colloquium-journal

ISSN 2520-6990

Międzynarodowe czasopismo naukowe

Art
Jurisprudence
Historical sciences
Economic sciences
Philological sciences
Pedagogical sciences
Physical education and sports

№10(97) 2021
Część 2

colloquium-journal

ISSN 2520-6990

ISSN 2520-2480

Colloquium-journal №10 (97), 2021

Część 2

(Warszawa, Polska)

«Colloquium-journal»
Wydawca «Interdruk» Poland, Warszawa
Annopol 4, 03-236
E-mail: info@colloquium-journal.org
http://www.colloquium-journal.org/

CONTENTS

ART

HISTORICAL SCIENCES

PHYSICAL EDUCATION AND SPORTS

PHILOLOGICAL SCIENCES

ECONOMIC SCIENCES

JURISPRUDENCE

PEDAGOGICAL SCIENCES

UDC 681.518

Kysh LM.
Candidate of Economic Sciences, A
ssociate Professor of the Department of computer sciences and economic cybernetics
Vinnytsia National Agrarian University
DOI: 10.24412/2520-6990-2021-1097-23-29

ANALYSIS OF E-COMMERCE RISK TYPOLOGIES

Abstract.
The economic impact of data breaches is a serious problem for retailers. It may be difficult for SMEs to predict the impact of data breaches on brand perception and calculate the impact on stock prices, but they should not underestimate the dull financial cost of a cyber-attack as one of the risks of e-commerce. E-commerce today is one of the fastest growing sectors in the world, adding 6 million new members each month with the support of a growing Internet user base. The e-commerce industry in its current form is a complex ecosystem. It includes large volumes of transactions, reliance on newer technologies such as mobile payment wallets and mobile applications for customer access, and reliance on third-party vendors for product purchasing and logistics. The purpose of the article is to explore and analyze the main typologies of risks associated with e-commerce. When the problem is simply the ordering of unconditional phenomena, it is difficult to distinguish typologies from classifications. The latter were considered preliminary to the discovery of sequences or laws. Because typologies invariably use ordering for additional purposes, classifications can be considered as typologies that are limited to the problem of order. Typologies that typically exist at the frontiers of research are less durable than classifications because their descriptions are accepted only insofar as they continue to provide solutions to problems. The application of the typology method has a number of clear advantages for research and measurement, and is in fact a central feature of these efforts. Typology is the main descriptive tool.

Keywords: *e-commerce, risk, risk-oriented approach, legislation, influencing factors.*

Introduction. When cyberattacks occur, retailers have to answer to their consumers and employees, but they are also increasingly held accountable by regulators. Most retailers (78 percent) cite concerns about data privacy and security policies, according to a 2017 survey by CFOs of BDO, which found that 70 percent of CFOs anticipate tightening cybersecurity regulations by 2017.

SMEs can protect data and minimize regulatory oversight by organizing employee training programs and creating coordinated incident response plans.

The economic impact of data breaches is a serious problem for retailers. It may be difficult for SMEs to predict the impact of data breaches on brand perception and calculate the impact on stock prices, but they should not underestimate the dull financial cost of a cyberattack as one of the risks of e-commerce.

Nowadays e-commerce is one of the fastest growing sectors in the world, it is adding 6 million new members every month with the support of a growing Internet user base.

The e-commerce industry is a complex ecosystem. It includes large volumes of transactions, reliance on newer technologies such as mobile payment wallets and mobile applications for customer access, and reliance on third-party vendors for product purchasing and logistics. Over time, the risks of fraud, including phishing, theft of personal data related to payment systems, and the risks of third-party fraud in procurement and logistics, such as counterfeiting, bribery, corruption, etc., began to affect e-commerce businesses.

E-commerce companies may be forced to ignore their internal processes and controls increasing the risk of fraud in a highly competitive environment to gain market share through aggressive pricing strategies such as deep discounts, meeting investor profitability expectations and the race to seek funds for expansion [5].

Therefore, it is advisable to study and analyses the main classifications (typologies) of e-commerce risks.

Recent researches and publications. The researches of Batrymenko V.V., Madiar R.O., Hlinenko L., Dainovskyi Yu., Marusei T., Oriekhova T., Pysarenko N. are devoted to the study of e-commerce risk typology [14, 15].

The **purpose of the article** is to research and analyse the main typologies of risks associated with e-commerce.

