapon aimed at destabilizing the economic, political or social situation in a country and gaining world supremacy. The most attacked country is the United States, which is the target for 38% of all cyberattacks. India (17%), Japan (11%), Taiwan (7%), Ukraine (6%), South Korea (6%), Brunei (4%), Russia (4%) are also worth noting (PurpleSec LLC, 2021). The acts of information wars are usually directed at important objects of state infrastructure - government organizations, defense companies, banks, giant companies, etc. – and perpetrated through mass virus attacks, cyber espionage, hacktivism, cyberterrorism, etc.

Information intrusion is a type of information warfare, carried out by filling the information space with a certain type of information, usually of negative nature, *en masse*. It leads to resonance in society and its spheres, thus creating an “information bubble”. The “information bubble” is an unpredictable event that does not occur permanently, but whose emergence is purposefully aimed at achieving specific political or economic results. As a result of the attack, information activities in the global information environment (messages, tweets, articles, publications, etc.) about a specific object against which the attack is directed grow rapidly. At the peak of such activity, there is an information injection (release of energy), which ends with the rupture of such a bubble. After that, for a certain period, there are fluctuations of information entities that reflect the results of actual sector events, closely related to information activities, and identified in the global information space. These can be consequences in the economic environment, or in the political sphere, or of a social nature, which grow exponentially and can destabilize the country in these spheres or even collapse. Today, this type of information warfare is the most popular because it allows their initiators to manipulate public sentiment and provoke appropriate reactions in the real sector. Therefore, it is extremely important to have tools to identify "information bubbles" of various kinds, predict their impact on other areas, and develop a mechanism for their detection and prevention.

The purpose of this research is to investigate a mathematical model for identifying "information bubbles". It will determine the temporal features of the economic agents' reaction in the global digital economic space to their gaps caused by parasitic information intrusions due to large-scale hacker attacks. It will determine the number of bubbles in the worldwide network of retrospect, the average duration of the disinformation period due to global cyber incidents, the average period of destabilization of digital economic transactions after the bubble rupture.

2. LITERATURE REVIEW

The Industrial Revolution 4.0 contributed to the formation of a digital environment where business and society function intensively (Afonasova et al., 2019; Baranauskas, 2020). The global COVID-19 pandemic has also created the conditions for its growth (Tiutiunyk et al., 2021). These processes have also affected the development of new areas of life, such as the creative industry (Bilan et al., 2019b), education digitalization (Cosmulese et al., 2019), digital medicine (Kotenko & Bohnhardt, 2021), the Internet of Things (Miskiewicz, 2020), FinTech (Petrushenko et al., 2018), omnichannel marketing (Bondarenko, 2020). One should note that there is a direct link between the development of the economy, its informatization and digitalization (Moradi, 2021). It requires the introduction of new innovative solutions aimed at creating a security space (Bilan et al., 2020a) and developing three dimensions - the digitalization of society, the ability of the economy to meet the challenges of technological development and the use of information technology in companies (Bilan et al., 2019a). In parallel, the digitalization growth has caused a rapid increase in information flows that require systemic protection, the effectiveness of which significantly affects the national security of any country (Petroye et al., 2020; Leonov et al., 2019; Bilan et al., 2020b). Thus, threats to information security form one of the main risks to sustainable development, especially for developing countries (Stukalo et al., 2020). This issue is relevant at the macroeconomic level, as noted by Brychko et al. (2021), and at the level of business entities (Chigrin & Pimonenko, 2014). It is manifested in the growing requirements for the personal information security of employees (Skrynnyk, 2020a), where possible solutions are proposed to create a surrogate model for digitization of organizational systems (Skrynnyk, 2020b). This process requires increased investment capacity, integrating modern management information systems with digitalization processes (Sotnyk et al., 2020). On the other hand, the Internet may be the most effective means of providing prompt information (Kundeliene & Stepanauskaite, 2018) and influencing economic processes, namely increasing consumer behavior (Rybaczewska et al., 2020). The level of information security undoubtedly affects the social sphere (Vasilyeva et al., 2020; Didenko et al., 2020), especially in terms of ensuring personal data protection as the object of cyber financial fraud (Vasylieva et al., 2020). In the matter of unwillingness to disclose personal data, this issue was resolved by Degutis et al. (2020). An essential aspect of the information space functioning is the state regulation of data protection, implemented by the European Union General Data Protection Regulation (Lăzăroiu et al., 2018; Vorontsova et al., 2020; Petrushenko et al., 2020). In quarantine measures, the digital information space is one of the active sources of social communication, ensuring the population well-being (Vasilyeva et al., 2018; Sułkowski, 2020). However, on the other hand, its use is related to a negative effect, namely the digital deprivation in the population (Kuc-Czarnecka, 2020). The digital information space can be one of the key tools for propaganda and information wars (Lyeonov & Liuta, 2016). Targeted information attacks can lead to fluctuations in the foreign exchange market, securities market, cryptocurrency market, etc. (Sokolovska et al., 2020). According to MacKay & Munro (2012), information wars can lead to changes in the country's political landscape. Although today most information attacks do not reach the level of terrorism, governments use them to gather information, funds, political and social destabilization, etc. (Kenney, 2015). Knapp & Boulton (2006) emphasize that information wars turn from a political and military tool into a commercial problem because they are actively used for industrial espionage. Thus, there is a need to study information flows to identify potential attacks to prevent them.

Undoubtedly, the most popular method for working with big data is artificial intelligence, based on bibliographic and retrospective analyses of Delanoy & Kasztelnik (2020). It has gained the most practical application in the banking sector for information protection, positively affecting the image of banking institutions (Giebe et al., 2019). It is also one of the main prerequisites for introducing corporate social responsibility to increase the information protection in large companies (Hammerström et al., 2019). Such world leaders as the United States and China try to realize their ambitions by using artificial intelligence to espionage information (Obeid et al., 2020). As one of the artificial intelligence areas, data mining has many opportunities to analyze large amounts of information and identify patterns of linear and nonlinear nature (Kuzmenko et al., 2020; Olena & Tetyana, 2020a). Its effectiveness has been proven, for example, in money laundering (Lyeonov et al., 2020). Genetic algorithms are effective tools for studying behavioral patterns, particularly the attitudes of social network users (Olena & Tetyana, 2020b). The main competitor of artificial intelligence is blockchain technology, which gradually gains application in various spheres of life and modern information security systems (Kibaroğlu, 2020). Although such technologies may have a downside, especially in decision-making (Lopez et al., 2019), the risks of implementing Industry 4.0 should be considered (Snieška et al., 2020). The risks related to distortion, loss of information and knowledge, which is relevant for any economic entity and its various areas (Yarovenko et al., 2021; Nitsenko et al., 2019), should also be considered. Undoubtedly, the application of analytical methods for analyzing social networks and global databases has significant potential for identifying potential problems (Belz et al., 2019). Therefore, to detect information intrusions as tools of information attacks, there is a need to use not standard analytical approaches but those that will fully identify this phenomenon, namely the Sedov-Taylor blast wave model.

