Бізнес, кібербезпека, інформаційне право. Економіка

УДК 657:004.056

Mysiuk Roman
Assistant at the Department
Ivan Franko National University of Lviv
Мисюк Роман Володимирович
асистент кафедри
Львівського національного університету імені Івана Франка
ORCID: 0000-0002-7843-7646

Fedorchak Oleksii
PhD in Economics
OnePet, USA
Федорчак Олексій Євстахійович
кандидат економічних наук
OnePet, США
ORCID: 0000-0002-0767-8346

Rorat Ivan
Postgraduate Student of the
Lviv University of Business and Law
Рорат Іван Степанович
аспірант
Львівського університету бізнесу та права
ORCID: 0009-0001-1862-7288

Vizniak Yaroslav
Postgraduate Student of the
Lviv University of Business and Law

Візняк Ярослав Ярославович
аспірант
Львівського університету бізнесу та права
ORCID: 0009-0008-7221-5787

Repeta Pavlo
Postgraduate Student of the
Lviv University of Business and Law
Репета Павло Іванович
аспірант
Львівського університету бізнесу та права
ORCID: 0009-0009-2788-5797

ANALYSIS AND METHODS OF CYBER SECURITY OF BUSINESS STRUCTURES IN SOCIAL NETWORKS
АНАЛІЗ ТА МЕТОДИ КІБЕРБЕЗПЕКИ БІЗНЕС-СТРУКТУР У СОЦІАЛЬНИХ МЕРЕЖАХ

Summary. *Introduction. Ensuring security on the Internet today is an important part of the work of world-famous companies, namely: LinkedIn, Facebook, Twitter, Instagram, which provide, support and develop social networks. Cyber security of business structures needs constant support and improvement based on analysis of its efficiency and effectiveness. This will contribute to the increase of cyber resistance and the development of the business structure in modern conditions.*

Purpose. The purpose of the article is to investigate the main principles of ensuring cyber security of business structures in social networks, taking into account the specifics of information law and the latest technologies.

Materials and methods. Research materials are scientific and reference

literature, practical experience on the outlined topic. In the research process, general scientific and special methods were used, in particular: theoretical generalization, systematization and system analysis, as well as the graphic method.

Results. Theoretical provisions have been improved and practical recommendations have been developed to ensure the cyber security of business structures in social networks, taking into account the specifics of economic activity, information law and the latest technologies. The scientific novelty is the improvement of the system and mechanism of minimizing third-party (external) cybernetic influence, taking into account the corresponding consequences on the personal office of the manager (or administrator) of the business structure in social networks. A description of possible algorithms for data analysis of business structures in social networks as a data collection tool is also added. In addition, possible methods of countermeasures and increasing the security of the pages of administrators and account owners in social networks are evaluated. This is due to the fact that any information collected on the Internet can provoke attackers to launch a cyber attack. Given the impossibility of hacking social networks as a complete system, criminals use hacking of personal accounts of business leaders. The impact of business, economic connections in social networks is also considered to determine the group of people who are engaged in the promotion of goods in social networks. An analysis of the existing methods of ensuring cyber security in the most famous social networks Facebook and Instagram was carried out, taking into account the specifics of economic activity, information law and technologies.

Prospects. In the future, it is recommended to study the types of information systems and technologies in areas enshrined in the integrity of business structures.

Ключові слова: *business, business structure, cyber security, information technology, information, analytics, information law, business risks, user,*

corporate page, social network, result.

Анотація. *Вступ. Забезпечення безпеки в Інтернеті сьогодні є важливою частиною роботи всесвітньо відомих компаній, а саме: LinkedIn, Facebook, Twitter, Instagram, які надають, підтримують та розвивають соціальні мережі. Кібербезпека бізнес-структур потребує постійної підтримки та вдосконалення на основі аналізу її ефективності та результативності. Це сприятиме підвищенню кіберстійкості і розвитку бізнес-структури в сучасних умовах.*

Мета. Метою статті є дослідити основні засади забезпечення кібербезпеки бізнес-структур у соціальних мережах з урахуванням специфіки економічної діяльності, інформаційного права та новітніх технологій.

Матеріали і методи. Матеріалами дослідження є наукова та довідкова література, практичний досвід за окресленою темою. В процесі дослідження використано загальнонаукові та спеціальні методи, зокрема: теоретичного узагальнення, систематизації та системного аналізу, а також графічний метод.