Presenting main material. Firstly, let’s consider the theoretical essence of the typology concept. According to the Merriam-Webster Dictionary, typology is the doctrine of analysis or classification based on types or categories [9].

The interpretation is given in table 1.

Table 1

Interpretation of the typology category

Source	Definition
Cambridge Dictionary	the study of types, or a system of dividing things into types [4]
Merriam-Webster	study of or analysis or classification based on types or categories [9]
Your Dictionary [13]	the study and classification of types of people, religions and symbols
	study or systematic classification of types that have characteristics or traits in common
	study of types, symbols, or symbolism
	(archaeology) the result of the classification of things according to their characteristics
Britannica	system of groupings (such as "landed gentry" or "rain forests"), usually called types, the members of which are identified by postulating specified attributes that are mutually exclusive and collectively exhaustive—groupings set up to aid demonstration or inquiry by establishing a limited relationship among phenomena [1]

Source: summarized by the author.

We need a brief explanation of e-business meaning in order to explain what e-commerce is. E-business, also known as online business, means an online business or the use of Internet technology to increase the productivity or profitability of a business. The term e-business can be also used to describe any form of business using a computer.

The term e-business consists of e-commerce and e-procurement. The e-procurement system covers mainly supply chain management, and e-commerce deals with the consumer needs of goods.

E-procurement is an important part of B2B business models. E-procurement means the purchase and sale of materials and services over the Internet. Alibaba.com is a good example of an e-procurement website, where users can search for buyers and / or sellers of goods and services. Depending on the approach of the buyer or seller, they can indicate or offer a price.

E-commerce is the purchase and sale of products, services and information through electronic systems such as the Internet. However, we will mainly cover the World Wide Web. E-commerce can be divided into four main categories i.e., B2B, B2C, B2C and C2C.

B2B stands for business to business, when companies trade with each other. Examples of B 2B are manufacturers to distributors and wholesalers to retailers. Pricing is mainly based on the number of orders.

B2C stands for a business to the consumer when companies sell directly to the consumer. This can be through a directory using trading software such as a web store.

C2B stands for Consumer to Business, which is used internationally. In the C2B business model, the consumer or end user offers a product or service to an organization that can use it to complete the business process. Photographers and designers are known to use websites such as Fotolia.com and Istockphoto.com to offer their images and services to other companies.

C2C means when consumers offer goods and services to other consumers. A good example of this is eBay, where users can bid for their item at auction.

Typologies can be used to study variables and transients. Classifications, on the other hand, refer to natural classes, that is, groups that differ from other groups in as much detail as can be detected. For this reason, classifications can only be a preliminary step in the study of variables, as they cannot elegantly deal with the transitional situations in which variables are to be expected. The slower the change, the fewer the distinctive features by which natural classes can be determined, and the more difficult it becomes to draw the line between classes. Typologies can be used in this situation.

It is difficult to distinguish typologies from classifications. The latter were considered preliminary to the discovery of sequences or laws. Because typologies invariably use ordering for additional purposes, classifications can be considered as typologies that are limited to the problem of order. Typologies that tend to exist at the frontiers of research are less durable than classifications because their descriptions are accepted only insofar as they continue to provide solutions to problems.

The typology method has a number of clear advantages for research.

Typology is the main descriptive tool. It is the cornerstone of any discipline, as it provides a basic set of descriptive, multidimensional types or taxa. No other research method provides a comprehensive typology. Typology is the final reference source for the discipline. No other concept or presentation can match the complexity and conceptual range of types. One-dimensional descriptions are simply not an alternative to multi-vector types.

Strict explication of the multidimensional type demonstrates the degree of clarity and lack of ambiguity, which is extremely necessary in research. Typology is the main tool for rigorous multidimensional comparison and analysis of both conceptual and empirical types. The comparative procedure is very stingy, as it allows you to identify only the types for which there are empirical cases. Other potential types may remain hidden and unused as long as they are not needed, but are still available when needed.

Typologies are useful for illustrating the differences between two or more empirical cases. Typologies are the main tool for identifying empirical examples of specific type concepts. The complete typology allows to illustrate possible types, even if they cannot be found empirically.

Let's consider the main typologies of e-commerce risks.