3. DATA

The authors chose the bubbles by the formation of cybercrime information with the impact of their gaps on the economic agents' reactions in the global digital economic space for the study. Relevant quantitative criteria were selected in the form of daily data based on the results of the global web statistics query for the period from 05.08.2017 to 20.10.2020: the value of information activities that characterize the behavior of entities the activity of which relates to cryptocurrencies, the Internet things, online services, banking, e-commerce, etc., and the importance of information activities that describe cyber threats (Statoperator, 2021).

Figure 1 shows a time series constructed using the EViews analytics package, displaying information that identifies cyber threats. Based on its levels, four information intrusions were identified, i.e., information bubbles, the peak of actions that fell on 11/29/2017, 11/26/2018, 12/03/2019, 06/19/2020. These dates are identified as abnormal levels through the unexpected rapid jump with the subsequent establishment of the previous level of the time series level. We can say that there is a gap between these information activities on cyber incidents.

Figure 2 shows the information activity dynamics describing the economic agents' reactions in the global digital economic space from 05.08.2017 to 20.10.2020. This information reflects the results of responding to the massive cyber threat. Therefore, to study this impact, it is necessary to examine whether there is a link between activities that characterize cyber threats and the economic agents' reactions in the global digital economic space. For this purpose, a correlation coefficient of 0.52 was determined, indicating a noticeable relationship between the selected pair of information activities. It can be argued that the impact of one group of activities will be evident to another, so it is relevant to use information bubbles in the modeling process.

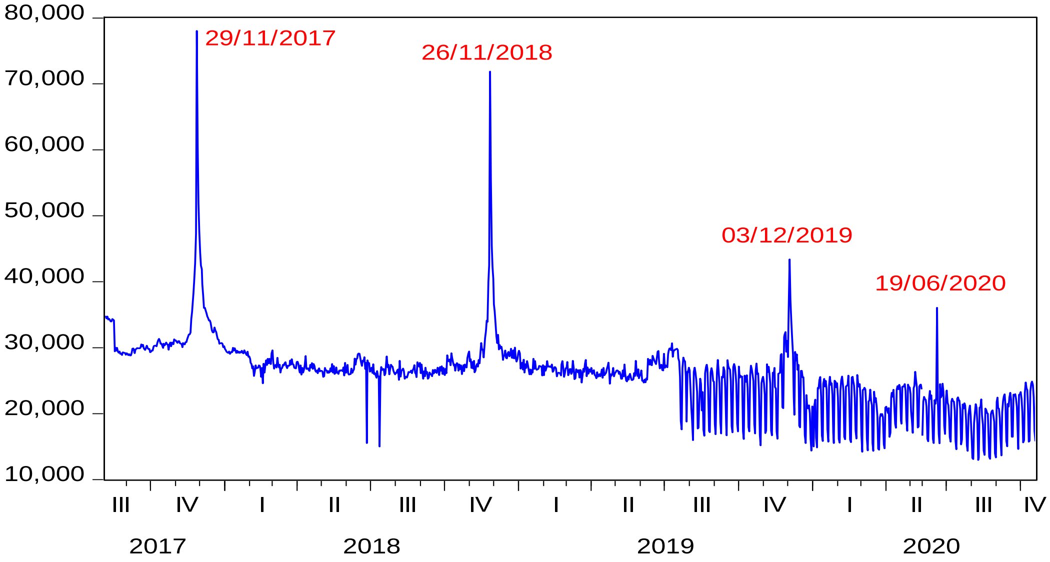


Figure 1. "Information bubbles", detected according to information activities that identify cyber threats in the global digital space, from 05.08.2017 to 20.10.2020

Source: developed by the authors based on Global Web Statistics "Statoperator"

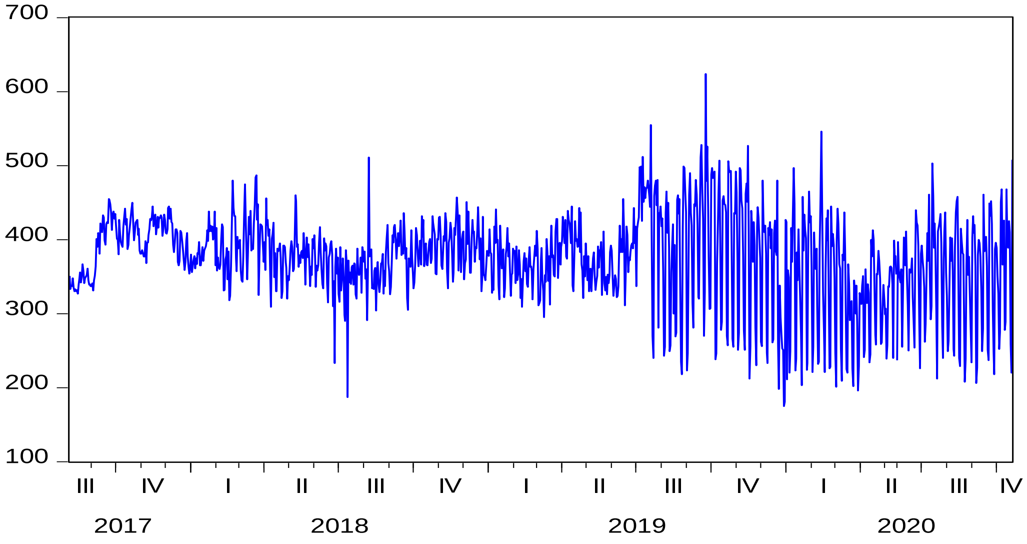


Figure 2. Information activity dynamics that characterize the economic agents' reactions in the global digital economic space, from 05.08.2017 to 20.10.2020

Source: developed by the authors based on Global Web Statistics "Statoperator"

4. METHODOLOGY

The information attacks in the information space and information bubbles can be identified with the explosion and the blast wave extension after it. We hypothesize that the rapid increase in information activities through mentioning the cyber threats, hacker attacks, information leaks, etc., leads to parasitic injection (release of energy) and ends with the rupture of the information bubble, which causes economic agents' appropriate reactions, online transactions. Then, its fluctuations occur for a certain period until its state stabilizes. It is reflected in the relevant activities in the global information space. We use the Sedov-Taylor blast wave model (Sedov, 1959; Taylor, 1950) to test the hypothesis. It will mathematically formalize the spread of the effects made by information attacks as factors destabilizing digital economic transactions in the form of "information bubble" rupture by the formula (1):

$$\begin{gathered} R_s(t) = a \cdot t^b, \\ b = \frac{s+2}{n+2}, a = \left(\frac{E_d/\left(\tau_0^s l_0^{3-n}\right)}{\rho}\right)^{1/(n+2)}, \end{gathered} \tag{1}$$

where R_s – the radius of the shock wavefront in the moment of time (t); n – spatial dimension ($n = 1$ for flat space, $n = 2$ for cylindrical space, $n = 3$ for spherical space); s – energy release rate factor ($s = 0$ for instantaneous release, $s = 1$ for constant rate release); E_d – detonation energy with the following features: l_0 - length, τ_0 - time; ρ – atmospheric air density.

