Current State and Trends in the Development of *E*-Commerce Software Protection Systems

Valentyna Pleskach[a], Viktor Krasnoshchok[a], Mariia Melnyk[a], Svitlana Klymenko[a] and Romanas Tumasonis[b]

[a] *Taras Shevchenko National University of Kyiv, Volodymyrs'ka str. 64/13, Kyiv, 01601, Ukraine*
[b] *Vilniaus kolegija/University of Applied Sciences, J. Jasinskio str. 15, Vilnius, 01111, Lithuania*

Abstract

The purpose of the article is to review and analyse the state and trends in the development of *e*-commerce software systems protection. The publication discusses the problems of ensuring security in *e*-commerce systems, and also highlights the main directions of development of e-commerce systems in a modern digital society. The standard structure of an *e*-commerce system is presented, containing a website, digital infrastructure, an electronic document management system, and data processing systems. A method for analyzing hierarchies for choosing the composition of information security means in *e*-commerce systems and an appropriate optimization method are proposed. It also describes the approach of the legal regulation of *e*-commerce in Ukraine.

Keywords [1]

e-commerce systems, *m*-commerce, security system, information security, legal regulation

1. Introduction

E-commerce is the activity of electronically buying/selling goods or services through digital services using information and communication technologies. It is the future of the world. Over the past five years, the global digital market for *e*-commerce has more than doubled from $ 2.3 trillion to $ 4.5 trillion In the next 20 years, almost all commerce will be transferred to the digital space.

Experts predict that most online sales will be through mobile devices. 95 % of purchases will take place on the global Internet, as a quarter of the world's population is now online shoppers (in 2021 this indicator is 2.14 billion) [1]. The largest *e*-commerce market in the world is in China, in this country accounts for more than 50% of all retail online transactions [2].

More than half of consumers use smartphones for shopping. As the introduction of mobile devices is rapid, especially in regions where there is no other digital infrastructure, mobile commerce (65% of the total volume of transactions through mobile traffic) will be determined by *m*-commerce. Emerging *e*-commerce markets in mobile-oriented countries is a very important factor in the development of this trend. In 2021, *m*-commerce (a powerful segment of *e*-commerce) will occupy 72.9% of the *e*-commerce market. Mobile retail sales as a percentage of global *e*-commerce retail sales 2016 to 2021 according to Statista.com is shown on Figure.1. Source: https://marketer.ua/e-commerce-worldwide-statistics-facts/. Today, most online customers pay by credit card. There are now more than 3.4 billion *e*-commerce users and 24 million *e*-commerce websites worldwide. In 2021, global *e*-commerce sales of the B2C buiseness model will reach $ 4.5 trillion. In 2020, the volume of retail trade via the Internet amounted to more than 4.2 trillion dollars. Cross-border *e*-commerce sales worldwide grew by more

Information Technology and Implementation (IT&I-2021), December 01–03, 2021, Kyiv, Ukraine
EMAIL: v.pleskach64@gmail.com (V. Pleskach); kivinme@gmail.com (V. Krasnoshchok); marija_melnik@ukr.net (M. Melnyk), klymenkosvitlana@gmail.com (S. Klymenko), r.tumasonis@eif.viko.lt (R. Tumasonis)
ORCID: 0000-0003-0552-0972 (V. Pleskach); 0000-0002-0967-9131 (V. Krasnoshchok); 000-0002-1581-335X (M. Melnyk); 0000-0002-3629-8158 (S. Klymenko)

than 20% in 2020. In 2020, *e*-commerce in the US grew by more than 40%, and Amazon's net profit increased by more than 80% in 2020. According to Statista.com, 63% of online shoppers switch to Amazon to start searching for products (Figure 2). Source: https://marketer.ua/e-commerce-worldwide-statistics-facts/

