FEATURES OF E-BUSINESS AND E-COMMERCE WITH A REFLECTION ON PRIVACY IN THE DIGITAL AGE

*Irina Noninska, Radi Romansky**

(*) Technical College of Sofia at the Technical University of Sofia
Bulgaria

* Corresponding Author, e-mail: rrom@tu-sofia.bg

Abstract: E-business and its basic component e-commerce are components of the modern digital society. The application of contemporary information and communication technologies allows their establishment in social and economic life. The article presents an overview of the main features, models and approaches in building e-business and e-commerce systems. In addition, specific problems in the processing of personal data in the network environment are structured and basic requirements that must be respected in their e-business and e-commerce communications are summarized.

Key words: digital age, contemporary technologies, electronic business, electronic commerce, privacy, personal data protection.

1. INTRODUCTION

Electronic business (e-business) in the modern digital space uses information technology, which enables process efficiency, both in large, medium, and small enterprises [1]. The cited article, however, states that an adequate assessment of the overall costs of maintaining online business processes should be made. To determine the level of usefulness, an analysis was made based on a defined "technology-organization-environment" strategy and the limits of applicability to micro-businesses were determined. Another point of view is presented in [2], where digital business is considered as a subset of e-business and the influence of digital technologies on the rapid development of world business is confirmed. However, it also states that „*the utilization of e-business in a business unit might result in profits or losses for that particular business unit*".

What can be the main risks for e-business in the modern digital space? The main answer can relate to the entry of digital technologies themselves (Cloud Computing, Internet of Things - IoT, Big Data Analytics, etc.) and the challenges they create for the processes and for the personal privacy of the participants in them. An example of this is the IoT business model presented in [3], where information, capital and logistics flows are recognized in the industry chain based on IoT platforms. Another direction is the opportunity discussed in [4] to study the risk in banking operations with the application

of Big Data Analytics techniques. An index system has been designed, allowing for effective evaluation of credit risk in e-business processes, indicating that the accuracy of the ranking is higher than that of the logistic regression model. Last but not least, the entry of artificial intelligence (AI) into e-business platforms should be noted, as in [5] it is stated „*although AI offers e-businesses multiple advantages, in order to differentiate themselves from their competitors, it is still a relatively new technology*". It is further emphasized that both AI and other modern technologies are subject to increased discussions regarding ethical and privacy concerns.

Electronic commerce (e-commerce) is a part of e-business, uniting processes in the global network for offering, selling, or transferring goods, services and information resources [6]. This allows the implementation of remote access to resources, but also the provision of certain personal data of users in the Internet space. This reflects on the privacy of users and creates certain challenges to their personal data, which generally coincides with similar problems in e-business and with the challenges of the digital space [7] and the requirements regarding processes in cyberspace [8].

The subject of discussion in this article are the features of the organization of processes for e-business and its component e-commerce, presenting the participants, the relationships between them and last but not least the challenges of the digital world to privacy and personal data protection.

2. TECHNOLOGICAL ASSPECTS OF E-BUSINESS

The term "e-business" determines the realization of main processes of business management and functionality based on digital platforms in the global network. The main goal is to improve the efficiency of internal and external communications in online processes, as well as to reduce physical contacts between participants. The models of e-business are determined based on the relationships between basic participants in the processes which could be defined as follows: Business organization, firm, or institution (B); Client (C); Administration (A); Government (G); Program Application (P) [5]. The functioning of a business environment with the participation of the represented participants can be considered as part of the electronic management system, which requires ensuring the necessary level of information security when accessing the resources [9]. A brief presentation of the main models in the field of e-business is made below.

Model "Business-to-Business" (B2B) is the main model that represents the relations between manufacturing companies and companies with other business institutions such as banks, insurers, trading companies, intermediaries, suppliers of goods and services, etc. This model reflects a huge a market with complex relationships, dynamic changes, and business planning, requiring serious means and strategies to protect resources and transactions. The latter determines a high importance of the implementation of a business scenario for the selection and application of information and communication technologies. Main activities included in a B2B-system are the following: ✓ Ensuring a connection between producers and users of production, as a rule they are legal entities and have sufficiently developed back-office systems; ✓ Information provision for the supplies and logistics of all contractors for the main

production. Listed below are the main functions that an Internet portal must perform in order to ensure adequate implementation of business processes in the B2B model.