We adapt formula (1) to the model for spreading the results of information attacks in the information space as a factor of digital economic operation destabilization in the country. When describing this system, it makes sense to use four-dimensional space considering the time factor. The quantitative description formula of the blast wave "pressure" of the information bubble rupture and its attenuation tendency, which accompanies the successive energy dissipation as a destabilization factor of economic agents' digital operations, takes the form (2). A similar approach has been used to model financial crises by Bulkin (2016).

$$\Delta R(t) = \frac{E}{t^4} + a_1\left(\frac{E}{t^4}\right)^{3/4} + a_2\left(\frac{E}{t^4}\right)^{2/4} + a_3\left(\frac{E}{t^4}\right)^{1/4}, \tag{2}$$

where $\Delta R(t)$ – change of information activities occurring in the form of information inserts for period t in the global digital space; E – the energy at the initial moment after the rupture of the bubble, i.e., the value of economic agents' losses in the global digital economic space, identified as a change in information activities; t – the time after the rupture of information bubble (number of days); a_1, a_2, a_3 – features of the shock wave extension environment as a result of information intrusions.

In the process of bubble rupture, it is necessary to minimize the economic agents' losses, identified in the form of information entities in the global information space. Therefore, the Sedov-Taylor model can be solved as an optimization problem of nonlinear programming. In terms of each direction of digital economic transaction destabilization, it is necessary to identify the type of information attack and the rupture of the information bubble. The parameters of model (2) should provide the minimum possible level of information activity loss that occur due to the bubble rupture and characterize fluctuations in information flows about actual sector events caused by information messages about cyber threats. There are also other options for destabilizing the country's economy, the results of which are reflected in business, financial, public sectors, etc., considered in the system of optimization model constraints. Given the above, the model of dissemination of the information attacks consequences as a factor of digital economic operations destabilization of the country acquires a general (universal) form (3), which was presented by Yarovenko (2021):

$$\begin{cases} U_i \to min \\ U_i = \sum_{j=1}^{V} U_{ij}^{t_j} = \\ = \sum_{j=1}^{V} \left(\frac{z_{t_j}^i}{\tau_j^i} + a_1 \left(\frac{z_{t_j}^i}{\left(\tau_j^i\right)^2} \right)^{3/4} + a_2 \left(\frac{z_{t_j}^i}{\left(\tau_j^i\right)^3} \right)^{2/4} + a_3 \left(\frac{z_{t_j}^i}{\left(\tau_j^i\right)^4} \right)^{1/4} \right) \end{cases}, \qquad (3)$$

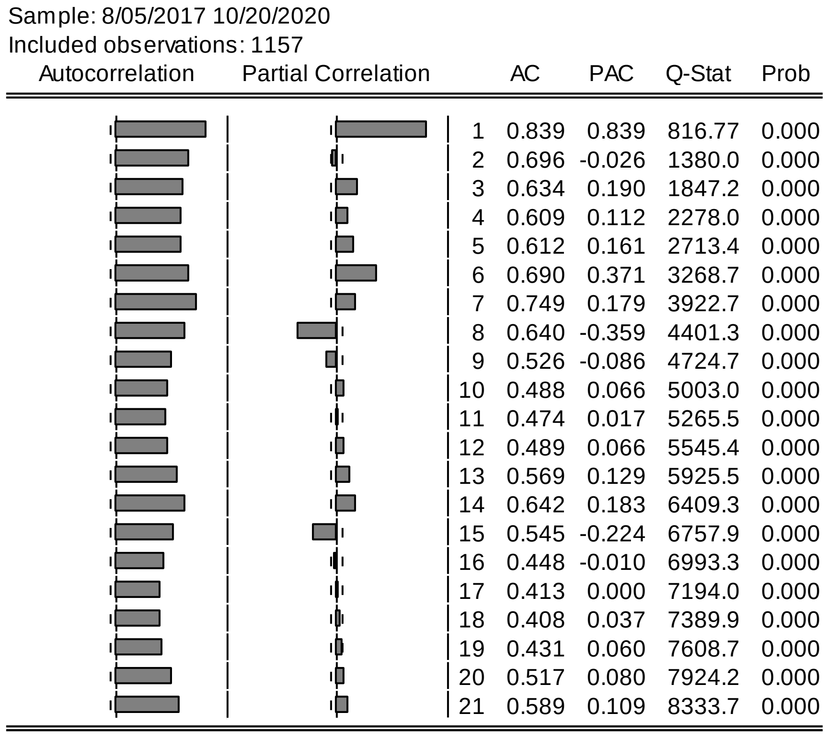
where U_i – scattering of the blast wave energy after the rupture of the information bubble in the first channel of the spread of digital economic operations destabilization in the country; V – the number of information wars (information intrusion, hacker attack, information espionage, information propaganda, etc.). Under the terms of our problem, only information input is considered; $z_{t_j}^i$ – the initial energy at time t_j, i.e., the initial values of information activities on cyber threats before the implementation of the information injection; t_j – time, which corresponds to the lag of the j-level of the time series of information activities on cyber threats in the i-th direction of digital economic operations destabilization in the country; τ_j^i – the duration of the j-type of information war in the i-direction of digital economic operations destabilization in the country.

The practical implementation of formula (3) will model the spread of the information bubbles rupture consequences generated, affected by different information wars, the extension of which is manifested through fluctuations in the information activities regarding the economic agents' performance in the global digital economic space.

5. EMPIRICAL RESULTS

It is necessary to determine the period after the information bubble rupture (number of days) for its spread to calculate the blast wave propagation model regarding the consequences of information attacks and their impact on the destabilization of economic agents' digital operations. To this end, we will perform an autocorrelation analysis using the EViews analytical package for both time-series - quantitative features of information activities on cyber threats and the economic agents' response in the global digital economic space (Figures 3-4).

The results of the analysis on the autocorrelation functions, presented in Figure 3, allow us to conclude that there are fluctuations in the time series of activities against cyber threats, which occur every seven days. Similarly, every seven days, there are periodic fluctuations in the time series of activities on the economic agents' response in the global digital economic space (Figure 4). This synchronicity suggests that changes in one-time series are related to another. It means that there may be the dissemination of information about cyber threats during this period, which affects changes in information activities on the economic agents' reactions. Therefore, after the rupture of the information bubble for its distribution, we choose seven days.