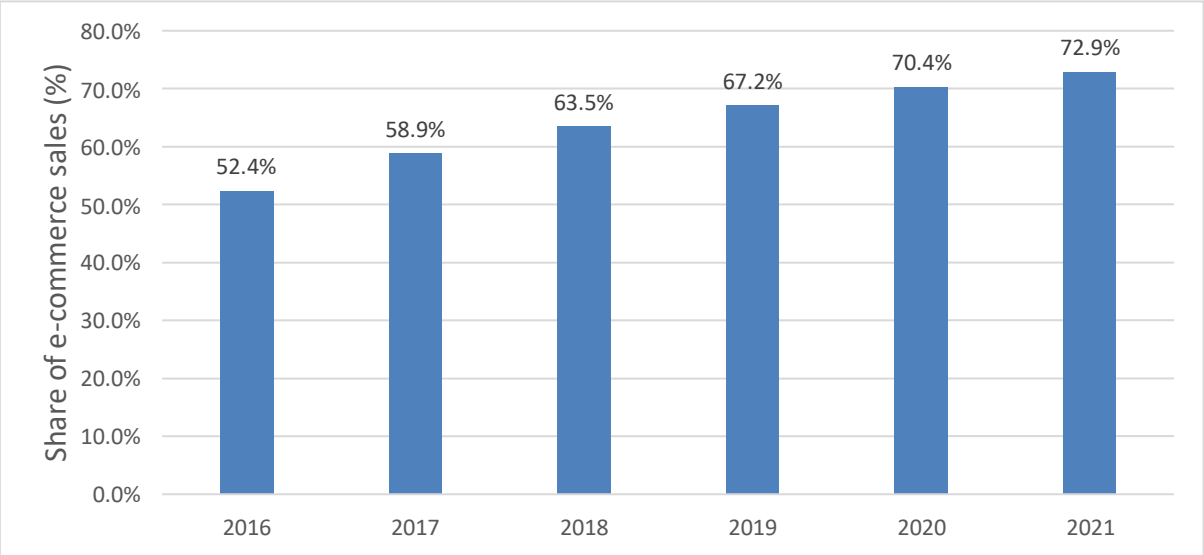

Figure 1. Sales in *m*-commerce as a percentage of global *e*-commerce from 2016 to 2021

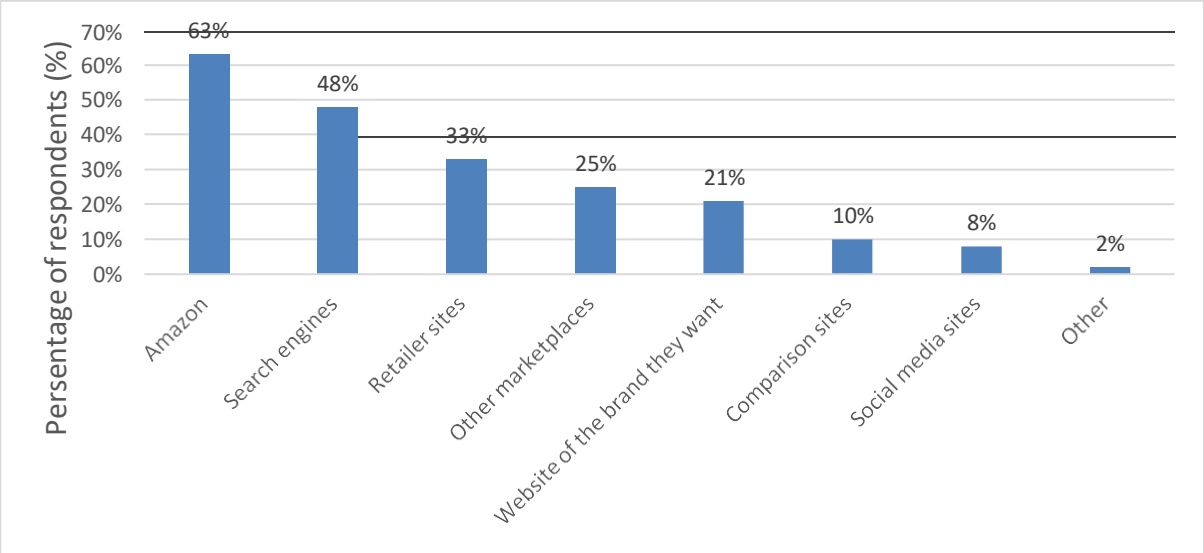

Figure 2. Internet sources used by consumers around the world at the start of their search for products

In recent years, *e*-commerce has become an integral part of the global retail system. *E*-commerce sales worldwide have exceeded $ 3.5 trillion, and *e*-commerce is projected to accelerate even more.

As a result of the COVID-29 pandemic, millions of people have stayed home to prevent the spread of the virus, and digital channels have become an alternative to crowded stores and personalized shopping. In 2020, global *e*-commerce retail traffic reached a record 22 billion visits per month, with a high demand for everyday consumer goods, such as food, clothing and technical goods.

25 % of *e*-shops on the global Internet use WooCommerce. According to statistics, WooCommerce is the most reliable platform for online shopping, occupying 25 % of the market. In second place is Shopify with 19%, and the market share of Wix Stores is 13%. 10 best *e*-commerce platforms for 2021 are nex: BigCommerce, Shopify, Wix, Shift4Shop, WooCommerce, Volusion, Prestashop, Weebly, Squarespace, Magento [3].

The most famous *e*-commerce sites are Amazon (traffic of 2.5 billion visitors per month); eBay (940 million visitors per month); Walmart (traffic 450 million visitors per month); Craigslist (traffic 420

million visitors per month; Etsy (traffic 352 million visitors per month) . Top seven countries that spend money on the global Internet are China, USA, UK, Japan, Germany, France and South Korea. Industry of *e*-commerce is growing by 23% year on year.