Table 2

Typologies of e-commerce risks proposed by researchers

Author	Classification
Anup K Ghosh Tara M Swaminatha [2]	By security system creation object: - software risk; - confidentiality risk.
Steve G. Sutton Deepak Khazanchi Clark Hampton Vicky Arnold [10]	By the conceptual approach to modelling: - technical risks; - users' risks; - business risks.
Duh, Rong-Ruey and Jamal, Karim and Sunder, Shyam [6]	By place of origin: - internal risks; - external risks.
Lawrence J. Trautman [11]	By influence object: - cyber risks; - information technologies risks; - payment systems risks

Source: summarized by the author.

The importance of e-commerce, especially e-commerce through the Internet, has been recognized by both academics and the business press.

The importance of e-commerce goes beyond so-called Internet firms. Internet firms are firms that have redesigned business processes to take full advantage of the advances in telecommunications, computer hardware, and computer software. It is reasonable to expect that enterprises of different activities will follow the first movements in this direction at different speeds. Most industries will include firms with different levels of e-business. It potentially creates intra-industry differences in the specific e-risk of the business.

Despite all the tangible benefits of establishing an integrated business relationship, there is still a certain uncertainty when entering into this relationship for many organizations. It may be the result of costs, but more often it is the result of the perception of risks in the enterprise. Some authors generalize these risks as the costs associated with the exposure they exploit in the relationship. These risks include transaction-specific capital (i.e., one-party investments that have little or no value outside the business relationship), information asymmetries (i.e., problems with monitoring activities that create the risk of evading a business partner) and loss of resources control (i.e., resources which are transferred in a relationship that cannot be returned or controlled in the event of termination of the relationship).

These risks primarily focus on the loss of investment, which can have negative financial consequences for the organization. However, in an era where the focus has been on improving core business processes, outsourcing what other organizations can do better, and developing integrated value chains, relationship breakdowns can have far greater consequences than just financial losses and / or inefficiency. For example, in a timely environment where the supplier is responsible for managing inventories of materials and parts, the supplier's failure to supply parts for an extended period of time may result in prolonged production downtime.

These disruptions can jeopardize the manufacturing company due to the inability to produce goods, the inability to meet obligations down the supply chain, the loss of trust of other business partners and the decline of the overall reputation. Such risks may jeopardize the sustainable development of the enterprise.

The three components of the B2B model provide a basis for assessing the risks associated with an organization's B2B e-commerce activities. Although the model provides a solid conceptual framework for studying the risks of B2B e-commerce, its definition is limited to broad categories of issues that may make it desirable to ensure the reliability of B2B transactions of trading partners. However, before such assurance services can be provided, an understanding of the specific key risk factors within this component is critical at this research stage. Derivation of critical risk factors is problematic because knowledge in complex systems is expertise embedded in basic operational levels, as opposed to general knowledge known to senior management. Knowledge often remains silent only because no one has tried to articulate knowledge, but articulating tacit knowledge through investigation can allow management to understand key organizational risk factors. This transformation of tacit expertise into explicit knowledge is a mandatory first step in developing effective measurements and/or monitoring in complex systems. This philosophy is based on the belief that the best way to understand and develop tools for effective process monitoring is to involve individuals who regularly perform the process at key operational levels.

Forbes offers a classification of e-commerce risks, which should be considered in more detail.

1. Internet security risks.

Security risks can be a significant part of your financial risk when doing business online.

Data breaches can lead to the loss of millions of dollars. However, the damage to reputation can be immeasurable. As technology advances, hackers are becoming more sophisticated. Main measures are implementation of a reliable security policy, personnel training, saving the necessary data, and saving backups.

2. The risk of low website traffic.

3. The risk of interrupting website traffic [7].

Another approach to the typology of e-business risks is used by professional accountants.

For example, the Australian Accounting Standards Board (AuASB) is the world's first standard-setting body to develop authoritative guidelines for addressing new audit issues in the new e-commerce business environment. Audit Guideline Statement 1056, E-Commerce: An Assessment of Audit Risks and Control Considerations, was published in August 2000. Auditors perform their duties in a dynamic business environment. Therefore, to develop an appropriate strategy, they must be aware of the impact of changes in the planning of audit procedures [1].

E-commerce is fundamentally changing our business. The constant development of technology and the e-commerce growth have a significant impact on the traditional business environment. E-commerce is changing the competitive market and making international trade viable for many more businesses.