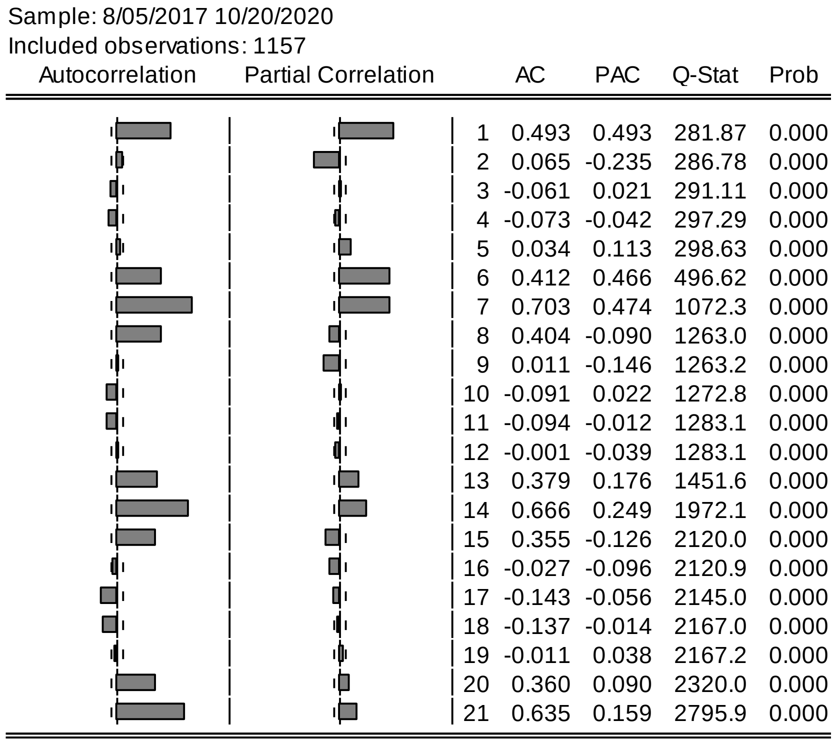


Sample: 8/05/2017 10/20/2020
Included observations: 1157

Autocorrelation	Partial Correlation		AC	PAC	Q-Stat	Prob
		1	0.839	0.839	816.77	0.000
		2	0.696	-0.026	1380.0	0.000
		3	0.634	0.190	1847.2	0.000
		4	0.609	0.112	2278.0	0.000
		5	0.612	0.161	2713.4	0.000
		6	0.690	0.371	3268.7	0.000
		7	0.749	0.179	3922.7	0.000
		8	0.640	-0.359	4401.3	0.000
		9	0.526	-0.086	4724.7	0.000
		10	0.488	0.066	5003.0	0.000
		11	0.474	0.017	5265.5	0.000
		12	0.489	0.066	5545.4	0.000
		13	0.569	0.129	5925.5	0.000
		14	0.642	0.183	6409.3	0.000
		15	0.545	-0.224	6757.9	0.000
		16	0.448	-0.010	6993.3	0.000
		17	0.413	0.000	7194.0	0.000
		18	0.408	0.037	7389.9	0.000
		19	0.431	0.060	7608.7	0.000
		20	0.517	0.080	7924.2	0.000
		21	0.589	0.109	8333.7	0.000

Figure 3. Autocorrelation analysis on time series of information activities on cyber threats

Source: Authors' calculations



Sample: 8/05/2017 10/20/2020
Included observations: 1157

Autocorrelation	Partial Correlation		AC	PAC	Q-Stat	Prob
		1	0.493	0.493	281.87	0.000
		2	0.065	-0.235	286.78	0.000
		3	-0.061	0.021	291.11	0.000
		4	-0.073	-0.042	297.29	0.000
		5	0.034	0.113	298.63	0.000
		6	0.412	0.466	496.62	0.000
		7	0.703	0.474	1072.3	0.000
		8	0.404	-0.090	1263.0	0.000
		9	0.011	-0.146	1263.2	0.000
		10	-0.091	0.022	1272.8	0.000
		11	-0.094	-0.012	1283.1	0.000
		12	-0.001	-0.039	1283.1	0.000
		13	0.379	0.176	1451.6	0.000
		14	0.666	0.249	1972.1	0.000
		15	0.355	-0.126	2120.0	0.000
		16	-0.027	-0.096	2120.9	0.000
		17	-0.143	-0.056	2145.0	0.000
		18	-0.137	-0.014	2167.0	0.000
		19	-0.011	0.038	2167.2	0.000
		20	0.360	0.090	2320.0	0.000
		21	0.635	0.159	2795.9	0.000

Figure 4. Autocorrelation analysis on time series of information activities on the economic agents' reaction in the global digital economic space

Source: Authors' calculations

After the information bubble rupture, the blast wave will spread in any case, but its consequences may not reach the real sector. If it occurs, they may not have a significant impact. We calculate the initial energy of ruptures of certain information bubbles on the set dates according to formula (2). The results of the calculations are presented in Table 1.

Table 1

Initial energy of information bubbles rupture

Date	Cyber Threats	Digital economy	ΔR	E/t^4	$(E/t^4)^{3/4}$	$(E/t^4)^{2/4}$	$(E/t^4)^{1/4}$
27.11.2017	78044	405	-25	32.50	13.61	5.70	2.39
26.11.2018	71898	433	75	29.95	12.80	5.47	2.34
03.12.2019	43396	480	224	18.07	8.77	4.25	2.06
19.06.2020	36057	375	17	15.02	7.63	3.88	1.97

Source: Authors' calculations

At the next stage of calculating the blast wave model of the information attacks to destabilize the economic agents' digital operations, we find the coefficients of the blast energy scattering model. Given the initial levels of burst energy of the information bubbles presented in Table 1 and the seven days of bubble extension after its rupture identified by autocorrelation analysis, we write the optimization model (3) as the following system of equations (4). Equations are used in the context of each rupture of the information bubble. The values of the Sedov-Taylor function were equal to the absolute increments of the current level of the time series activities in the digital economy to their previous level.

$$\begin{cases} \frac{78044}{7^4} + a_1\left(\frac{78044}{7^4}\right)^{\frac{3}{4}} + a_2\left(\frac{78044}{7^4}\right)^{\frac{2}{4}} + a_3\left(\frac{78044}{7^4}\right)^{\frac{1}{4}} \to min \\ \frac{78044}{7^4} + a_1\left(\frac{78044}{7^4}\right)^{\frac{3}{4}} + a_2\left(\frac{78044}{7^4}\right)^{\frac{2}{4}} + a_3\left(\frac{78044}{7^4}\right)^{\frac{1}{4}} = -25 \\ \frac{71898}{7^4} + a_1\left(\frac{71898}{7^4}\right)^{\frac{3}{4}} + a_2\left(\frac{71898}{7^4}\right)^{\frac{2}{4}} + a_3\left(\frac{71898}{7^4}\right)^{\frac{1}{4}} = 75 \\ \frac{43396}{7^4} + a_1\left(\frac{43396}{7^4}\right)^{\frac{3}{4}} + a_2\left(\frac{43396}{7^4}\right)^{\frac{2}{4}} + a_3\left(\frac{43396}{7^4}\right)^{\frac{1}{4}} = 224 \\ \frac{36057}{7^4} + a_1\left(\frac{36057}{7^4}\right)^{\frac{3}{4}} + a_2\left(\frac{36057}{7^4}\right)^{\frac{2}{4}} + a_3\left(\frac{36057}{7^4}\right)^{\frac{1}{4}} = 17 \end{cases} \tag{4}$$

The search of the blast wave extension coefficients regarding the consequences of information attacks to destabilize the economic agents' digital operations in the formula (4) is performed using the generalized reduced gradient method in the tool Solution Search software MS Excel. The direct solution of the equations system (4) considers the coefficients using the software application Mathcad. Then, a model of information attacks extension is formed as a result of information bubble rupture as a destabilizing factor of economic agents' digital operations via the equation (5):

$$y(x) := x + -1735.63859 \cdot x^{\frac{3}{4}} + 7526.0874 \cdot x^{\frac{2}{4}} + -8088.55 \cdot x^{\frac{1}{4}} \tag{5}$$

We have constructed a graph of the information attacks extension as a destabilizing factor of economic agents' digital operations in the country to visualize the blast wave extension model after the rupture of the "information bubble" (Figure 5) in the software application "Mathcad". The nature of the curve in Figure 5, i.e., its growth after the critical decline, indicates the breakpoint of the second kind, which accompanies the rupture of the "information bubble" with the subsequent adaptation of the system and combating the shock wave effects.

