

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

IRINA NONINSKA, RADI ROMANSKY
TECHNICAL UNIVERSITY OF SOFIA (BULGARIA)

Contents

1. Introduction
 2. Technological Aspect of e-Business
 3. Functional Organization of e-Commerce
 4. Requirements for User Privacy and Data Protection
 - 4.1. Informatization and privacy*
 - 4.2. Mine requirements for user privacy protections*
 5. Conclusion
- References

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.

Keywords

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. In order 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. What can be the main risks for e-business in the modern digital space? The main answer can be connected with 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.

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. 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 and the requirements regarding processes in cyberspace.

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 they enter into and last but not least the challenges of the digital world to privacy and personal data protection.

2. TECHNOLOGICAL ASPECTS 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).

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.

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 web-site (electronic showcase) for the presentation of information about the goods, located according to the seller's marketing strategy.

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).

The following stages can be defined for the specific implementation:

1. Construction
2. Management
3. Implementation
4. Expansion

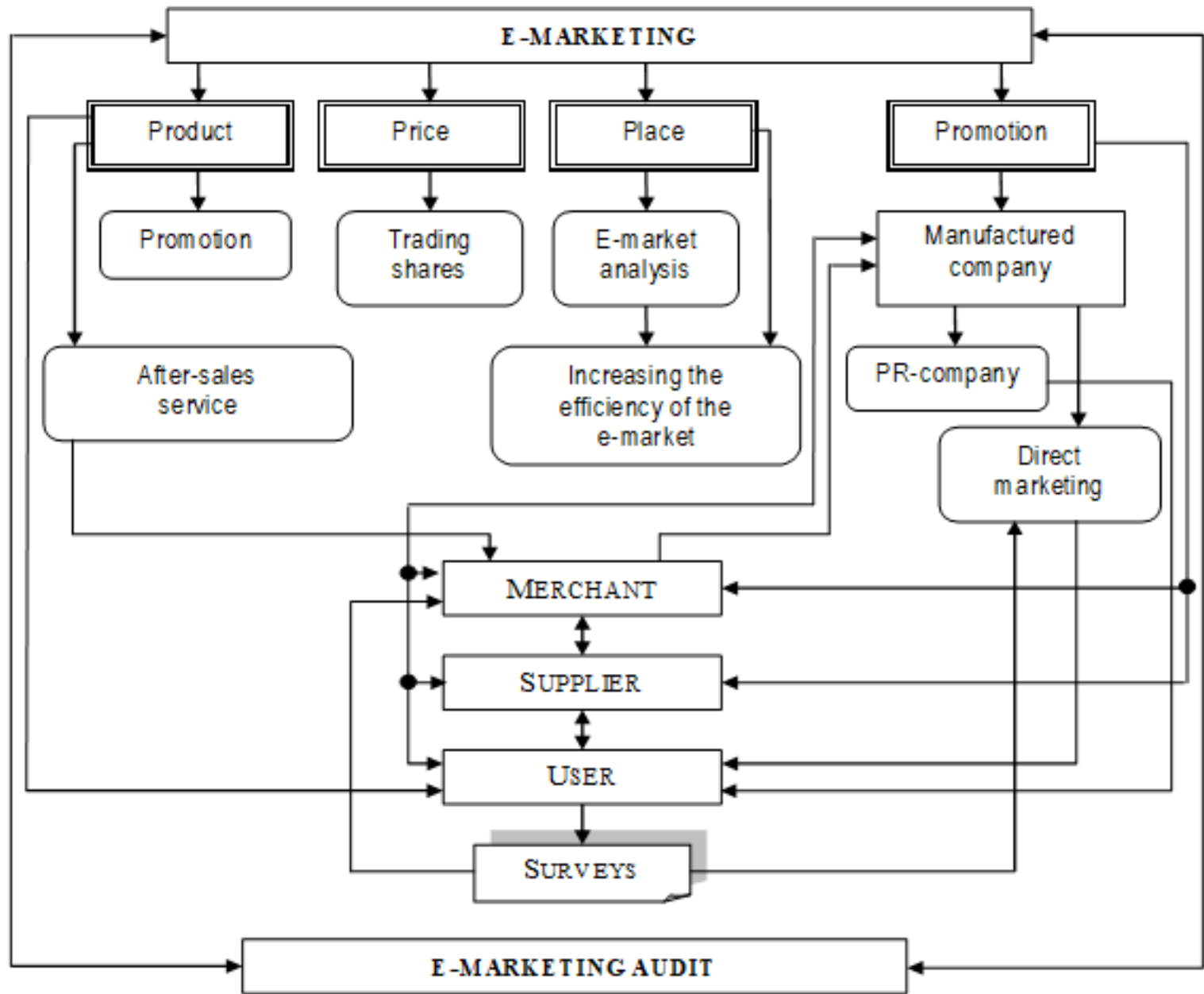
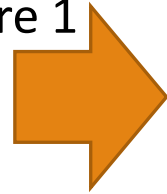
E-business should be seen as a collection of skilled people, technological elements and relevant business processes, which defines several aspects of the infrastructure.

1. Technical aspect
2. Technological aspect
3. Human aspect

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.