1. *Content Management*. The information coming from the various sources must be checked for correctness and processed in order to extract the necessary metadata. It can be displayed for different users only after customizing each one and filtering the data according to the user's own privacy requirements.

2. *Description of business processes*. Collecting, processing, and summarizing the data necessary for a detailed description of all business processes in the B2B model is carried out. An analysis of the transactions that will implement the main functions and services for the business partners is being prepared.

3. *User settings*. A more in-depth study of user requirements is carried out and services tailored to the characteristics of individual groups of users are implemented (personalization of services).

4. *Functionality*. The parameters of the portal and the conditions for its use are described, the requirements for user devices, equipment and technologies are defined.

5. *Information security*. The information security system must provide a flexible approach for authorization and authentication of users, without making them unnecessarily difficult or slowing down their work. After successful identification, further checks are made in individual cases for access to confidential or personal data, which is in line with network and information security requirements.

6. *Expanding Access*. This function is related to creating suitable conditions for the use of all types of e-devices for connection to the B2B portal. To the requirements for high speed, reliability of operations and security, business users are increasingly adding requirements to minimize time, place and cost constraints on access to e-services.

Model "Business-to-Client" (B2C) is the equivalent of retail trade, where different independent individuals (clients, buyers) interact with the store (seller). The implementation of the model is directly related to the creation and maintenance of its own website (electronic showcase) for the presentation of information about the goods, located according to the seller's marketing strategy. The main task of this "showcase" is to provide accurate and complete information about each product and facilitate the buyer to make the right choice.

The remaining pattern of relationships is summarized in Table 1.

Table 1. Additional models of business relationships

Model	Comments
B2A	Business-to-Administration – reflects relationships that cover all types of transactions between corporations and government organizations (VAT payments, payment of corporate taxes).
C2A	Client-to-Administration – covers the payments of citizens to the administration (taxes, social and health insurance).
B2G	Business-to-Government – a type of business relationship for the sale of products from commercial structures to government institutions and is usually associated with the material and technical provision of state structures.
C2B	Client-to-Business – relationships related to the sale of goods and services from private individuals to corporations (consulting, transportation).
C2C	Client-to-Client – serves commercial transactions between private individuals.
P2P	Program App-to-Program App – transmission of data from one program product directly to another program product providing integration of applications located in the systems of commercial partners.

Building a successful e-business strategy depends on two types of factors – positional (technology, services, markets, and sales network) and binding (leadership, infrastructure, and organizational learning). Two basic approaches can be applied to the implementation of the chosen strategy – a centralized approach (a small group of well-prepared employees in a given company makes strategic decisions) or a decentralized approach (each business unit in the company makes its own strategic decisions, taking into account the company's strategy the company). The following stages can be defined for the specific implementation.

1. Construction – an initial stage requiring the creation of appropriate information infrastructure, services, and transactions, for which a plan for re-engineering business processes has to be developed.

2. Management – a stage at which companies have started the transition to individual elements of e-business, but intuitively, without a concrete plan and have spent funds, which necessitates the development of an effective management plan.

3. Implementation – in the presence of information infrastructure, it is necessary to develop projects to increase competitiveness.

4. Expansion – preservation of the achieved position and development of projects to increase the possibilities.

E-business should be seen as a collection of skilled people, technological elements and relevant business processes, which defines several aspects of the infrastructure.

1. Technical aspect – communication networks (Internet, intranet, extranet), server technologies, hardware and software products, various specialized applications.

2. Technological aspect – technological means for management (of personnel, of customer relations, of knowledge), for business e-learning, for maintaining control, for ensuring security and data protection, etc.

3. Human aspect – the main part is the human element, namely company management, staff, even customers.

When building an e-business system, the basic models presented below can be applied.

1. Markets driven by sellers – in this model, sellers are at a disadvantage because they have to compete with other producers in a transparent environment.

2. Neutral markets driven by commercial intermediaries – commercial intermediaries have clear opportunities to add value and their behaviour is driven by the needs of sellers and buyers. They need to find a way to integrate their business processes with those of customers.