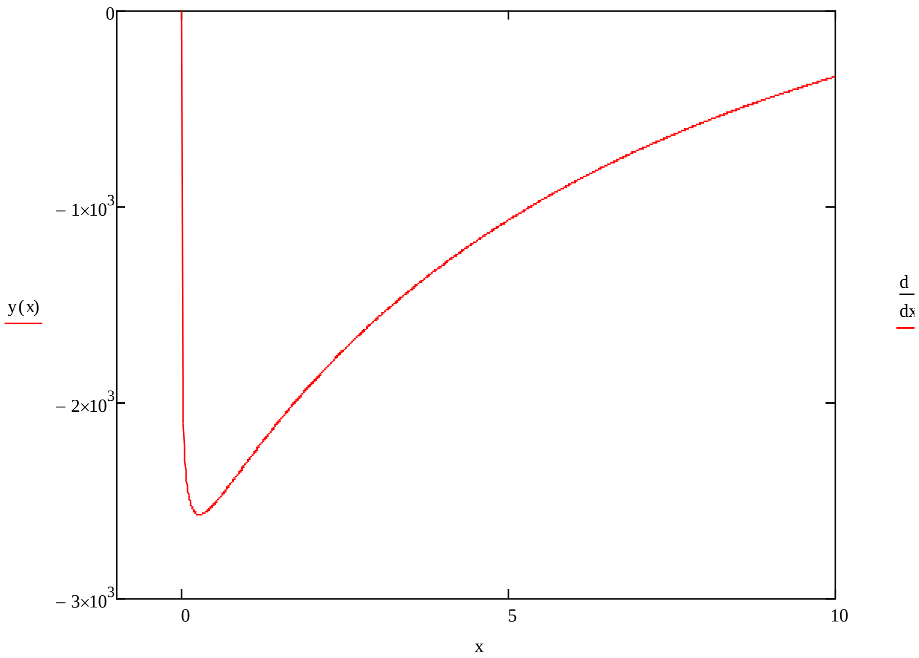


Figure 5. Graphical representation of the model of information attacks extension as a destabilizing factor of economic agents' digital operations

Source: Authors' calculations

We find the value $\frac{E}{t^4}$, using which the absolute increase in the current level of information activities on the digital economy to the previous level will be zero. For this purpose, function (5) is equated to zero. The corresponding result is presented in the form of a matrix (6):

$$\begin{pmatrix} 2.845857250858869264\text{2e}12 \\ 0.25880665931218240 41 - 4.781365653050416083\text{6e-22}i \\ 22.701480114635548483 + 4.478085629413948289\text{e-21}i \end{pmatrix} \tag{6}$$

The obtained value $\frac{E}{t^4} = 2{,}85 \cdot 10^{12}$ indicates the constant volatility of the activity level concerning the digital economy and the almost inability to achieve zero value of its absolute growth. In practice, it means that there will be fluctuations in information activities, i.e., interest in the object will constantly be changing.

We conduct additional research using the differential calculus and find: 1) the points of the function inflexion, which identify levels of information activities on cyber threats, which will change the consequences of the "information bubble" rupture, identified by activities; 2) extreme points of the function, which will determine the peak values of the information activities on cyber threats, at which the maximum and/or minimum possible levels of activity on the digital economy will be achieved.

To solve the first task, we determine the first derivative of function (5) for the corresponding variable, the equation of which is presented as function 7, and the graph is shown in Figure 6, using the software application "Mathcad":

$$\frac{d}{dx}y(x) \rightarrow \frac{3763.0437}{\sqrt{x}} - \frac{1301.7289425}{x^{\frac{1}{4}}} - \frac{2022.1375}{x^{\frac{3}{4}}} + 1 \quad (7)$$

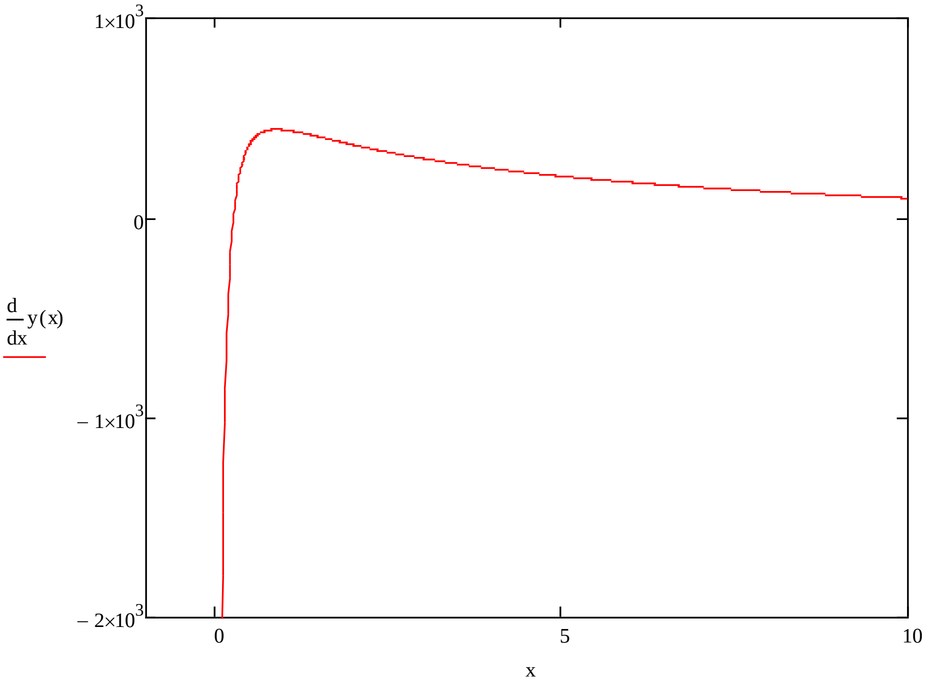


Figure 6. Graphical representation of the first derivative model function regarding the information attacks consequences as a destabilizing factor of economic agents' digital operations

Source: Authors' calculations

Figure 6 shows an increase in the information activity on the digital economy due to the "information bubble" rupture initiated by the rise in the information activity on cyber threats. This process reaches the level of 0.879 for the variable $\frac{E}{t^4}$; the absolute growth of digital economy activities will be 536 units. It will happen the day after the rupture of the "information bubble". After this peak, the increase in the information activities on cyber threats will be accompanied by a decrease in the information activities in the digital economy.

To solve the second task, we define the extreme points of the function, i.e., find the value of the activity on cyber threats, which will achieve the maximum and minimum possible action on the digital economy. For this purpose, we take the second derivative of function (5), the result of which takes the form (8):

$$\frac{d^2}{dx^2}y(x) \rightarrow \frac{325.432235625}{x^{\frac{5}{4}}} + \frac{1516.603125}{x^{\frac{7}{4}}} - \frac{1881.52185}{x^{\frac{3}{2}}} \quad (8)$$

Using the obtained results, we construct the function of the second derivative model describing the blast wave regarding the spread of the information attacks consequences as a destabilizing factor of economic agents' digital operations in the country (Figure 7).