However, the auditor's responsibility for providing an opinion on the financial statements remains unchanged. Online and computer-based communications and transactions are not new features of the business environment, the increasing use of the Internet for e-commerce is introducing new risk and control variables that require audit. E-commerce is not limited; it has open boundaries in scope terms. The auditor needs the appropriate skills to understand how the entity e-commerce strategy responds to the commercial risks that arise. Assessing audit risk for e-commerce requires a paradigm shift in how auditors view client organizations and in how auditors plan audit procedures to reduce audit risk to an acceptable level.

When a business is engaged in e-commerce, it creates many new risks. The Internet gives every business the opportunity to trade on the world market. When transactions are initiated by unknown parties on the Internet, there are risks associated with the reliability and integrity of trading partners and e-commerce transactions. Management usually identifies commercial risks of e-commerce and addresses these risks through appropriate security and control measures. The auditor will consider e-commerce business risks to the extent that they affect audit risk. Audit risk refers to the risk that the entity's financial statements (for which the auditor provides an audit report) are materially misstated [1].

Businesses may face a number of limitations developing of e-commerce, they include the availability of appropriate technical and marketing expertise, the need for further investment, and the identification and resolution of security issues. Although these issues may remain unresolved, many organizations continue to develop e-commerce based on the risk-reward principle. As a result, the e-commerce market is growing rapidly, in particular business-based e-commerce (B2B) reduce supply lines and reduce costs. Such growth affects both business risk and audit risk.

AGS 1056 identifies specific issues that the auditor believes determine the importance of e-commerce, monitor the impact of e-commerce on the auditor's risk assessment, and develop audit strategies to respond to the various risks arising from e-commerce. E-commerce business risks include those arising from:

- personality and nature of relations with e-commerce trading partners;
- integrity of operations;
- electronic processing of transactions;
- reliability of systems;
- issues of confidentiality;
- return of goods and product guarantees;
- issues of taxation and regulation [1].

AGS 1056 includes a discussion of how an e-commerce strategy and business model identifies and addresses these business risks. This understanding allows the auditor to determine how the entity has applied its control system to its e-commerce activities. It also helps to assess whether the entity's development processes are defined, clear and transparent. Security issues arising from online transactions are considered, especially emphasizing that the security infrastructure of the entity is fundamental to the effectiveness of other security measures [1].

Another area of e-commerce that concerns the auditor is the availability of financial information (both auditable and non-auditable) on the entity's website. Guidance on this aspect of e-commerce is provided in AGS 1050, issued in Australia in December 1999.

The AuASB recognizes that the e-commerce audit guidelines are only one part of a much larger project requiring ongoing research.

E-commerce involves doing business over the Internet being a major trend in today's world. Companies in various industries have switched to e-commerce in order to optimize market opportunities, increase efficiency and minimize operating costs. However, a huge amount of information is involved in these operations, which means that information security must be considered to eliminate the negative consequences associated with online business. The information assets are exposed to various types of threats that can affect the activities of the organization both directly and indirectly. Business organizations have invested in intensive research to develop various models for identifying and managing potential threats to successful online transactions. The government has taken significant steps through regulations to mitigate various forms of threats to e-commerce. Vulnerability of information assets can lead to various adverse effects that adversely affect the integrity, reliability, accountability, reliability and confidentiality of information. The adoption of sophisticated information management systems in e-commerce firms aims to improve the security of their databases in order to minimize malicious attacks that significantly threaten their critical infrastructure. As investment in e-commerce increases, there is a growing need for effective risk management techniques to protect aspects such as artificial intelligence, financial information and trade secrets facing serious threats from cyber activities.

The e-commerce risks typology is another typology proposed by O. Vitez [12].

E-business is an electronic form of business conducted over the Internet. This business model has grown in popularity as technology has improved with smaller and better forms of computer hardware. Nowadays many modern businesses operate online exclusively and may never open a traditional brick-and-mortar display case. Although e-business can be easy to start and requires little money.

Systematic risk is the risk that a company faces from the entire market or market segment in which it operates. A classic example of systemic risk in the e-business market is the collapse of dotcom in 2000 and 2001. Several e-businesses started and went public, and then acquired other e-companies. Most e-businesses had little cash flow and were unable to make a profit; these companies measured growth relative to financial stability, creating an unstable economic bubble that burst, destroying many dotcom companies. Although this type of systematic risk may not recur, most market segments may tend to operate in business cycles, growing, reaching plateaus and shrinking. E-business owners and entrepreneurs should be able to assess their market segment and plan each stage of the business cycle.