As mentioned in [4], *e*-commerce is becoming more and more important in national economies every year, it is the flagship of innovation, the latest information technology (IT) and *e*-services through the use of *e*-transactions. In Ukraine, the number of electronic orders of goods increases by about 25% annually, the number of users who purchased goods/services online in 2021 is 44%, and the percentage of GDP comprised of *e*-commerce sales - 2.56% (Figure 3).

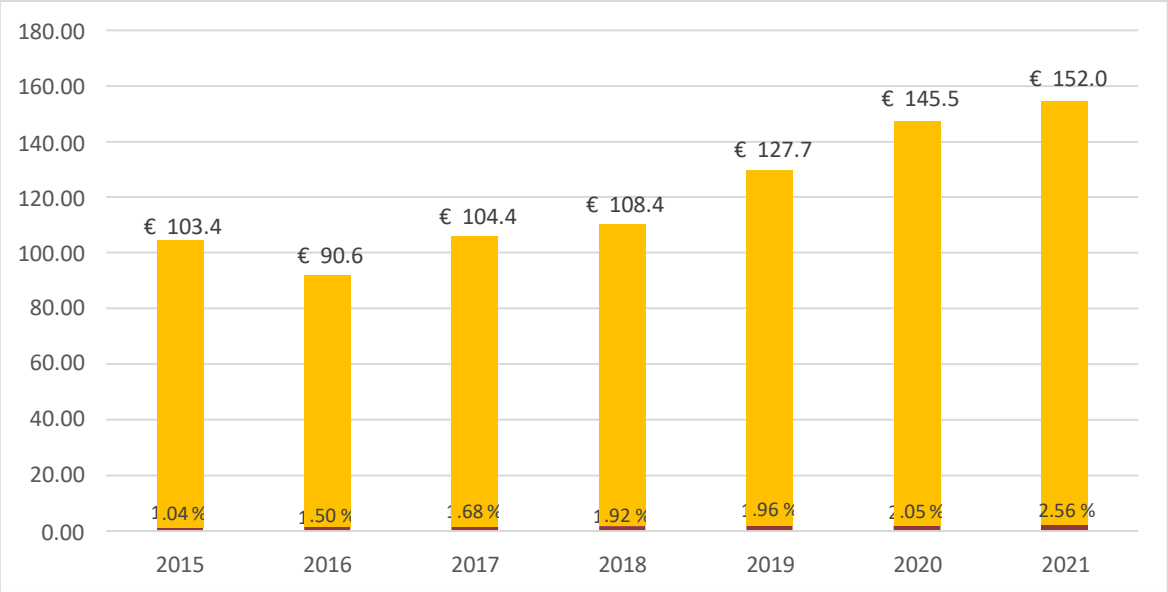

Figure 3. The Gross Domestic Product (GDP) in €Billion and the percentage of GDP comprised of *e*-commerce sales

Source: *https://ecommerce-europe.eu/wp-content/uploads/2021/09/2021-European-E-commerce-Report-LIGHT-VERSION.pdf (P.94)*

According to the report in 2021 European B2C E-commerce Report 2020 (Europe *e*-commerce report 2021, [5, P.10]) there are such indicators of average growth in percent, in particular in Moldova - 49%, Russia - 41%, Poland - 34%, Romania - 30%, and in Ukraine - 22%. According to the same report [5, P.6], Ukraine ranks 66th in terms of the Logistics Performance Index (LPI - measures the efficiency of logistics of supply chains within the country); 64th place in terms of ease of doing business; 69th place on the *e*-Government Development Index (E-Government Development Index measures the willingness and ability of government administrations to use information and communication technologies to provide public services), 48th place on the inclusive Internet index (Internet accessibility benchmark); 30th place in the Postal Development Index based on reliability, relevance and sustainability), 51st place in the UNCTAD B2C *e*-commerce Index that measures the economy's willingness to support online shopping), 60th place in the Environmental Performance Index, 78th place regarding the indicator of Global Cybersecurity Index: This index maps questions on Member State cybersecurity commitments across five pillars: legal measures; technical measures; organizational measures; capacity development measures; cooperation measures.

2. Problem statement

These statistics show the extraordinary role of *e*-commerce systems in the digital society, and the latest Global Cybersecurity Index shows the unresolved issues of security threats to *e*-commerce systems. The most important task in the development of digital society is to build a comprehensive system of security of *e*-commerce platforms. This publication is devoted to the problems of *e*-commerce systems as objects of security and cybersecurity.