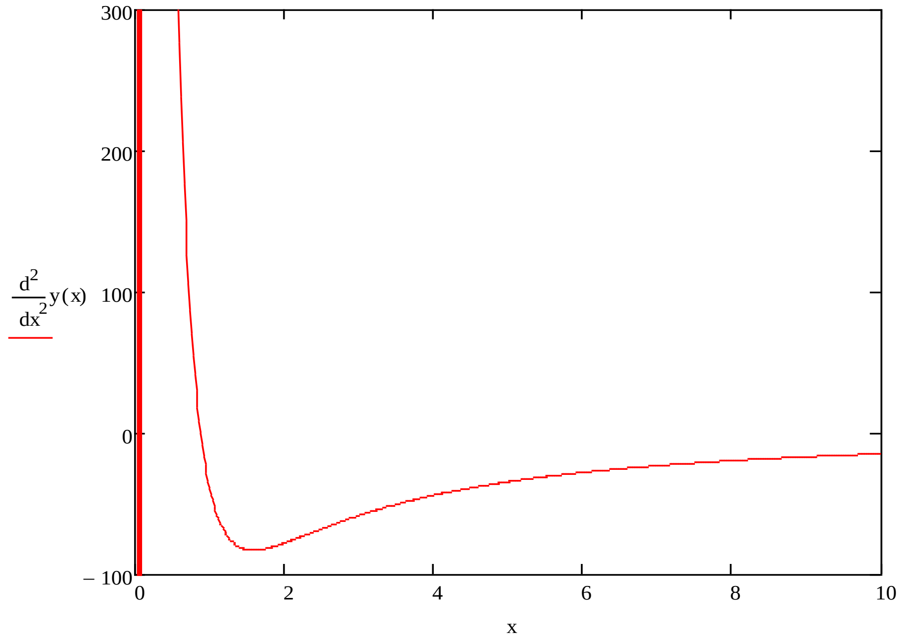


Figure 7. Graphical representation of the second derivative model function regarding the spread of the information attacks consequences as a destabilizing factor of economic agents' digital operations in the country

Source: Authors' calculations

Analysis of the graph shows that the extreme minimum possible value of the absolute increase in the information activities concerning the digital economy is -80 units. At the level of the variable $\frac{E}{t^4}$, about 1.5 units, i.e., there is a decrease in their growth. Stabilization of their level will begin after the tenth day from the "information bubble" rupture, i.e., during this time, there will be a decline in information activity in the real sector of the digital economy. A ten-day period is sufficient for the information space to stabilize the information flows for a specific object.

6. CONCLUSION

Over the last decade, information wars have become a real weapon for countries struggling for supremacy in the world economic and political arenas. Its most effective measures are information outbursts, which lead to the spread of panic among the population or fluctuations in the foreign exchange market, securities market, among the digital economy subjects, etc. The authors consider that the growth of information activities on specific objects in the information warfare conditions leads to information injection, i.e., there is an analogy between this process and the process of bubbling, the rupture of which is like the blast wave process. Therefore, this paper proposes using the Sedov-Taylor blast wave model to spread the consequences of information attacks as a factor in destabilizing the economic agents' digital operations. This model was considered for four-dimensional space, considering the time factor affecting the information flow change in digital space. The model was also adapted to disseminate the effects of the information bubble rupture formed under the influence of information activities on cyber threats for the information activities dissemination channel that identify the results of the real economy sector subjects' reactions. Empirical data are selected to implement the model. It reflects the change in information activities in the global digital space and characterizes the cyber threats and digital economy reactions as the most active part. It is determined that there is a moderate relationship between these indicators, making it possible to implement the Sedov-Taylor model. There was also a large-scale information overload due to cyberattacks, which led to the rupture of four "information bubbles" in the world in three years. Construction and analysis of autocorrelation functions revealed that the spread of misinformation occurs within seven days and is repeated with this frequency. As a result of the "information bubble" rupture, the absolute growth of activities in the digital economy reaches 536 units. The reaction of the real sector of the economy in the information space begins the day after the rupture. The digital economic operation destabilization lasts for ten days, after which there will be an increase in information activity to the current average level. In other words, the ten-day effect of the information drop may be sufficient to cause negative consequences for economic entities.

The same models might be used as an information weapon that can help identify some threatening factors destabilizing the information space, the most vulnerable areas of the information security system, and predict potential scenarios for possible negative consequences of information wars. Therefore, it is proposed to use it to predict the possible "information bubbles" generated by information activities in the global digital space and predict the quantitative and temporal features of their rupture spread. It will allow government agencies to introduce preventive measures that will help maximize the impact of information attacks on the real sector. The application of this model is appropriate for response groups to cyber incidents and information wars.

ACKNOWLEDGEMENT

The work was performed within the framework of state budget research: № 0121U109559 "National security through the convergence of financial monitoring and cybersecurity systems: intelligent modeling of financial market regulation mechanisms"; № 0121U100467 "Data-Mining to combat cyber fraud and legalization of criminal proceeds in the context of financial sector digitalization in the Ukraine's economy."

REFERENCES

Afonasova, M.A., Panfilova, E.E., Galichkina, M.A, & Ślusarczyk, B. (2019). Digitalization in Economy and Innovation: The Effect on Social and Economic Processes. *Polish Journal of Management Studies, 19(2)*, 22-32. doi:10.17512/pjms.2019.19.2.02.

Baranauskas, G. (2020). Digitalization Impact on Transformations of Mass Customization Concept: Conceptual Modelling of Online Customization Frameworks. *Marketing and Management of Innovations, 3*, 120-132. doi:10.21272/mmi.2020.3-09.

Belz, G., Wawrzynek, L., & Wasowicz, M. (2019). Network Potential of Innovation in Digital Transformation Projects. *Transformations in Business & Economics, 18,* 2B(47B), 694-709. Retrieved April 30, 2021 from http://www.transformations.knf.vu.lt/47b/article/netw.

Bilan, Y., Pimonenko, T., & Starchenko, L. (2020a). Sustainable business models for innovation and success: Bibliometric analysis. Paper presented at the *E3S Web of Conferences, 159.* doi: 10.1051/e3sconf/202015904037.

Bilan, Y., Rubanov, P., Vasylieva, T., & Lyeonov, S. (2019a). The influence of industry 4.0 on financial services: Determinants of alternative finance development. [Wpływ przemysłu 4.0 na usługi finansowe: determinanty rozwoju alternatywnych finansów]. *Polish Journal of Management Studies, 19(1)*, 70–93. doi:10.17512/pjms.2019.19.1.06.

Bilan, Y., Tiutiunyk, I., Lyeonov, S., & Vasylieva, T. (2020b). Shadow economy and economic development: A panel cointegration and causality analysis. *International Journal of Economic Policy in Emerging Economies, 13(2)*, 173-193. doi: 10.1504/IJEPEE.2020.107929.

Bilan, Y., Vasilyeva, T., Kryklii, O., & Shilimbetova, G. (2019b). The creative industry as a factor in the development of the economy: Dissemination of european experience in the countries with economies in transition. [Kūrybinė industrija kaip ekonomikos plėtros veiksnys: Europietiškosios patirties sklaida pereinamojo laikotarpio ekonomikos šalyse]. *Creativity Studies, 12(1)*, 75-101. doi: 10.3846/cs.2019.7453.