E-businesses face many different types of risks associated with protecting their business and customer information. Computer viruses and hackers are constantly trying to hack Internet companies and steal customers' personal data and financial information. These security risks force e-businesses to use software and encryption codes that limit the ability of third parties to hack their secure systems. Online security risks can also lead to legal problems for e-businesses, as they are required to protect consumer information under federal and state law. Violations in the e-business system will also increase the company's insurance risk, as insurers demand higher premiums for companies with legal problems if they decide to take e-business as a customer.

Business risk is related to the risk faced by companies in conducting day-to-day operations. These risks include problems with inventories, labour, overhead, or supply chains. Since most e-businesses do not have large physical locations or warehouses, they must rely on a supply chain to deliver goods to consumers. Whenever a business has to rely on individuals or other businesses to help distribute goods, the risk can increase. Business risk also arises if an e-business cannot quickly and efficiently acquire inventory and move it along the supply chain.

E-commerce is expanding rapidly around the world. This fast-growing business also carries several types of risks. According to the researcher M. Gola, these risks include the following typology proposed by scholar [8].

1. Online threat.

Every type of business gets threatened. The full range of security threats we can see in e-commerce business include phishing attacks, malware, and e-mail about hacking and spam. These threats can be quite risky for all of us. You must regularly update your platform's operating system to address these threats.

2. Privacy issues.

Company and customer personal data and information are very important to protect them. There are many hackers and spammers who can misuse personal data for spam, identity theft and unwanted marketing. Therefore, you need to use a strong password.

3. Disputes with customers.

When a customer does not receive his order on time or encounters some damaged products, there is a chance that he may argue with you. So, you always need to make sure that you provide your customers with first-class customer service. You can't afford to settle your client's disputes.

4. Exit from SEO.

Google and other platforms can update their algorithms and view your site at any time, ensuring that your website traffic is significantly reduced overnight. Therefore, your site may run the risk of insufficient traffic and reduced sales conversions.

5. Intellectual property issues.

They include images, products, videos, designs, logos, etc. that you originally designed, but other people can copy your design and present it as their own. This infringes your intellectual property rights. When your ideas and thoughts are copied, you think of giving them back to others.

6. Credit card fraud.

It can be a big risk for an e-commerce seller. People may use a stolen credit card to make an online purchase, or a hacker may be able to use stolen credit card information from other customers on your system. No matter how tough your online securities are, you should always be aware of suspicious transactions.

There are also perfectly legal actions and changes in the commercial environment that can threaten companies. Consumer behaviour, supplier efficiency and the exchange rate affect profits today and tomorrow.

Top companies have shown great interest in supporting and developing business-to-business (B2B) exchanges (electronic markets). The accumulation of power by higher-level enterprises in a particular industry is one of the consequences. Their goal is to reduce the cost. It will reduce the margin further down the supply chain. Procurement may have been unsuccessful in the past in terms of the best purchase price. However, Internet technology can smooth out customers' ignorance. Companies always want suppliers if we do not see vertical integration on an unprecedented scale. The real implications are that customer-supplier relationship management and non-price factors will become even more important.

Companies depend on their suppliers. Three areas of particular concern are IT operations, transport / logistics and disintermediation for e-business. For example, if a company's website is hosted by an Internet Service Provider (ISP), the promotion and sale of products depends on the ISP's ability. It is also important that the goods reach their destination on time, so the results of logistics suppliers should be closely monitored. Contingency plans should be developed so that switching to alternative vendors can be made immediately if outbound IT or logistics vendors fail. Web companies tend to place the greatest emphasis on the web interface. The pleasure comes to the customer with the enthusiasm of the product. Finally, there is also the risk of disinmediation, through which the supplier implements a strategy that cuts out the middleman and sells directly to your customers.

Business risk depends more on the sophistication and experience of the company than on its transition to e-commerce through exchange rate movements. However, the small businesses opportunity to sell to the world market is a part of the Internet commercial attraction. These companies can start trading internationally without managing the propensity for adverse exchange rate changes. The simple answer is to charge a fee in the company's national currency. Thus, the risk is transferred to the client; although such an approach can cause sales loss.

The next external source of risk to be considered are laws and regulations designed to manage business activities.