3. Buyer-driven marketplaces – buyers can benefit from competition between sellers and their goal is to quickly organize marketplaces driven by them.

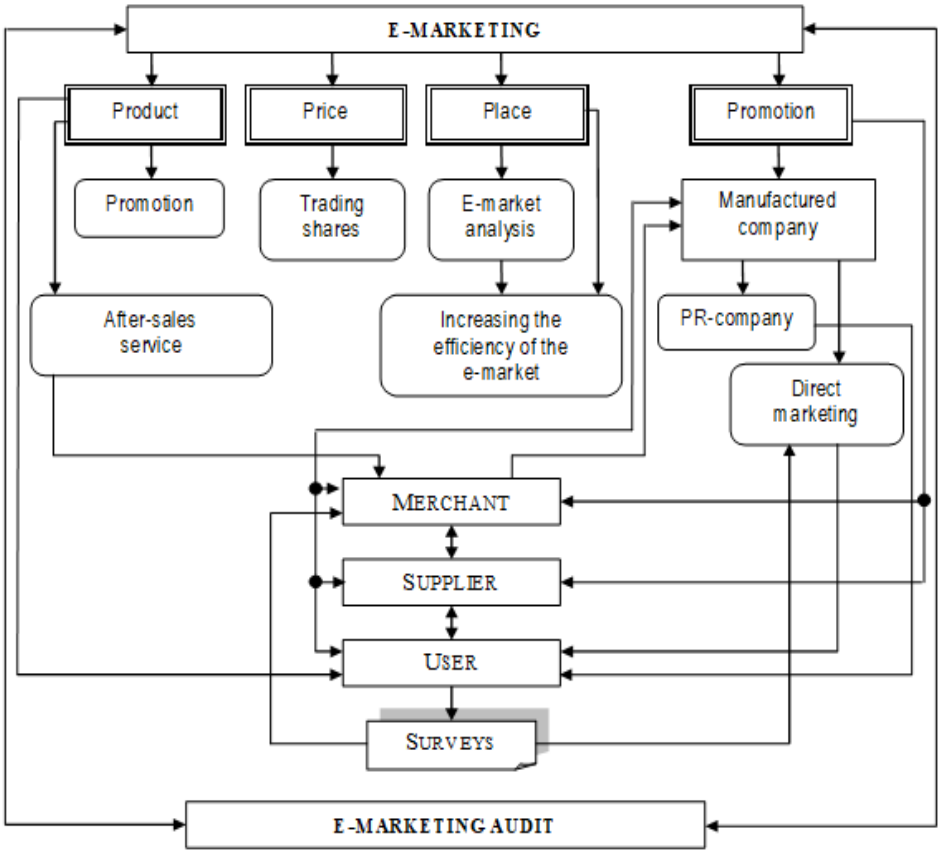
A major category in e-business is electronic marketing (e-marketing), which is the activity of researching a certain market to give an idea of how much a given product or service will be in demand. It includes 4 main elements known as "4p" – **p**roduct, **p**rice, **p**lace, **p**romotion. Functional structure of e-marketing is presented in Figure 1.

The tasks that are set for e-marketing are determined by the experience accumulated over the years in traditional marketing and are supplemented with activities specific to e-markets. Below are formulated three of the most important tasks with the means for their realization.

(1) Increasing the volume of the company's realized production or the number of services provided. This can be achieved mainly through advertising and direct marketing, as well as periodic publication of information about the goods and services offered.

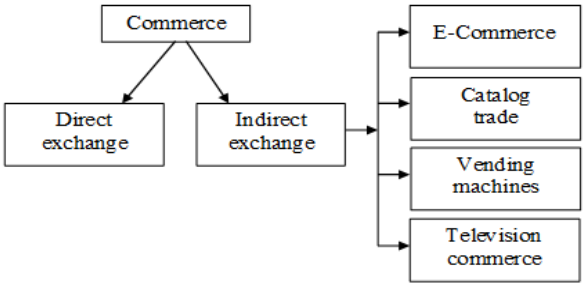
(2) Attracting new commercial intermediaries and brokers, for which it is necessary to conduct periodic surveys with various means of communication, as well as those with online access on the company's website.

(3) Increase the number of visits to the Web site to attract new users. The decisions depend on the requirements and preferences of the customers, which also determines the method and frequency of updating the site.