There are different types of threats faced by *e*-commerce: denial of service or distributed denial of service attacks, DDoS attack, SQL injections, XSS attacks, customer journey hijacking, bad bots, credit card frauds, etc. The standard structure of an *e*-commerce system can be represented in the form of a website, network (digital) infrastructure, document management information system that reflects the processes of business infrastructure, data processing and storage systems. Organizational and technological process of information processing can be submitted through the processes of authorization, user identification, request (ordering, creating a personal account, forming a response), order payment (input/output of payment details, confidential information with limited access), receipt of goods/services and deletion of data if necessary by the user ("right to be forgotten" [6]) or administrative disconnection from the *e*-commerce system. From the point of view of information security, the processes of user authorization, transfer of identification / authentication data, personal data, transfer of financial resources, storage and processing of restricted data, data substitution, etc. can be vulnerable. The widespread use of personal data in *e*-commerce systems creates the preconditions for a large number of violations or threats in their processing, including their collection, accumulation, storage, renewal and use, which significantly increase the risk of illegal interference by third parties.

The State Service of Special Communications and Information Protection of Ukraine, Cyberpolice, and the Security Service of Ukraine are state regulatory authorities in the field of *e*-commerce.

Based on current trends in *e*-commerce, including its rapid growth, mobile commerce, automation of B2B sales, development of omnichannel trade, introduction of CDP instead of CRM, growing popularity of marketplaces, social commerce, partnership with influencers, simplification of entering *e*-commerce with the help of zero-coding, growing interest in PWA, the use of artificial intelligence, the introduction of dynamic price setting, the growing popularity of chatbots, the use of augmented reality, the promotion of voice commerce, video consultations from offline stores, a variety of electronic payment systems, should focus on relevant latest protection systems for *e*-commerce systems.

3. The results and discussion

Common requirements and model solutions for information security and cybersecurity in *e*-commerce software systems.

The information security system of *e*-commerce platforms should include such components as: means of protection against unauthorized access; cryptographic means of information protection, including qualified electronic signature, cryptographic transfer protocols; monitoring and control of compliance with information security requirements at digital infrastructure facilities of *e*-commerce systems; antivirus protection tools; means of intrusion prevention; event logging and cyber incident detection tools; means of ensuring continuity and resumption of activities. The types of *e*-commerce security threats are internal human or non-human (accidental / intentional) and external human or non-human (accidental / intentional). The choice of the most appropriate *e*-commerce security system can be made by various methods, for example, by the analytic hierarchy process (AHP) by Thomas Saaty: pairwise comparison of alternatives, multi-criteria evaluation. It is possible, for example, as alternatives to take separately software and hardware, singly software, separately hardware and take cost, reliability, accessibility as criteria in adjustment of the corresponding maintenance (Figure 4). Source: Author`s model solution. According to the security model, one of the main criteria for choosing protection is the number of threats. The cost of the implemented means of protection, the ratio of protection costs should not exceed the cost of information and the magnitude of the maximum risk. In [7] work, when choosing the rational composition of means of security of the *e*-commerce system, it is proposed to use such criteria as: the cost of means of protection; the amount of prevented damage; the number of threats that are prevented; interoperability with other means of protection. These criteria can have both quantitative and qualitative assessment depending on the issues that arise. The set of assessments against these criteria will indicate the overall effectiveness of the security. The better the performance of the evaluated tool, the higher the priority it will have over other alternatives. The more complete, effective and rationally selected set of means of protection is used, the higher will be the general security of *e*-commerce systems. The problem of choosing the means of information protection and cybersecurity in *e*-commerce software systems can be presented as an optimization problem:

$$F(x_i) \to opt, i = 1..n \quad (1)$$

where $F(x_i)$ is a function that depends on n factors that affect the security of *e*-commerce software systems. Depending on the problem statement, formula (1) can take the form:

$F(x_i) \to max, i = 1..n$, for example, in the case of maximizing the effectiveness of protection;

$F(x_i) \to min, i = 1..n$, for example, in the case of minimizing the costs incurred by an individual or legal entity in the case of threats to the security of the *e*-commerce software system.