Результати. Удосконалено теоретичні положення й розроблено практичні рекомендації щодо забезпечення кібербезпеки бізнес-структур у соціальних мережах з урахуванням специфіки економічної діяльності, інформаційного права та новітніх технологій. Наукова новизна полягає у вдосконаленні системи й механізму мінімізації стороннього (зовнішнього) кібернетичного впливу з урахуванням відповідних наслідків на особистий кабінет керівника (або адміністратора) бізнес-структури в соціальних мережах. Також додано опис можливих алгоритмів аналізу даних бізнес-структур у соціальних мережах як інструменту збору даних. Крім того, оцінюються можливі методи протидії та підвищення безпеки сторінок адміністраторів і власників акаунтів у соціальних мережах. Це

обумовлено тим, що будь-яка інформація, зібрана в Інтернеті, може спровокувати зловмисників на кібератаку. Враховуючи неможливість зламу соціальних мереж як цілісної системи, зловмисники використовують злом особистих акаунтів керівників бізнес-структур. Вплив ділових, економічних зв'язків у соціальних мережах також розглядається для визначення групи людей, які займаються просуванням товару в соціальних мережах. Проведено аналіз існуючих методів забезпечення кібербезпеки в найвідоміших соціальних мережах Facebook та Instagram з урахуванням специфіки економічної діяльності, інформаційного права та технологій.

Перспективи. У перспективі рекомендується дослідити типи інформаційних систем і технологій за сферами застосування в діяльності бізнес-структури.

Ключові слова: *бізнес, бізнес-структура, кібербезпека, інформаційні технології, інформація, аналітика, інформаційне право, бізнес-ризики, користувач, корпоративна сторінка, соціальна мережа, результат.*

Introduction. Any business initiatives must be balanced with practical security issues. At the same time, it is known that today ensuring the cyber security of a business structure is an important aspect of its successful functioning and development [1]. Here, from the standpoint of the institutional approach, business structures should be understood as: a) business entities that are legal entities that have structural subdivisions and a specific management hierarchy; b) association of business entities that have common business goals [1; 2].

It was established that the cyber security of a business structure is the state of protection of the cyberspace of the business structure as whole or individual objects of its information infrastructure (a computer system, computer data, etc.) from the risk of third-party (external) cyber influence, under which permanence and stability in the implementation of set tasks and achievement of economic

goals are ensured, as well as timely detection, prevention (or counteraction) and neutralization of real and potential challenges, cybernetic interventions and threats to the interests of the business structure [1; 3–10]. Cybersecurity needs constant support and improvement based on the analysis of its efficiency and effectiveness. This will contribute to improving the cyber resilience of the business structure.

Analysis of recent research and publications. According to the results of the research, it was found that the main structural components of cyber security in the system of diagnostics and ensuring the economic security of the business structure are [1]: survey of information and telecommunication systems and cryptosystems of opposing parties; cybernetic influences; protection of one's own information environment in the field of economy and management of business structures.

To minimize or counteract the negative impact of cyber threats and cyber protection of information, a complex system of general and specific measures is necessary: a) organizational, b) technical, c) personnel, and d) legal in nature [9; 10].

The main principles of the system of measures for cyber protection of information (any information and data) in the management of the business structure are [10]: 1) software support; 2) protection of confidential information and effective control of access to information and data; 3) personal responsibility; 4) secrecy and complexity.

Implementation of new or improvement of existing IT solutions in the field of cyber security will make it possible to increase quality, stability and effective management, and in view of the process and result will contribute to the development of the business structure.

Here, in addition to methods of applying information systems and technologies [11; 12], management standards, information processing, data monitoring systems [13; 14], quality criteria (similar to approaches [15-18]),

including aspects of operations research [19; 20] and modeling in the field of cyber security, it is also necessary to take into account decision-making support tools, in particular investment ones [21; 22] in the "type of innovation – type of development" system, to ensure the efficiency and effectiveness of the use of information technologies and systems in the management of the business structure, in conditions of risk, uncertainty, complexity and ambiguity [23–32].

The purpose of the article. The purpose of the article is to investigate the main principles of ensuring cyber security of business structures in social networks, taking into account the specifics of information law and the latest technologies.

Research results.

Methods of Cybersecurity of Business Structures.