The amount of relevant legislation that companies need to know is growing. In the UK, this includes laws governing investigators' powers over electronic communications, data protection and even human rights. For example, if a company intends to read e-mails from its employees, it must explain this to them in advance and set a contract term for their work.

It is important to remember that all the usual rules still apply in addition to the new legislation introduced in response to new e-business technologies. However, e-business does not receive another distribution. The laws on copyright rules, patents, acceptance and offer, trademarks and data protection are applied. For example, a British software company has entered a brand name owned and used by a competitor into its computer code on its website. The trademark has been included as a meta tag, a keyword used by search engines to help people find a website, although the meta tag cannot be seen on a regular web page that appears on the user's screen. The court ruled that this was a copyright infringement.

The laws of other countries, where businesses can now operate through e-business channels, should also be taken into account.

The efficiency and effectiveness of a company business processes can lead to a further set of risks. Perhaps these are the risks that the company imposes on itself, perhaps due to the employment of the most prominent aspects of day-to-day management. Two examples will be considered, i.e., intellectual property and reliability of delivery.

The value of business knowledge and information and the need to protect them are growing. For example, data integrity must be ensured for any e-business. In addition, intellectual property must be protected as fully as possible. Part of the solution is to protect intellectual property rights (IP) through legal contracts, but preventive measures should also be taken to ensure that everyone in the organization evaluates the value of IP and acts to support it in their day-to-day work. Protecting computer data and intellectual property requires rigorous processes, including notifying all personnel.

If business does not meet its customers' delivery expectations it loses its customer base. It may be the inability to deliver goods on time or an immediate response to customer inquiries by e-mail.

The biggest risk lies in choosing a business strategy. There must be a viable path to profitability. The emergence of a network economy does not destroy the fact that during the relevant period the company must be able to generate a positive balance of discounted cash flows.

Business strategies must be viable, acceptable and sustainable. Let's look at each of these three concepts and illustrate them with examples based on real e-business experiences.

The strategy must be viable; it needs to make sense and offer the product or service that the market wants now or will want in the future. A grocery auction is unlikely to be viable because people will not be willing to invest more time than price increases are worth.

Acceptability is the reaction of other stakeholders. An operation aimed at demarcating car dealerships will not work if there are powerful suppliers (car manufacturers) who prefer to sell through their dealer networks. Therefore, e-business must consider the acceptability of its business strategy for top organizations in the supply chain.

Finally, it must be possible to protect the product or service from imitation or legal action for a sufficient period of time. A peer-to-peer system for sharing music files can be an exciting use of technology and a concept that attracts millions of users, but if it cannot be defended as a fair practice in the courts, it is not sustainable as a business strategy.

Conclusion. The e-commerce business has been given considerable attention and access to a larger audience. It is usually not achieved by conventional retail methods. However, it has also made business owners and customers vulnerable to serious security threats.

The e-commerce model carries a huge risk for both retailers and consumers. Consumers trust their financial and personal data when they make purchases both in-store and online instructing retailers to ensure the dissemination of data on many digital platforms. Companies are concerned about the potential release of confidential information about customers, employees and corporations that could be used for personal data fraud, financial theft or damage to the brand reputation.

References

1. AccountancyDaily (2001). E-commerce: what's the risk? URL: https://www.accountancydaily.co/e-commerce-whats-risk
2. Anup K Ghosh, Tara M Swaminatha (2001). Software security and privacy risks in mobile e-commerce. Communications of the ACM, Vol. 44, No 2. URL: https://dl.acm.org/doi/fullHtml/10.1145/359205.359227
3. Britannica (2020). Typology. URL: https://www.britannica.com/science/typology
4. Cambridge Dictionary (2020). Typology. URL: https://dictionary.cambridge.org/dictionary/english/typology
5. Deloitte (2020). Beyond the growth story Mitigating fraud risks in the e-commerce industry. URL: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance/in-fa-e-commerce-brochure-noexp.pdf
6. Duh, Rong-Ruey and Jamal, Karim and Sunder, Shyam, Control and Assurance in E-Commerce: Privacy, Integrity and Security at Ebay (April 1, 2001).