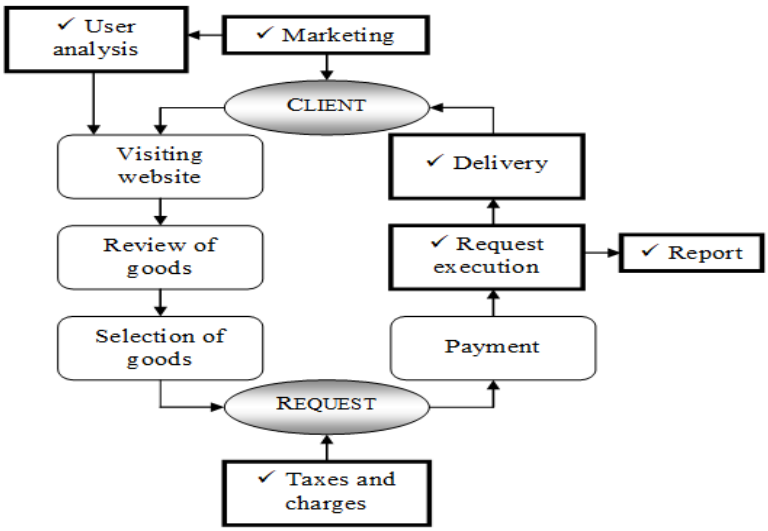


3. FUNCTIONAL ORGANIZATION OF E-COMMERCE

Trade relationships are related to the exchange of goods and money between the two entities (seller and buyer) and can be considered in two aspects – direct and indirect trade (Figure 2).



Direct trade is the traditional form based on the direct personal contact of the buyer with the seller. Indirect trade is characterized by the complete absence of personal contact, using an intermediary (magazines, mail, telephone network, Internet). This group includes e-commerce, in which the capabilities of the global network environment are used to implement marketing, commercial offers, sales, leasing, licensing, delivery of goods, services or information. This category is the most dynamic segment of the e-market, generating the predominant volume of financial transactions. The main stages in the implementation of e-commerce are presented in Figure 3. The activities marked with the sign „✓“ are performed without the direct participation of the client.



Some of the activities are not significantly different from those of traditional commerce except that they are performed in the network space. This requires compliance with the rules for preserving user privacy. When conducting marketing, an approach analogous to traditional trade is applied, with the clear goal being to attract a larger number of potential buyers than those who visited the relevant Web site. In addition, visits to the site allow for the analysis of potential users to provide good opportunities

for the realization of the following activities – a review of the offered goods and a successful selection of some of them. This implies filling out and submitting an application and subsequent activities in the chain.

When visiting the website, users can be offered inclusion in specially organized discussion forums, registration of interests, questions, and comments. Usually, the activities of selling goods or services are related to various checks – identification of the client, authentication of requests, review of the conditions for electronic transfer of funds, and many of the necessary functions are implemented based on the mechanism for electronic exchange of documents [10]. This involves building a "customer profile" that contains a lot of information, including personal data. The latter also applies to the "Payment", "Request execution" and "Delivery" stages, which also require certain personal information, including names, contact details, location, delivery address and method of receipt, etc.

Payment for the requested goods can be made in different ways, depending on the customer's preferences (debit and credit cards, payment orders, cash on delivery, etc.), but all of them require the provision of sensitive personal data, which requires taking serious security and protection measures.

The preparation of documents for the processing of requests, payment and delivery of goods implies the processing of personal data and again requires compliance with the regulation on the privacy of consumers. The main requirements in this direction, both for e-commerce and for e-business processes, are summarized in the next section.

4. REQUIREMENTS FOR USER PRIVACY AND DATA PROTECTION

4.1. Informatization and privacy

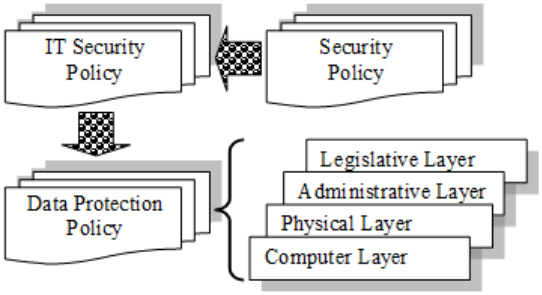
The development of e-business and e-commerce technologies is directly related to an increase in the level of informatization of society in the digital age. The results of this are obtaining new knowledge, higher quality, and speed in the provision of information services, efficiency, and improvement of processes in organizational and production systems based on the use of computer equipment and management of all processes through the use of information technologies. These aspects of modern society set requirements for the development of an adequate policy for using the functional capabilities of the network space, which is especially important for 5G networks. One possibility is to develop an adequate Application Program Interface (API) to allow mobile end applications to monitor subscriber spending limits regardless of the measurement method [11]. It should be considered that the geolocation of users in the network space affects the effectiveness of interaction between objects [12].

In practice, two approaches are adopted when discussing the global informatization of society: ✓ *Technocratic approach*, considering informatization as an opportunity and a means of increasing labour productivity and managing production processes; ✓ *Sociological approach*, perceiving informatization as a process covering all spheres of human activity with impact on the person himself. In both approaches, there must be answers to an important question – "Does global informatization create problems for the privacy of the participants?". An important task of the digital age is to counteract the processes of unauthorized access to information resources and to take measures for

adequate protection of personal data of users in the network space. These are some of the main requirements formulated by the General Data Protection Regulation (GDPR) that has entered into force. The regulation clearly defines the responsibilities of all participants in information processes (especially in the global network) in this direction, which, however, sets specific requirements for their level of technological literacy [13]. The authors of the article do not deny that "*the process of acquiring technological literacy is costly and not trivial*", and therefore offer a methodology for optimally achieving an effective result, declaring that it "*has a significant contribution to protecting users' privacy and security in the digital world*".

One of the main requirements in the GDPR is formulated as "*right to privacy*", and there are different interpretations, but basically, they reflect the legal right of participants in network processes to personal privacy. This right gives users the opportunity to choose for themselves how much of their personal space can be available to others, managing its expansion and ways of use.

In the contemporary digital age, the information approach is a major component of various public, social, private, and business areas of society's life. E-governance is a typical example of relationships between different areas of society, and e-business and e-commerce also participate in this category. In these two directions, the active use of modern information and communication technologies creates real conditions for the development of initiatives and systems of open government. In the specific implementations of the open management processes, a higher degree of data transparency should be ensured, but at the same time, the requirements for the privacy of the participants should not be violated. To achieve this, it is necessary to conduct a timely risk assessment for the protection of personal data and private resources [14, 15]. The processes and organization of structures in e-business and e-commerce are related to the technologies of the digital world, which requires the development of an adequate resource security policy and protection of personal data. This is a hierarchical policy structure that is summarized in Figure 4.



4.2. Mine requirements for user privacy protection

When organizing an environment for e-business or e-commerce, a system for the protection of processed personal data must be built, which unites the necessary technological structures [16, 17]. An initial requirement is to develop and implement a

data security program in the structure, which contains clear rules for counteracting various external and unwanted impacts, the main categories of which are summarized in Table 2.

Table 2. Major categories of adverse effects

Category	***Comment***
Force majeure circumstances	The cause of the violation must be events related to fire, flood, earthquake, etc., which occur rarely, but are unpredictable and cause serious damage
Technical errors	More frequently occurring causes, although they have a weaker effect (inadvertent operator errors; inadvertent or intentional errors of maintenance and/or administration specialists, etc.; spread of virus programs; electromagnetic emissions; technical failures, etc.);
External threats and attacks	Cause intentional illegal access and violation of the basic rules for information security of data, which may in certain cases have serious consequences.

When choosing a strategy and building an environment for e-business and e-commerce, provision of the fundamental rights defined in the GDPR should be considered:

✓ "*Right to privacy*", ensuring the protection of the space around us (body, home, property, thoughts, feelings, secrets, and identity) with the ability to choose what part of it is made available for use.

✓ "*Right to data protection*" for privacy of personal information and requirement for its protection during processing and access.

Both requirements determine the need for a clearly expressed and informed consent of the individual (Data Subject) for further processing of his personal data, which must also be considered in the cross-border processing of such data.

The basic principles presented below should be followed when organizing privacy procedures.

1. Minimizing the probability of unauthorized removal of personal data from the system by outsiders (by copying, theft of media or printouts, etc.).

2. Ensuring protection against illegitimate access to the system (secrecy of the installation of the system, the exact location of the workstations, the type of hardware and software used and the nature of the stored information).

3. Minimizing the dangerous consequences of system malfunctions.

4. Developing a strategy for quick and efficient system recovery regardless of the type of failure (hardware, file loss or corruption, deleted or compromised data records, etc.).

5. Preparation of a specific plan (instructions, inspection schedule, and responsible officials) based on the adopted strategy.

6. Fulfilment of the requirement "*the right to be forgotten/erased*", which obliges the manager of the e-business/e-commerce system (Data Controller) to maintain collected personal data only for the period of realization of a defined purpose, after which they will be blocked or removed.

7. In a certain case of personal information processing, it is required to implement a pseudonymization procedure so that it cannot be linked to a specific data subject

without the use of additional information. The latter must be stored separately and with necessary protection measures. For the reason stated, pseudonymized data is considered to be information that allows the identification of a specific person. To avoid this, it is possible to apply anonymization of the information, which will ignore the possibility of identifying a specific person which is data subject. This type of data is usually used in the preparation of reports, analysis of market relations, research of development prospects, etc.

8. The e-business and e-commerce processes are related to Internet communications, including the use of the mobile network. This requires compliance with the rules of the data protection regulation, which are briefly summarized in Table 3.

Table 3. Requirements for correct network communications

Requirement	***Comment***
Confidential communication	Prohibition to listen, eavesdrop or store messages without the consent of the Data Subject
Servicers security	Service providers must guarantee the using appropriate measure for this
Data breach notifications	It is the supplier's duty to notify the national authority and the data subject upon detection of a security breach (loss or theft of data)
Traffic and location data	This data must be deleted or anonymized when it is no longer required for communication purposes or for billing purposes, unless otherwise consented to use
Spam consent	To require consent before sending unsolicited commercial messages, SMS text messages and other electronic messages
Public directories	Prior consent must be given before a phone number, email/postal address is included in a public directory
Caller identification	To have the possibility that the caller's personal phone number is not displayed when connecting

5. CONCLUSION

In the public and private sectors, a large amount of information is collected and processed, including personal data about employees, customers, collaborators, etc. In the conditions of the digital society, a huge part of this information is collected, processed, and stored in electronic form, which sets certain requirements for ensuring computer and network security as specific components of the general concept of information security. In the organization of e-business and e-commerce systems, technological and physical measures must be taken to protect the hardware, software, local networks and supported data arrays against external influences, intrusions, and other unwanted events. One of the main tasks is to ensure business continuity to maintain the functioning of business-critical processes with timely counteraction to possible incidents. This requires ensuring mobile and network security, connection point security, internet communications security and last but not least, application security.

REFERENCES

[1] Mkansi, M. E-business adoption costs and strategies for retail micro businesses. *Electronic Commerce Research*, vol. 22, 2022, pp.1153–1193. https://doi.org/10.1007/s10660-020-09448-7

[2] Himki, A., Ramadhan, T., Durachman, Y., & Pramono, E. S. Digital business entrepreneurship decisions: An e-business analysis (a study literature review). *Startupreneur Business Digital (SABDA Journal)*, vol. 1, no. 1, 2022, pp. 107-113.

[3] Ruan, J., Hu, X., Huo, X. et al. An IoT-based E-business model of intelligent vegetable greenhouses and its key operations management issues. *Neural Computing and Applications*, vol. 32, 2020, pp. 15341-15356. https://doi.org/10.1007/s00521-019-04123-x

[4] Wang, F., Ding, L., Yu, H., & Zhao, Y. Big data analytics on enterprise credit risk evaluation of e-Business platform. *Information Systems and e-Business Management*, vol.18, 2020, pp. 311-350. https://doi.org/10.1007/s10257-019-00414-x

[5] Castillo, M. J., & Taherdoost, H. The impact of AI technologies on e-business. *Encyclopedia*, vol. 3, no. 1, 2023, pp. 107-121. https://doi.org/10.3390/encyclopedia3010009

[6] Kedah, Z. Use of e-commerce in the world of business. *Startupreneur Business Digital (SABDA Journal)*, vol. 2, no. 1, 2023, pp. 51–60. https://doi.org/10.34306/sabda.v2i1.273

[7] Romansky, R., & Noninska, I. Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering*, vol. 17, No. 5, 2020, pp.5288-5303 (article MBE2020268), DOI: 10.3934/mbe.2020286;

[8] Romansky, R., & Noninska, I. Cyber space features – security and data protection requirements. *Proceedings of the 2019 IEEE International Conference on Information Technologies (InfoTech-2019)*, IEEE Xplore DL, 2019, 4 p., DOI: 10.1109/InfoTech.2019.8860880

[9] Romansky, R., & Noninska, I. Business virtual system in the context of e-governance: Investigation of secure access to information resources. *Journal of Public Affairs*, vol. 20, no. 3, August 2020, e2072; (https://doi.org/10.1002/pa.2072).

[10] G. Janssens, L. Cuyvers. Challenges of Electronic Data Interchange in the digital age. *International Journal on Information Technologies and Security*, vol. 15, no. 2, 2023, pp. 3-14. DOI: https://doi.org/10.59035/SJRE5572

[11] Atanasov, I., Pencheva, E., Nametkov, A., Trifonov, V. Functionality of policy control at the network edge. *International Journal on Information Technologies and Security*, vol. 11, no. 3, 2019, pp.3-24.

[12] Goryachko, V.V., Choporov, O.N., Preobrazhenskiy, A.P., Kravets, O.Ja. The use of intellectualization management decision-making in the interaction of territorially connected systems. *International Journal on Information Technologies and Security*, vol. 12, no. 1, 2020, pp. 87-98.

[13] Hirschprung, R.S., Tayro, S., Reznik, E. Optimising technological literacy acquirement to protect privacy and security, *Behaviour & Information Technology*, Published online 09 Nov 2020; Taylor & Francis Online: https://doi.org/10.1080/0144929X.2020.1842907

[14] Tsaregorodtsev, A.V., Kravets, O.Ja., Choporov, O.N., Zelenina, A. N. Information security risk estimation for cloud infrastructure. *International Journal on Information Technologies and Security*, vol. 10, no. 4, 2018, pp. 67-76.

[15] Albahar, M., Thanoon, M., Albahr,A. The use of fractal dimension (FD) analysis in detection of anomalies, sabotages, and malicious acts in a cyber-physical system using Higuchi's algorithm**,** *International Journal on Information Technologies and Security*, vol. 14, no. 2, 2022, pp.111-121.

[16] Noninska, I., Romansky, R. Organization of Technological Structures for Personal Data Protection. *International Journal on Information Technologies and Security*, No. 1 (vol. 14), 2022, pp. 97-106.

[17] Romansky, R. Mathematical Model Investigation of a Technological Structure for Personal Data Protection. *Axioms,* 2023, vol. 12, no. 2, art.102. https://doi.org/10.3390/ axioms12020102

Information about the authors:

Irina Noninska is an Associate professor in Cryptography and data security and PhD in Databases and Local Area Networks. Her scientific and research interests are in the area of Information and Network Security, Data Protection, Cryptographic Algorithms and Protocols, Quantum cryptography, Cyber security, Internet of Things, Telecommunication Standards. She is author and co-author of more than 90 scientific papers, articles and 11 books and chapters in books. She is a member of: Union of Scientists, Bulgaria; Union of Automatics and Informatics; International Editorial Board of International Journal on IT and Security; Organizing and Program Committee of Information Technologies.

Radi Romansky is a full professor at Technical University of Sofia, Doctor (Dr) in Computer Engineering and Doctor of Science (D.Sc.) in Informatics and Computer Science; Full member of European Network of Excellence on High Performance and Embedded Architectures and Compilation (HiPEAC). He has over 220 scientific publications and over 25 books. Areas of scientific interests: ICT, informatics, computer architectures, computer modelling, privacy and data protection, etc.

Remark:

Manuscript received on 14 June 2023 and is accepted after double-blind reviewing to take part in the 37th International Conference on Information Technologies (InfoTech-2023), IEEE conference, Rec. # 58664, Section F: "Technological Aspects of e-Governance and Privacy" and has not been published in full text elsewhere.