Considering the high risk of Widespread cybercrime and cyber insecurity from the technological risk categories of The Global Risks Report 2023 (World Economic Forum), the issue of user security is an important part of the business structure of any company [28]. Business structures usually conduct an advertising campaign on social networks in order to reach the largest possible audience of potential users or buyers of the product. Brand advertising and product promotion takes place in the metaverse with the help of mostly visual presentation of information in social networks.

A. Analytics as a Tool for Identifying Active Authors

All visual information for analytics is present in the Document Object Model structure of the hypertext web page. The process of gathering information for content analytics can be automated using automated testing tools.

Commercial giants usually do not publish content that could potentially be hacked. Information is usually promotional in social networks:

– video up to 30 seconds long with sensitive or controversial content;

– direct link to a web page with a more detailed description for promotion with Search Engine Optimization;

– 2-3 question sentences to attract attention from the first words;

– emoticons and emotions in texts for easier perception and attracting attention.

The frequency of adding posts in social networks is on average 4-5 per day. It was analyzed based on the social networks of Amazon Web Service. Usually, social networks lead special groups of people who select the appropriate context, cooperate with bloggers and famous people, and choose trending things related to products and services. If a web page is hacked, a company can suffer reputational losses that often affect all related products and profits.

The same people can share, comment and like posts on social networks. And it is not an exception that the author of those posts may be among those who spread this information. This may be related to the desire of the authors of the posts to spread the context created by them as best as possible.

For such cases, programs have been developed that, based on information about user activity on the web page, allow you to determine a potential author who has direct rights to upload content to business social networks.

In Fig. the example of analytics process to identify active users based on collected data.

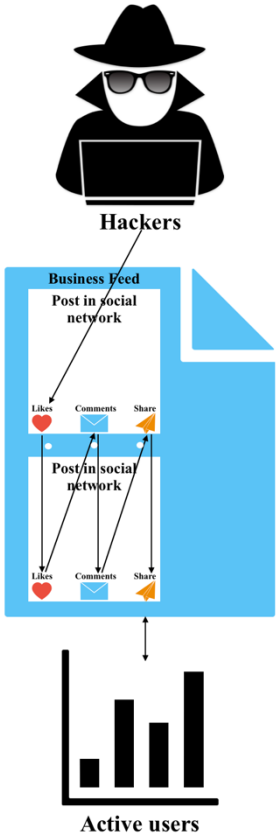

Fig. 1. An example of analytics process of social network content to identify active users

Source: compiled by the authors

The main figure in this scheme is a human attacker, called a hacker. It is not necessarily one person, it can even be a group of people for whom the task of tracking activities in a certain area, both business structure and personal pages, is set.

Tracking takes place with the help of ready-made programs for collecting statistics according to the behavior of users on social networks. Any information about a particular user is of considerable value. An example of collecting information based on user behavior is shown, collecting their likes, comments, and distribution of certain posts for further processing. Tracking takes place obviously not from the personal page of the hacker, but from a third party to make it impossible to attract attention.

You can collect information about a business structure or a personal page using many methods, for example, from the user's news feed. Such information

gives the hacker insight into the most active environment and connections between other leaders or pages.

The next stage of detection is analytics. This stage identifies the influence and security of a certain person in the social network, finding the connection between other team members in the business structure, or identifying the most important person, namely the head of the page. The data may contain many parameters for analysis necessary for a hacker, which, depending on the business structure or topic, he will use against users.

Thus, users are automatically tracked and victims of such a scam are identified. Business structures are a desirable target for hackers due to the large use of virtual money. After all, for inorganic coverage of a certain group of people, there is a virtual payment from Google Ads or any other electronic wallet in social networks. Having hacked the page of the customer of advertising posts or other activities, hackers will mostly stop its distribution and withdraw the remaining funds to their accounts or use it for their own needs.

In order to prevent such an algorithm of actions, the author of the posts should not show excessive activity on the customer's pages.

In large business structures, multifactor checks of received messages or an excessive number of requests, so-called DDoS attacks, are used to prevent hacker attacks. Employees can undergo regular training and tests on the ability to recognize danger from the outside.

Smaller business structures can often be more vulnerable to information leakage or hacking due to smaller staff and correspondingly less technical security capabilities to prevent such attacks.

B. Vulnerabilities of Corporate Connections Through Social Networks

Social networks such as Facebook, Instagram, Twitter and others are protected against various attacks on their resources. Therefore, the personal pages of administrators are often the easiest way. LinkedIn is the largest social network covering business and connecting companies with employees. In the

same way, often in the descriptions of profiles of other social networks, users indicate information about where they work or what they belong to. Similarly, in the LinkedIn social network, anyone can find those who are part of the organization and have relevant skills in promoting the content. Such cases are known as "ducktail". In this way, hackers can bypass the social network's security measures and gain access to users' business accounts. From a legal point of view, cyberattacks can be considered as demanding the transfer of someone else's property, money for restoring access, fraud or others. Another way to collect data from users of social networks is to create wrapper web pages. The theft of information can occur through sites that are very similar in design, but with slightly changed web page hosting. In this way, the user can enter his credentials without suspecting that the password can be quickly changed in the real system and lose access. In this case, a set of different links can also be sent to personal mail with phishing content, even in promotional posts or with a hidden hyperlink under a popular picture or video.

Means and Measures to Prevent the Potential Hacking of Corporate Pages of Social Networks

Data theft is one of the most common ways to perform cyber-attacks [29–31]. Several stages of improving the security of personal pages of business administrators can be distinguished. These steps, in turn, can affect the security of business pages.

To prevent password cracking, use strong and frequently changed application passwords without patterns. Another method is to use geolocation to track logins of the location of the created account.

The next method to avoid being tracked by a hacker can be to check your signed friends and followers. It is better to have only reliable friends who you know personally. In addition, you should avoid open Wi-Fi hotspots, have a privacy policy in place, and avoid clicking on suspicious links.

To prevent access in social networks, one of the stages is two-factor

authentication as it is shown in Fig.. The same options are available in other social networks such as Facebook, Instagram, LinkedIn, Twitter and others. The most common applications for login verification are Duo Security and Microsoft Authenticator. Most often, this happens with a link to a phone number. Users will receive a push request or a code that needs to be entered to access the page from another device or under another IP address.

Fig. 2. Stages of improving security in social networks

Source: compiled by the authors

Access to personal information can be protected by two-factor authentication. However, this can be considered as an additional layer of login protection rather than a requirement. In many cases, users can ignore this possibility and can be hacked much faster.

To ensure security, user should often change passwords to the page and blog or group, sensitive information should be properly protected, and you should have at least one additional page in reserve with access to the personal page or blog for later recovery. Large companies check the integrity of each employee to avoid information leakage.

The security of social network pages is ensured by the developers. Users, for their part, can use the developed options for data protection. Since these mentioned steps are optional and disabled by default for users, all the mentioned steps can improve security and make it harder for social media pages to be hacked.

To ensure security on pages for business structures, the best method would be to use several protected accounts as page administrators at the same time. Each of these methods in combination will allow slow actions of the hacker on the page in social networks.

Conclusions. The work considers the provision of cyber security for the business structure and potential cyber threats. Some types of potentially dangerous places from the point of view of business structure are considered on the social network, namely: analytics of active users and use of corporate connections to identify administrators of individual business pages. The scientific novelty is the improvement of the mechanism of minimizing third-party (external) cybernetic influence, taking into account the relevant consequences, on the personal account of the manager (or administrator) of a business structure in social networks. Proposed possible options for measures and actions to prevent account hacking and cyber-attacks for both employees and businesses. In order to avoid detection of administrators of business pages in social networks, it is possible to minimize input activity through personal accounts. Instead, the use of options for frequent password changes avoiding the use of open Wi-Fi hotspots, location tracking and unspecified login, adding multiple administrators, and the use of additional authentication services provide an opportunity to more effectively protect information and business reputation.

In the future, it is recommended to study the types of information systems and technologies in areas enshrined in the integrity of business structures.

References

1. Skrynkovskyy R., Pawlowski G., Harasym P., Koropetskyi O. (2017). Cybernetic Security and Business Intelligence in the System of Diagnostics of Economic Security of the Enterprise. *Path of Science*, 3(10), 5001–5009. doi: https://doi.org/10.22178/pos.27-6.

2. Skrynkovskyy R., Pawlowski G., Harasym L., Haleliuk M. (2017). Improvement of the Model of Enterprise Management Process on the Basis of General Management Functions. *Path of Science*, 3(12), 4007–4014. https://doi.org/10.22178/pos.29-7.

3. Buriachok V. L., Bohush V. M. (2014). Guidelines for the development and implementation training profile «cyber security» in Ukraine. *Ukrainian Scientific Journal of Information Security*, 20(2). doi: https://doi.org/10.18372/2225-5036.20.7297.