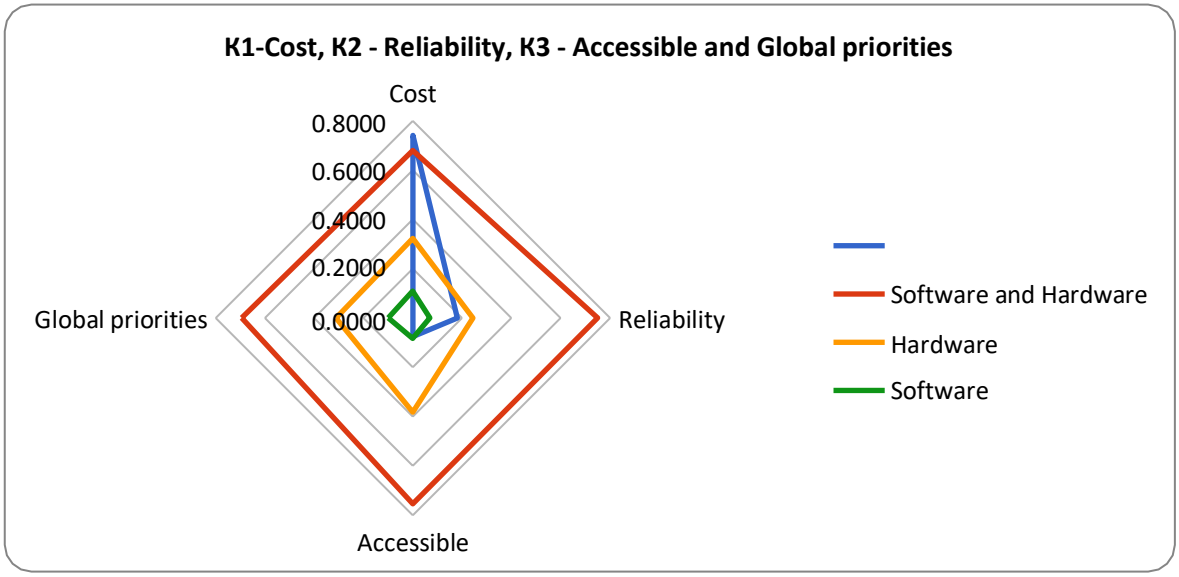

Figure 4. Indicators of the values of the three criteria of cost, reliability and accessibility when choosing the composition of the *e*-commerce security system

Similar problems have already been considered in works by Oladko V. [7], Petrov A. [8], [9].

Such problems are formulated and solved such as as linear programming problems.

The main limitations in such problems are the resources (financial, informational, human) that are allocated to information security and cybersecurity.

The maximization and minimization problems can be solved simultaneously, but it is obvious that these problems are not linear. So, in the problem of finding the maximum investment of a small amount of money will lead to low efficiency of protection. Doubling the funds will not double the security means. Similarly, achieving the maximum effectiveness of security (which is less than 100%), doubling the cost will not improve efficiency. Funds allocated for protection are spent discretely, not continuously. So, if you allocate funds to pay for the work of system administrators, you can hire, for example, 2 or 3 system administrators, rather than 2,71. Thus, the algorithm for determining the means of information security and cybersecurity in *e*-commerce software systems will be as follows:

1. determining the list of requirements for the *e*-commerce software system;
2. determination of the composition and subsystems of protection;
3. choice of means of protection;
4. determination of approximate quantitative indicators of factors that affect the effectiveness of means of protection. Approximate quantitative indicators can be calculated, for example, by the method described in [6];
5. choose a more important factor;
6. for the selected factor for all values that satisfy the requirements of $|x_i - \hat{x}| \leq 1$, where

x_i – is the approximate calculated value of the factor

$\hat{x}$– is an arbitrary integer

calculate at $x_i = \hat{x}$approximate quantitative indicators of all factors for which the exact value has not yet been determined;

7. calculate the effectiveness of protection for each obtained value of the factor and the approximate values of other indicators;
8. choose the option in which the effectiveness of protection will be the best;

9. record the value of the factor selected in step 5 and conduct all subsequent calculations with a fixed value of this factor;

10. go to step 5. The algorithm continues until all the factors are sorted.

By constructing the response surface in this way, you can optimize the choice of information security and cybersecurity in *e*-commerce software systems.

Also extremely important is the issue of regulatory protection of *e*-commerce systems.

4. General principles of legal regulation of *e*-commerce in ukraine

Since about the mid-1990s, there have been objective changes in legislation in many countries around the world to regulate business through telecommunications. Innovative use of the Internet has become the basis for the introduction of e-business and its component - *e*-commerce, which is reflected in its key place in the segment of national markets in most countries [10]. The essence of such a transformation is that the market has acquired convenient and adapted to today's conditions forms of communication in the areas of consumption and distribution of property and other goods, as a result, the offer and acceptance, as the driving force of trade, have acquired completely new ways of recording the initiative, consent or denial. In this regard, there are relations that are aimed at making a profit that arise during the transaction to acquire, change or terminate civil rights and obligations with the remote use of information and telecommunications systems. The classic agreement is increasingly giving way to a transaction, the specificity of which is traditionally seen in a special material medium on which the content of the agreement and the conclusion in electronic form is recorded, which excludes physical contact between the parties [11, P.87].