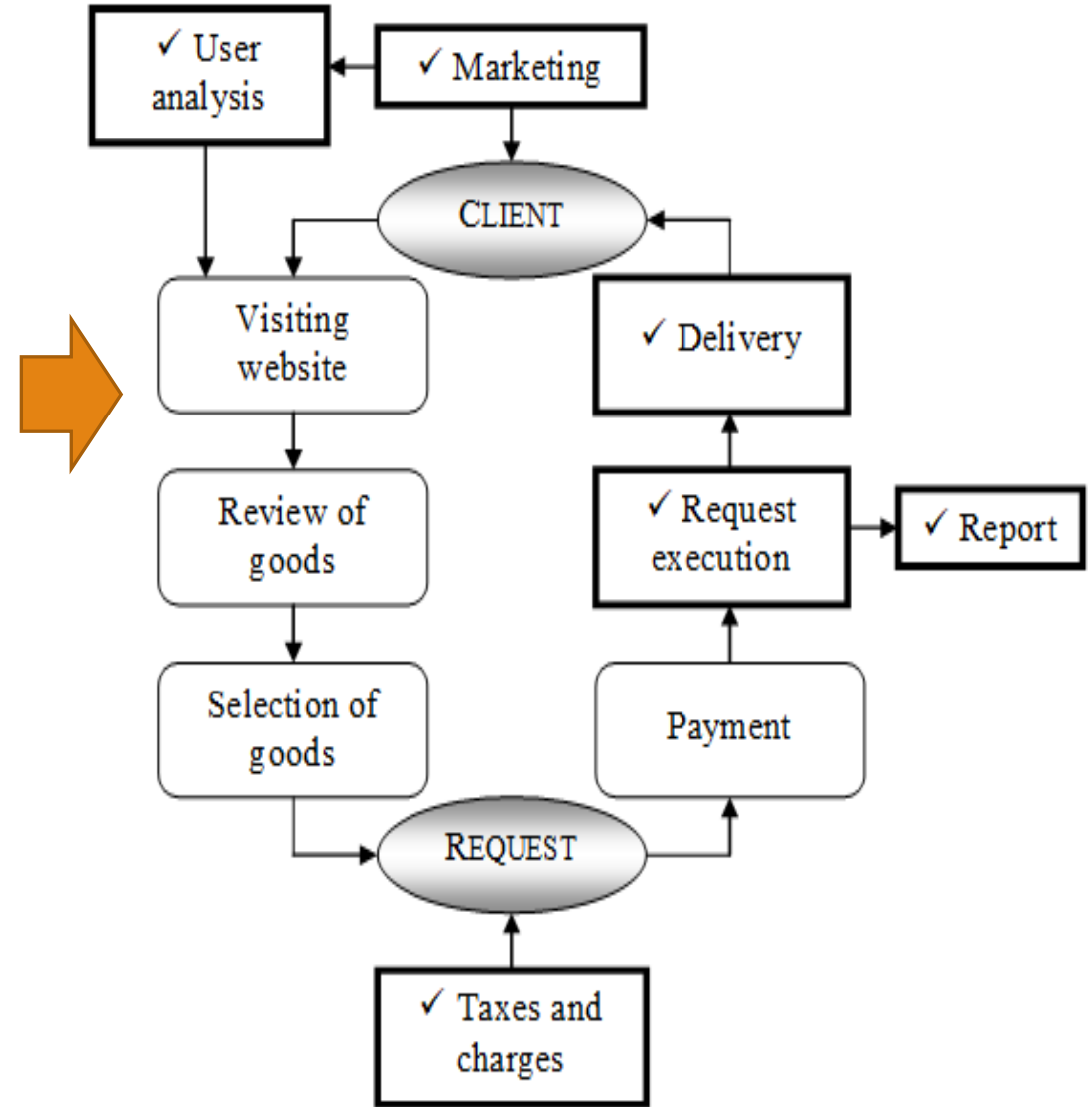
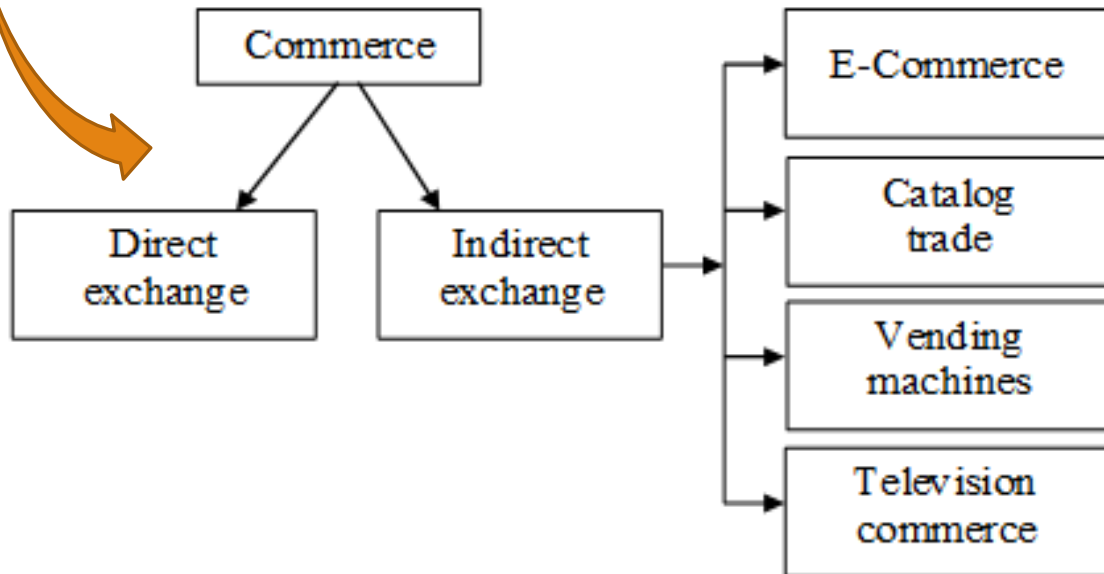
A major category in e-business is electronic marketing (e-marketing), which is the activity of researching a certain market to give an idea of how much a given product or service will be in demand. It includes 4 main elements known as "4p" – **p**roduct, **p**rice, **p**lace, **p**romotion. Functional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