Bondarenko, A. F., Zakharkina, L. S., Syhyda, L. O., & Saher, L. Y. (2020). The economic and marketing attractiveness of countries: Measurement and positioning in terms of economic security. *International Journal of Sustainable Development and Planning, 15(4)*, 439-449. doi: 10.18280/ijsdp.150404.

Brychko, M., Bilan, Y., Lyeonov, S., & Mentel, G. (2021). Trust crisis in the financial sector and macroeconomic stability: A structural equation modelling approach. *Economic Research-Ekonomska Istrazivanja, 34(1)*, 828-855. doi:10.1080/1331677X.2020.1804970.

Bulkin, S.M. (2016). Udarno-khvylova model poshyrennia finansovoi kryzy | [The shock wave model of the spread of the financial crisis]. *Prometei: rehionalnyi zbirnyk naukovykh prats z ekonomiky | [Prometheus: a regional collection of scientific papers on economics]*. 1(46). 132-140. Retrieved April 30, 2021 from http://projects.dune-hd.com/bitstream/handle/2010/31452/ZE_2019_142.pdf?sequence=1&isAllowed=y [in Ukrainian].

Chigrin, O., & Pimonenko, T. (2014). The ways of corporate sector firms financing for sustainability of performance. *International Journal of Ecology and Development, 29(3)*, 1-13. Retrieved April 30, 2021 from https://www.scopus.com/record/display.uri?eid=2-s2.0-84904394388&origin=resultslist&sort=plf-f.

Cosmulese, C.G., Grosu, V, Hlaciuc, E., & Zhavoronok, A. (2019). The Influences of the Digital Revolution on the Educational System of the EU Countries. *Marketing and Management of Innovations, 3*, 242-254. doi:10.21272/mmi.2019.3-18.

Cvetićanin, N. (2020). *The largest battlefield in history – 30 Cyber warfare statistics*. Retrieved April 30, 2021 from DataProt WebSite: https://dataprot.net/statistics/cyber-warfare-statistics/.

Delanoy, N., & Kasztelnik, K. (2020). Business Open Big Data Analytics to Support Innovative Leadership Decision in Canada. *Business Ethics and Leadership, 4(2)*, 56-74. doi: 10.21272/bel.4(2).56-74.2020.

Degutis, M., Urbonavicius, S., Zimaitis, I., Skare, V., & Laurutyte, D. (2020). Willingness to Disclose Personal Information: How to Measure It? *Inzinerine Ekonomika-Engineering Economics, 31(4)*, 487–494. doi:10.5755/j01.ee.31.4.25168.

Didenko, I., Paucz-Olszewska, J., Lyeonov, S., Ostrowska-Dankiewicz, A., & Ciekanowski, Z. (2020). Social safety and behavioral aspects of populations financial inclusion: A multicountry analysis. *Journal of International Studies, 13(2)*, 347-359. doi: 10.14254/2071-8330.2020/13-2/23.

Giebe, C., Hammerström, L., & Zwerenz, D. (2019). Big Data & Analytics as a sustainable Customer Loyalty Instrument in Banking and Finance. *Financial Markets, Institutions and Risks, 3(4)*, 74-88. doi: 10.21272/fmir.3(4).74-88.2019.

Hammerström, L., Giebe, C., & Zwerenz, D. (2019). Influence of Big Data & Analytics on Corporate Social Responsibility. *SocioEconomic Challenges, 3(3)*, 47-60. doi: 10.21272/sec.3(3).47-60.2019.

Kenney, M. (2015) Cyber-Terrorism in a Post-Stuxnet World. *Orbis, 59(1)*, 111-128. doi: 10.1016/j.orbis.2014.11.009.

Kibaroğlu, O. (2020). Self Sovereign Digital Identity on the Blockchain: A Discourse Analysis. *Financial Markets, Institutions and Risks, 4(2)*, 65-79. doi: 10.21272/fmir.4(2).65-79.2020.

Knapp, K.J, & Boulton, W.R. (2006) Cyber-warfare threatens corporations: Expansion into commercial environments. *Information Systems Management, 23(2)*, 76-87. doi: 10.1201/1078.10580530/45925.23.2.20060301/92675.8.

Kotenko, N., & Bohnhardt, V. (2021). Digital health projects financing: challenges and opportunities. *Health Economics and Management Review, 2(1)*, 100-107. doi: 10.21272/hem.2021.1-10.

Kundeliene, K., & Stepanauskaite, A. (2018). Information Disclosure and its Determinants on Lithuanian Companies' Websites: A Quantitative Approach. *Inzinerine Ekonomika-Engineering Economics, 29(4)*, 455–467. doi:10.57.55/j01.ee.29.4.17271.

Kuc-Czarnecka, M. (2020). COVID-19 and digital deprivation in Poland. *Oeconomia Copernicana, 11(3)*, 415–431. doi:10.24136/oc.2020.017.

Kuzmenko, O., Šuleř, P., Lyeonov, S., Judrupa, I., & Boiko, A. (2020). Data mining and bifurcation analysis of the risk of money laundering with the involvement of financial institutions. *Journal of International Studies, 13(3)*, 332-339. doi: 10.14254/2071-8330.2020/13-3/22.

Lăzăroiu, G., Kovacova, M., Kliestikova, J., Kubala, P., Valaskova, K., & Dengov, V. V. (2018). Data governance and automated individual decision-making in the digital privacy General Data Protection Regulation. *Administratie si Management Public, 31*, 132-142, doi: 10.24818/amp/2018.31-09.

Leonov, S., Yarovenko, H., Boiko, A., & Dotsenko, T. (2019). Information system for monitoring banking transactions related to money laundering. Paper presented at the *CEUR Workshop Proceedings, 2422*, 297-307. Retrieved April 30, 2021 from https://www.scopus.com/record/display.uri?eid=2-s2.0-85071081226&origin=resultslist.

Lopez, B.S., García, D.I., & Alcaide, A.V. (2019). Blockchain Technology Facing Socioeconomic Challenges. Promise versus Probability. *SocioEconomic Challenges, 3(4)*, 13-24. doi: 10.21272/sec.3(4).13-24.2019.

Lyeonov, S., & Liuta, O. (2016). Actual problems of finance teaching in Ukraine in the post-crisis period. The financial crisis: Implications for research and teaching (pp. 145-152) doi: 10.1007/978-3-319-20588-5_07.

Lyeonov, S., Żurakowska-Sawa, J., Kuzmenko, O., & Koibichuk, V. (2020). Gravitational and intellectual data analysis to assess the money laundering risk of financial institutions. *Journal of International Studies, 13(4)*, 259-272. doi:10.14254/2071-8330.2020/13-4/18.

MacKay, B., & Munro, I. (2012) Information Warfare and New Organizational Landscapes: An Inquiry into the ExxonMobil-Greenpeace Dispute over Climate Change. *Organization Studies, 33(11)*, 1507-1536. doi:10.1177/0170840612463318.

Miskiewicz, R. (2020). Internet of Things in Marketing: Bibliometric Analysis. *Marketing and Management of Innovations, 3*, 371-381. doi: 10.21272/mmi.2020.3-27.