Legal support of such activity requires determining the range of principles enshrined in the legislation of a mandatory nature, determining the grounds and procedure for the transaction, the peculiarities of its fixation and operation, the requirements for participants, the scope and nature of their rights, responsibilities with the guarantee of liability in case of violation. These are the basic principles of *e*-commerce - the basic rules of binding nature, in accordance with which there is legal regulation. Since *e*-commerce is a segment of the property sector, the legal basis for its operation is a systemic set of basic elements that act as indisputable requirements that ensure the balance of public and private interests. As general principles in the form of guiding legal provisions, they are enshrined at the international legal, complex, sectoral and institutional levels, which ensures stability and stimulates regulatory progress in this area, as market participants receive a coordinate system that reveals the full range of opportunities for legal entities in a particular area.

General imperatives are contained in international legal documents (UNCITRAL Model Law on Electronic Commerce (1996), which is an element of *e*-commerce, UNCITRAL Model Law on Electronic Signatures (2001)); in regional legal documents, delineated by European borders (conventions, declarations, directives and resolutions defining priorities for national economies, focused on the latest information technologies); in national legal documents (codified legislation and laws in the field of *e*-commerce). General principles of civil law, regulated in Article 3 of the Civil Code of Ukraine and the general principles of management, defined in Article 6 of the Civil Code of Ukraine lay the foundations for the functioning of *e*-commerce at a comprehensive level, their vector expansion has a specific sectoral focus enshrined in Articles 12, 13 of the Civil Code of Ukraine on of implementation of the civil laws. The proposed measures to recodify the Central Committee of Ukraine include not only clarification of areas in which private law relations are formed, but also expansion of general principles in particular in the information sphere - freedom of information and information exchange, inadmissibility of arbitrary interference in personal information [12, PP .7-8], which is directly related to *e*-commerce.

Consolidation of *e*-commerce principles at the institutional level is contained in Article 5 of the Law of Ukraine on *E*-Commerce [13], the provisions of which are a structural set of several components - the basis for *e*-commerce, the requirement to regulate restrictions, expand the presumption of legality, defined in Article 204 of the Civil Code of Ukraine in terms of the form of the transaction and the establishment of a legal incentive for lawful behavioral activity, the activity of distribution of certain goods, performance of works or provision of services is subject to obtaining a license or permit.

Proper legal organization of *e*-commerce relations is ensured by the functioning of the mechanism of exercising the rights and responsibilities of entities by complying with all elements of the system of basic provisions, resulting in a comfortable environment where justice, integrity and reasonableness prevail. The importance of consideration of the norms of international law in the implementation of legislation in the field of commerce is due to the global availability of digital services, which is primarily related to personal data of the users. In general, the analysis of the legislation of the EU countries shows that the issues of application of digital, information and communication technologies are regulated by the following types of legislative acts, in particular, the Laws on: *e*-commerce (trade), which covers the widest range of public relations; electronic document; electronic digital signature; electronic payments related to the use of various electronic payment systems and digital money.

The only recognized international treaty for the protection of freedom, security and human rights on the World Wide Web is the Budapest Convention on Cybercrime [14], developed by the Council of Europe in 2001 and ratified by the Verkhovna Rada of Ukraine in 2005. Under the Convention, any illegal access to, interception or interference with computer data is considered illegal. The Convention includes personal data of individuals or confidential data of legal entities placed on computer networks.

In 2000, the European Parliament and the Council of the EU adopted a Directive on certain legal aspects of information services in the internal market, in particular on *e*-commerce (the *E*-commerce Directive) [15]. Its purpose is to approximate certain national regulations to the existing uniform requirements for the subjects of relations related to the provision of information services in the EU internal market, requirements for service providers, requirements for means of commercial communication (electronic means, means of communication) used in this area, as well as general requirements for the liability of intermediaries and provisions for the development of codes of conduct. The Directive also contains basic provisions on the organization of cooperation between EU member states in the field of *e*-commerce. Conclusion 1/2000 " On Certain Data Protection Aspects of Electronic Commerce" [16] developed by the Working Group draws particular attention to the importance of personal data protection in the *e*-commerce process, outlines European experience in regulating this issue at the legislative level. Whereas the legal framework for the protection of the fundamental right to privacy and the protection of personal data must comply with the principles of data protection laid down in Directive 95/46/EC [17] and Directive 2002/58/EC [18], which complements them in the field of telecommunications and contains a clear explanation of the full and proper application of data protection law to Internet services. The Working Group also considered the issues of personal data protection, taking into account the characteristics of the latest information technologies, and made relevant Conclusions on public sector information and personal data protection 3/99 [20], Recommendations on automated processing of personal data on the Internet 1/99 using software and hardware and Recommendations on the retention of traffic information by ISPs to ensure law and order 3/99 [21].