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).

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.



4. REQUIREMENTS FOR USER PRIVACY AND DATA PROTECTION

4.1. *Informatization and privacy*

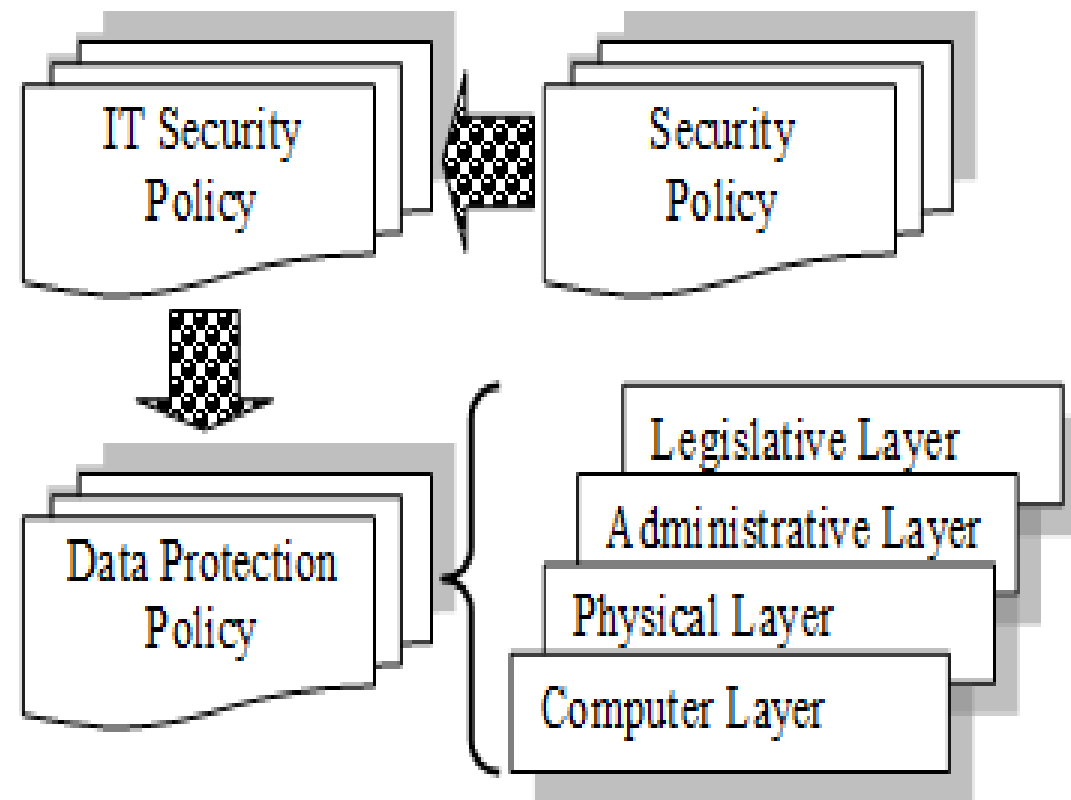
The development of e-business and e-commerce technologies is directly related to an increase in the level of informatization of society in the digital age. The results of this are obtaining new knowledge, higher quality, and speed in the provision of information services, efficiency and improvement of processes in organizational and production systems based on the use of computer equipment and management of all processes through the use of information technologies.

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.

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.

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

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.

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.

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.
2. Ensuring protection against illegitimate access to the system.
3. Minimizing the dangerous consequences of system malfunctions.
4. Developing a strategy for quick and efficient system recovery regardless of the type of failure.
5. Preparation of a specific plan for action 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. Where necessary, apply ***pseudonymization*** and ***anonymization*** principles to protect access to the data owner.

8. Due to the connection of e-business and e-commerce with Internet communications, it is necessary to comply with the rules of the data protection regulation, which are summarized in Table 3.



<i>Requirement</i>	<i>Comment</i>
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

15 publications are included in the list of references

Thank you for your attention
Irina Noninska & Radi Romansky