Moradi, M. (2021). Importance of Internet of Things (IoT) in Marketing Research and Its Ethical and Data Privacy Challenges. *Business Ethics and Leadership, 5(1)*, 22-30. doi: 10.21272/bel.5(1).22-30.2021.

Nitsenko, V., Mardani, A., Streimikis, J., Ishchenko, M., Chaikovsky, M., Stoyanova-Koval, S., & Arutiunian, R. (2019). Automatic Information System of Risk Assessment for Agricultural Enterprises of Ukraine. *Montenegrin Journal of Economics, 15(2)*, 139-152. 10.14254/1800-5845/2019.15-2.11.

Obeid, H., Hillani, F, Fakih, R., & Mozannar, K. (2020). Artificial Intelligence: Serving American Security and Chinese Ambitions. *Financial Markets, Institutions and Risks, 4(3)*, 42-52. doi: 10.21272/fmir.4(3).42-52.2020.

Olena, S., & Tetyana, V. (2020a). Comparison of open learning forms in organizational education. Paper presented at the *CEUR Workshop Proceedings, 2732*, 1314-1328. Retrieved April 30, 2021 from https://www.scopus.com/record/display.uri?eid=2-s2.0-85096131621&origin=resultslist.

Olena, S., & Tetyana, V. (2020b). Neuro-genetic hybrid system for management of organizational development measures. Paper presented at the *CEUR Workshop Proceedings, 2732*, 411-422. Retrieved April 30, 2021 from https://www.scopus.com/record/display.uri?eid=2-s2.0-85096109482&origin=resultslist.

Petroye, O., Lyulyov, O., Lytvynchuk, I., Paida, Y., & Pakhomov, V. (2020). Effects of information security and innovations on Country's image: Governance aspect. *International Journal of Safety and Security Engineering, 10(4)*, 459-466. doi: 10.18280/ijsse.100404.

Petrushenko, Y., Kozarezenko, L., Glinska-Newes, A., Tokarenko, M., & But, M. (2018). The opportunities of engaging FinTech companies into the system of crossborder money transfers in Ukraine. *Investment Management and Financial Innovations, 15(4)*, 332-344. doi: 10.21511/imfi.15(4).2018.27.

Petrushenko, Y., Vadym, A., Vorontsova, A., & Ponomarenko, O. (2020). Sustainable development goals as a tool for strategic planning in communities: A bibliometric analysis of research. Paper presented at the *E3S Web of Conferences, 202*. doi: 10.1051/e3sconf/202020203005.

PurpleSec LLC (2021). *2021 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends*. Retrieved April 30, 2021 from https://purplesec.us/resources/cyber-security-statistics/.

Rybaczewska, M., Chesire, B. J., & Sparks, L. (2020). YouTube Vloggers as Brand Influencers on Consumer Purchase Behaviour. *Journal of Intercultural Management, 12(2)*, 117-140. doi: 10.2478/joim-2020-0047.

Sedov, L.I. (1959). *Similarity and Dimensional Methods in Mechanics*. New York: Academic Press.

Skrynnyk, O. (2020a). Some Aspects of Information Security in Digital Organizational Management System. *Marketing and Management of Innovations, 4*, 279-289. doi: 10.21272/mmi.2020.4-23.

Skrynnyk, O. (2020b). Surrogate Leadership Model for Digital Organizational Systems. *Business Ethics and Leadership, 4(4)*, 140-146. doi: 10.21272/bel.4(4).140-146.2020.

Snieška, V., Navickas, V., Havierniková, K., Okręglicka, M., & Gajda, W. (2020). Technical, information and innovation risks of industry 4.0 in small and medium-sized enterprises – case of Slovakia and Poland. *Journal of Business Economics and Management, 21(5)*, 1269-1284. doi: 10.3846/jbem.2020.12279.

Sokolovska, A., Zatonatska, T., Stavytskyy, A., Lyulyov, O., & Giedraitis, V. (2020). The impact of globalization and international tax competition on tax policies. *Research in World Economy, 11(4)*, 1-15. doi: 10.5430/rwe.v11n4p1.

Sotnyk, I., Zavrazhnyi, K., Kasianenko, V., Roubík H. & Sidorov O. (2020). Investment Management of Business Digital Innovations. *Marketing and Management of Innovations, 1*, 95-109. doi: 10.21272/mmi.2020.1-07.

Statoperator (2021). *Global Web Statistics*. Retrieved April 30, 2021 from https://statoperator.com/.

Stukalo, N., Lytvyn, M., Petrushenko, Y., & Omelchenko, Y. (2020). The achievement of the country's sustainable development in the conditions of global threats. Paper presented at the *E3S Web of Conferences, 211*. doi:10.1051/e3sconf/202021101029.

Sułkowski, Ł. (2020). Covid-19 Pandemic; Recession, Virtual Revolution Leading to De-globalization? *Journal of Intercultural Management, 12(1)*, 1-11. doi: 10.2478/joim-2020-0029.

Taylor, G. I. (1950). The formation of a blast wave by a very intense explosion I. Theoretical discussion. Proceedings of the Royal Society of London. Series A. *Mathematical and Physical Sciences, 201(1065)*, 159-174. doi:10.1098/rspa.1950.0049.

Tiutiunyk, I., Humenna, Yu., & Flaumer, A. (2021). Covid-19 impact on business sector activity in the EU countries: digital issues. *Health Economics and Management Review, 2(1)*, 54-66. doi: 10.21272/hem.2021.1-06.

Vasilyeva, T., Bilan, S., Bagmet, K., & Seliga, R. (2020). Institutional development gap in the social sector: Crosscountry analysis. *Economics and Sociology, 13(1)*, 271-294. doi: 10.14254/2071-789X.2020/13-1/17.

Vasilyeva, T., Lyeonov, S., Adamičková, I., & Bagmet, K. (2018). Institutional quality of social sector: The essence and measurements. *Economics and Sociology, 2018, 11(2),* 248–262. doi: 10.14254/2071-789X.2018/11-2/17.

Vasylieva, T., Jurgilewicz, O., Poliakh, S., Tvaronavičienė, M., & Hydzik, P. (2020). Problems of measuring country's financial security. *Journal of International Studies, 13(2)*, 329-346. doi: 10.14254/2071-8330.2020/13-2/22.

Vorontsova, A., Vasylieva, T., Bilan, Y., Ostasz, G., & Mayboroda, T. (2020). The influence of state regulation of education for achieving the sustainable development goals: Case study of central and eastern European countries. *Administratie Si Management Public, 2020(34)*, 6-26. doi: 10.24818/amp/2020.34-01.

World Economic Forum (2021). *Wild Wide Web. Consequences of Digital Fragmentation.* Retrieved April 30, 2021 from https://reports.weforum.org/global-risks-report-2020/wild-wide-web/.

Yarovenko, H. (2021). Information Security as a Driver of National Economic Development. *(Doctoral dissertation)*. Retrieved April 30, 2021 from SumDU Repository: https://essuir.sumdu.edu.ua/handle/123456789/83664 [in Ukrainian].

Yarovenko, H., Bilan, Y., Lyeonov, S., & Mentel, G. (2021). Methodology for assessing the risk associated with information and knowledge loss management. *Journal of Business Economics and Management, 22(2)*, 369-387. doi:10.3846/jbem.2021.13925.