The Working Group also clarified the application of the European Data Protection Regulations to data processing for e-mailing purposes and stressed that a detailed and relevant mailing list must be in place. Before launching an advertising campaign or commercial mailing, the mailing organization or institution must have a detailed and relevant list of potential e-mail addresses that can be obtained from the Internet by collecting directly from consumers or website visitors. The features of electronic commercial mailings, which create the preconditions for the emergence of risks, include: low cost of practical implementation of this procedure for the sender, compared to traditional methods of direct marketing; the minimum time required for its implementation.

The *e*-commerce directive clearly defines the following technical aspects: the obligation to identify commercial e-mail, the obligation to verify and respect the registers of non-mailing lists where they are provided for by national regulations. However, this Directive does not in any way aim to change the legal principles and requirements of the existing legal framework. As data protection legislation fully applies to e-commerce, the implementation of the E-commerce Directive must fully comply with the data protection principles. Despite the availability of protected technologies and specialized software, the introduction of the principles of self-regulation and raising the level of awareness of users about the existing risks only at the legislative level can protect the right to privacy and protection of personal data.

The General Data Protection Regulation (GDPR) [21] is a strict regulation within the framework of European Union legislation on the protection of personal data of all persons within the European Union

and the European Economic Area, designed to provide citizens with and EU residents to control their personal data and simplify the regulatory environment for business by unifying regulation within the EU.

5. E-commerce software protection services

Email services are used to forward e-mail messages. Electronic mail requires a number of programs and services. E-mail messages are stored on e-mail servers in databases.

E-mail clients contact e-mail servers to send and receive messages. E-mail servers interact with other e-mail servers to exchange messages between domains. An email client does not connect directly to another email client to send a message. Both clients must trust the transport of messages to the e-mail server. E-mail supports the use of three separate protocols: Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), and Internet Message Access Protocol (IMAP). SMTP is used to interact with the programs that send mail. The client receives e-mail using one of two application-level protocols: POP or IMAP. Various services are used to protect *e*-commerce software systems. Access to network devices is usually controlled by authentication, authorization, and accounting services. These services, called AAA (authentication, authorization, accounting), provide the basic infrastructure to set up access control on a network device. AAA allows you to control which users have access to the network (authentication), what actions they can perform while on the network (authorization), and also allows to monitor their actions while accessing the network (accounting).

This concept is similar to using a credit card. A credit card determines who can use it, how much the user can spend, and records the goods and services that the user buys.

Intrusion Detection Systems (IDS) passively monitor network traffic. Isolated IDS systems are significantly inferior to intrusion prevention systems (IPS). However, the IDS detection function is part of any IPS implementation. An IDS-enabled device copies the traffic flow and analyzes the copied traffic, but not the transmitted packets themselves. Working offline, the system compares the flow of captured traffic with known malicious signatures similar to software that checks for viruses.

The IPS system is based on IDS technology. But unlike it, the IPS system is installed on the path of traffic. This means that all incoming and outgoing traffic must pass through the processing device. IPS does not allow packets to enter a trusted part of the network without prior analysis. The device can detect and fix network issues immediately. The Universal Threat Management System (UTM) is the common name for a comprehensive security system. UTM systems cover all the functionality of firewalls with status tracking and intrusion detection and prevention services (IDS/IPS). The firewall with status tracking provides packet filtering with status tracking by using information about active connections, which is stored in the status table. The status tracking firewall tracks each connection, recording source and destination addresses, as well as source and destination port numbers.

In addition to IDS / IPS and status tracking firewalls, UTM systems also typically provide additional security services such as:

- protection against unknown threats (Zero Day);
- protection against DoS-attacks (denial-of-service attacks) and DDoS-attacks (distributed denial-of-service attacks);
- filtering programs on a proxy server;
- filtering e-mail for spam and phishing attacks;
- protection against spyware;
- network access control;
- VPN services.

These functions may vary depending on the UTM provider.

Modern firewalls provide the following functionality:

- control of behavior within the programs themselves;
- restrictions on the use of the Internet and Web applications based on the state of the site;
- preventive protection against Internet threats;
- application of policies based on user profiles, devices, roles, types of programs and threats.

6. Conclusions

Some of these changes in the *e*-commerce landscape are certainly long-term due to the panepidemia, digital buying/selling skills, and the digitalization of society. For consumers, systemic issues related to connectivity, affordability, skills, and trust (e.g., digital security, privacy, and consumer protection) have become more acute. To solve this issue, it is necessary to extend accessible and high-quality broadband communication to rural areas at the state level, increase financial accessibility and information culture. It is necessary to promote the participation of the most vulnerable population in *e*-commerce, for example, through the implementation of community-based delivery programs for the elderly, to protect vulnerable consumers from unfair business practices and dangerous goods, to support the creation of innovative *e*-commerce business models, ensuring that the regulatory framework is flexible to combine online and offline business functions. According to the results of the study, it can be concluded that *e*-commerce systems are exposed to a number of threats and attacks due to distributed dispersion, availability of connections to global networks, round-the-clock availability of digital services, and a large number of users. Therefore, the model decision on the choice of rational composition of means of protection in *e*-commerce systems is of paramount importance.