Taiwan Accounting Review Vol. 3 Issue. 1 pp. 1-27 2002, University of Alberta School of Business Research Paper No. 2013-677, Yale SOM Working Paper No. AC-01, Available at SSRN: https://ssrn.com/abstract=254270 or http://dx.doi.org/10.2139/ssrn.254270

7. Edwards H. (2020). Three Key Risks To E-Commerce Businesses (And What You Can Do About Them). Forbes. URL: https://www.forbes.com/sites/forbesbusinesscouncil/2020/08/12/three-key-risks-to-e-commerce-businesses-and-what-you-can-do-about-them/?sh=5b95fe1e2e17

8. Gola M. (2020). What are the risks when launching E-Commerce businesses? URL: https://www.curvearro.com/blog/what-are-the-risks-when-launching-e-commerce-businesses/

9. Merriam-Webster Dictionary (2020). Typology. URL: https://www.merriam-webster.com/dictionary/typology

10. Steve G. Sutton, Deepak Khazanchi, Clark Hampton, Vicky Arnold (2008). Risk Analysis in Extended Enterprise Environments: Identification of Critical Risk Factors in B2B E-Commerce Relationships. Journal of the Association for Information Systems, Vol. 9, Nos. 3-4, pp. 151-174

11. Trautman, Lawrence J., E-Commerce, Cyber, and Electronic Payment System Risks: Lessons from PayPal (September 3, 2016). 16 U.C. Davis Business Law Journal 261 (Spring 2016), Available at SSRN: https://ssrn.com/abstract=2314119 or http://dx.doi.org/10.2139/ssrn.2314119

12. Vitez O. (2017). E-Business Risks. URL: https://bizfluent.com/how-6534709-start-dot-com-company.html

13. YourDictionary (2020). Typology. URL: https://www.yourdictionary.com/typology

14. Batrymenko V.V. (2020). Modern mechanisms for minimizing the risks of e-commerce. International relations, No 23. URL: http://journals.iir.kiev.ua/index.php/ec_n/article/view/4045/3688

15. Madiar R.O. (2020). Risks of foreign economic activity and key partners of Ukraine. Economy and state, No. 2. URL: http://www.economy.in.ua/?op=1&z=4741&i=10

УДК: 330.332

Очак Павел Константинович,
студент Кубанского государственного аграрного университета имени И. Т. Трубилина, г. Краснодар
Мамий Сима Асламбечевна
преподаватель Кубанского государственного аграрного университета имени И. Т. Трубилина, г. Краснодар

КОНКУРЕНЦИЯ И МОНОПОЛИЯ

Ochak Pavel,
student of the Kuban State Agrarian University named after I.T. Trubilin, Krasnodar
Mamiy Sima
Teacher at the Kuban State Agrarian University named after I.T. Trubilin, Krasnodar

COMPETITION AND MONOPOLY

Аннотация.
В данной статье исследуются понятия и основные виды конкуренции, рассматривается современное положение конкуренции, определяются характерные черты монополии в настоящее время.

Abstract.
This article examines the concepts and main types of competition, examines the current state of competition, defines the characteristic features of monopoly at the present time.

Ключевые слова: *конкуренция; монополия; дифференциация; олигополия; рынок*
Keywords: *competition; monopoly; differentiation; oligopoly; market*

Конкуренция — борьба субъектов рынка за невозобновляемые ресурсы и за наиболее выигрышные условия для производства и реализации товара.

Конкуренция существует в командной и рыночной экономике. При командной экономике организации конкурируют за расположение руководства. При рыночной экономике — ограниченные ресурсы перераспределяются на базе свободного рынка.

Colloquium-journal №10(97), 2021

Część 2

(Warszawa, Polska)

ISSN 2520-6990

ISSN 2520-2480

Czasopismo jest zarejestrowany i wydany w Polsce. Czasopismo publikuje artykuły ze wszystkich dziedzin naukowych. Magazyn jest wydawany w języku angielskim, polskim i rosyjskim.
Częstotliwość: co tydzień

Wszystkie artykuły są recenzowane.
Bezpłatny dostęp do elektronicznej wersji magazynu.

Czasopismo jest publikowane i indeksowane na portalu eLIBRARY.RU,
Umowa z RSCI nr 118-03 / 2017 z dnia 14.03.2017.

Redaktor naczelny - **Paweł Nowak, Ewa Kowalczyk**

«Colloquium-journal»
Wydawca «Interdruk» Poland, Warszawa
Annopol 4, 03-236
Format 60 × 90/8. Nakład 500 egzemplarzy.

E-mail: info@colloquium-journal.org

http://www.colloquium-journal.org/