4. Calder A. (2020). *Cyber Security: Essential principles to secure your organisation*. doi: https://doi.org/10.2307/j.ctv10crcbg.

5. Kniaz S., Brych V., Heorhiadi N., Tyrkalo Y., Luchko H., Skrynkovskyy R. (2023). Data Processing Technology in Choosing the Optimal Management Decision System. *2023 13th International Conference on Advanced Computer Information Technologies (ACIT)*, Wrocław, Poland, 372–375. doi: https://doi.org/10.1109/acit58437.2023.10275581.

6. Skrynkovskyy R., Pavlenchyk N., Tsyuh S., Zanevskyy I., Pavlenchyk A. (2022). Economic-mathematical model of enterprise profit maximization in the system of sustainable development values. *Agricultural and Resource Economics: International Scientific E-Journal*, 8(4), 188–214. doi: https://doi.org/10.51599/are.2022.08.04.09.

7. Mishra A., Alzoubi Y. I., Gill A. Q., Anwar M. J. (2022). Cybersecurity Enterprises Policies: A Comparative Study. *Sensors*, 22(2), 538. doi: https://doi.org/10.3390/s22020538.

8. Alahmari A., Duncan B. (2020). Cybersecurity Risk Management in

Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. doi: https://doi.org/10.1109/cybersa49311.2020.9139638.

9. Popivniak Y. M. (2019). Cybersecurity and Protection of Accounting Data under Conditions of Modern Information Technology. *Business Inform*, 8(499), 150–157. doi: https://doi.org/10.32983/2222-4459-2019-8-150-157.

10. Viter S. A., Svitlyshyn I. I. (2017). Protection of accounting information and cybersecurity of the enterprise. *Economy and Society*, 11, 497–502.

11. Pawlowski G., Skrynkovskyy R., Shpak O., Vizniak Y. (2017). Development of the Model of the System of Managerial Diagnostics of the Enterprise on the Basis of Improvement of Diagnostic Purposes. *Path of Science*, 3(11), 4010–4020. doi: https://doi.org/10.22178/pos.28-9.

12. Yuzevych V., Klyuvak O., Skrynkovskyy R. (2016). Diagnostics of the system of interaction between the government and business in terms of public e-procurement. *Economic Annals-XXI*, 160(7–8), 39–44. doi: https://doi.org/10.21003/ea.v160-08.

13. Mysiuk R. V., Yuzevych V. M., Yasinskyi M. F., Kniaz S. V., Duriagina Z. A., Kulyk V. V. (2022). Determination of conditions for loss of bearing capacity of underground ammonia pipelines based on the monitoring data and flexible search algorithms. *Archives of Materials Science and Engineering*, 115(1), 13–20. doi: https://doi.org/10.5604/01.3001.0016.0671.

14. Mysiuk R., Yuzevych V., Koman B., Yasinskyi M. (2022). High Availability System for Monitoring Material Degradation Processes at the Concrete-polymer Interface. *2022 12th International Conference on Advanced Computer Information Technologies (ACIT)*. doi: https://doi.org/10.1109/acit54803.2022.9913086.

15. Yuzevych L., Skrynkovskyy R., Koman B. (2017). Development of

information support of quality management of underground pipelines. *EUREKA: Physics and Engineering*, 4, 49–60. doi: https://doi.org/10.21303/2461-4262.2017.00392.

16. Lozovan V., Skrynkovskyy R., Yuzevych V., Yasinskyi M., Pawlowski G. (2019). Forming the toolset for development of a system to control quality of operation of underground pipelines by oil and gas enterprises with the use of neural networks. *Eastern-European Journal of Enterprise Technologies*, 2(5(98)), 41–48. doi: https://doi.org/10.15587/1729-4061.2019.161484.

17. Yuzevych V., Skrynkovskyy R., Koman B. (2018). Intelligent Analysis of Data Systems for Defects in Underground Gas Pipeline. *2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP)*. doi: https://doi.org/10.1109/dsmp.2018.8478560.

18. Dzhala R. et al. (2022). Simulation of Corrosion Fracture of Nano-Concrete at the Interface with Reinforcement Taking into Account Temperature Change. *4th International Workshop on Modern Machine Learning Technologies and Data Science, MoMLeT&DS 2022*, CEUR Workshop Proceedings 3312, Leiden–Lviv, The Netherlands–Ukraine, 123–133.

19. Skrynkovskyy R., Kataiev A., Zaiats O., Andrushchenko H., Popova N. (2021). Competitiveness of The Company on The Market: Analytical Method of Assessment and The Phenomenon of The Impact of Corruption in Ukraine. *Journal of Optimization in Industrial Engineering*, 14(Special Issue), 79–86. doi: https://doi.org/10.22094/joie.2020.677836.

20. Sumets A., Kniaz S., Heorhiadi N., Skrynkovskyy R., Matsuk V. (2022). Methodological toolkit for assessing the level of stability of agricultural enterprises. *Agricultural and Resource Economics: International Scientific E-Journal*, 8(1), 235–255. doi: https://doi.org/10.51599/are.2022.08.01.12.

21. Skrynkovskyi R. M. (2011). Methodical approaches to economic estimation of investment attractiveness of machine-building enterprises for

portfolio investors. *Actual Problems of Economics*, 118(4), 177–186.

22. Skrynkovskyi R. (2008). Investment attractiveness evaluation technique for machine-building enterprises. *Actual Problems of Economics*, 7(85), 228–240.

23. Serniak I., Serniak O., Mykhailyshyn L., Skrynkovskyy R., Kasian S. (2021). Evaluation of the level of the usage of social instruments for human resource management: example of agro-processing enterprises of Ukraine. *Agricultural and Resource Economics: International Scientific E-Journal*, 7(4), 82–99. doi: https://doi.org/10.51599/are.2021.07.04.05.

24. Popova N., Kataiev A., Nevertii A., Kryvoruchko O., Skrynkovskyy R. (2021). Marketing Aspects of Innovative Development of Business Organizations in the Sphere of Production, Trade, Transport, and Logistics in VUCA Conditions. *Studies of Applied Economics*, 38(4). doi: https://doi.org/10.25115/eea.v38i4.3962.

25. Popova N., Kataiev A., Skrynkovskyy R., Nevertii A. (2019). Development of trust marketing in the digital society. *Economic Annals-XXI*, 176(3–4), 13–25. doi: https://doi.org/10.21003/ea.v176-02.

26. Mysiuk R., Yuzevych V., Koman B., Tyrkalo Y., Farat O., Mysiuk I., Harasym L. (2023). Detection of Structure Changes in Lightweight Concrete with Nanoparticles Using Computer Vision Methods in the Construction Industry. *Proceedings of Eighth International Congress on Information and Communication Technology (ICICT 2023), Lecture Notes in Networks and Systems*, 694, Springer, Singapore, 339–348. doi: https://doi.org/10.1007/978-981-99-3091-3_27.

27. Mysiuk I., Mysiuk R., Shuvar R., Yuzevych V., Hudyma V., Vizniak Y. (2023). Category Classification of Content from Instagram Business Pages. *2023 13th International Conference on Advanced Computer Information Technologies (ACIT)*, Wrocław, Poland, 570–573. doi: https://doi.org/10.1109/acit58437.2023.10275458.

28. The Global Risks Report 2023, 18th Edition, World Economic Forum. Retrieved from https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf (date accessed: 02.06.2024).

29. Jain A. K., Sahoo S. R., Kaubiyal J. (2021). Online social networks security and privacy: comprehensive review and analysis. *Complex & Intelligent Systems*, 7(5), 2157–2177. doi: https://doi.org/10.1007/s40747-021-00409-7.

30. Sumets A., Serbov M., Skrynkovskyy R., Faldyna V., Satusheva K. (2020). Analysis of influencing factors on the development of agricultural enterprises based on e-commerce technologies. *Agricultural and Resource Economics: International Scientific E-Journal*, 6(4), 211–231. doi: https://doi.org/10.51599/are.2020.06.04.11.

31. Bendovschi A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance*, 28, 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1.

32. Kniaz S., Heorhiadi N., Sopilnyk L., Konovalyuk I., Tyrkalo Y., Skrynkovskyy R., Moroz S., Kalashnyk O., Khmyz M., Kaydrovych K. (2021). Analysis Algorithm And Factors Of International Economic Activity In The Coordinate System Of Enterprises' Organizational Development. *Proceedings of the 38th International Business Information Management Association (IBIMA)*. 3–4 November 2021, Seville, Spain, 923–931.