7. References

[1] Pavlenko A. E-commerce 2021: 21 indicator characterizing the industry. https://vc.ru/trade/200161-e-commerce-2021-21-pokazatel-harakterizuyushchiy-otrasl. Accessed on: October, 2021.

[2] Why China has the fastest growing e-commerce in the worldhttps. https://1news.com.ua/tsikave/chomu-v-kytayi-najshvydshyj-rist-elektronnoyi-komertsiyi-u-sviti.html. Accessed on: October, 2021.

[3] DeMatas D. 10 best e-commerce platforms compared&rated for 2021. https://www.ecommerceceo.com/ecommerce-platforms/. Accessed on: October, 2021.

[4] Pleskach V., Zatonatska T., Oleksyuk L. Problems e-commerce development in Ukraine. Scientific journal Economy of Ukraine. №17.11(672). P.73-84. Accessed on: October, 2021. http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=EkUk_2017_11_6

[5] 2021 European e-commerce report. 111 p. https://ecommerce-europe.eu/wp-content/uploads/2021/09/2021-European-E-commerce-Report-LIGHT-VERSION.pdf. Accessed on: October, 2021.

[6] Pleskach M. On the issue of realization of the right to be forgotten of users digital services in Ukraine. Modern achievements of EU countries and Ukraine in the area of law. Collective monograph. Izdevniecība "Baltija Publishing". Riga, 2020. Part 1. PP. 389–406. http://baltijapublishing.lv/omp/index.php/bp/catalog/view/58/1058/2317-1.

[7] Oladko V. The model of the choice of rational composition of the protection system in e-commerce. Scientific journal Cybersecurity issues.2016. №1(14). https://cyberleninka.ru/article/n/model-vybora-ratsionalnogo-sostava-sredstv-zaschity-v-sisteme-elektronnoy-kommertsii/viewer. Accessed on: October, 2021.

[8] Petrov A. Model of the optimal choice of information systems in computer networks. Bulletin of Volodymyr Dahl East Ukrainian National University: Science. Luhansk: SNU named after V. Dalia, 2013. № 15 (204). Part 1. PP.166-171. http://dspace.snu.edu.ua:8080/jspui/handle/123456789/2776. Accessed on: October, 2021.

[9] OECD/Inter-American Development Bank (2016), [Consumer protection and e-commerce", in Broadband Policies for Latin America and the Caribbean: A Digital Economy Toolkit, OECD Publishing , Paris. DOI: https://doi.org/10.1787/9789264251823-16-en. Accessed on: October, 2021.

[10] Holovii, L.V., Yanchuk, Yu.V. (2020). Legal regulation of information relations in the field of electronic commerce. «LAW. HUMAN. ENVIRONMENT». Vol.11, №2. 2020. P. 151. http://journals.nubip.edu.ua/index.php/Pravo/article/download/14152/12494. Accessed on: October, 2021.

[11] Cherkashyn, S.V., Milash, V.S. (2016). Aspects of concluding an electronic contract. Law and Society, №3. Part 2. 2016. PP. 87-91.
[12] The concept of updating the Civil Code of Ukraine. (2020). "ArtEK" Publishing House, Kyiv. 128 p. https://yurincom.com/legal_news/new_legislation/kontseptsiia-onovlennia-tsyvilnoho-kodeksu-ukrainy/
[13] "About electronic commerce" Law of Ukraine № 675-VIII of September 3, 2015. Information of the Verkhovna Rada of Ukraine. 2015, №245. 410. https://zakon.rada.gov.ua/laws/show/675-19. (Accessed on: October, 2021).
[14] Budapest Convention on Cybercrime. URL: http://zakon0.rada.gov.ua/laws/show/994_575 (Accessed on: October, 2021).
[15] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031
[16] Opinion 1/2000 of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data, established pursuant to Article 29 " On Certain Data Protection Aspects of Electronic Commerce", adopted on 3 February 2000: WP 28 (5007/00/EN/final). URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000 /wp28_en.pdf (Accessed on: October, 2021).
[17] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such dat. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046. (Accessed on: October, 2021).
[18] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002L0058/ (Accessed on: October, 2021).
[19] On the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the community and in third countries. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp46_en.pdf
[20] Working Party on the Protection of Individuals with regard to the Processing of Personal data. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp17_en.pdf
[21] Privacy on the Internet - An integrated EU Approach to On-line Data Protection. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp37_en.pdf
[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj