UDC 339.187

**Ilona Dumanska**[1]

# ENSURING DIGITAL TRUST IN E-COMMERCE WITH CYBER SECURITY GUARANTEES

[1] Khmelnytskyi National University

**Abstract:** *The publication substantiates that the basis of digital trust in e-commerce is cyber security, which provides confidence in the protection of information during the interaction between the seller and the buyer in the Internet environment. It is established that the pillars of digital trust are such parameters of loyalty and reputation of sellers as security, transparency, reliability and interaction with the user. Strategic digital trust safeguards for transparency, privacy and security are identified as AI-based data monitoring, investment in talent and infrastructure, data trust, Blockchain technology, customer trust. It has been proven that ensuring digital trust in e-commerce is based on cyber security guarantees.*

**Key words:** digital trust; e-commerce; cyber security; guarantees.

With the rapid growth of e-commerce in the world, the volume of cybercrime is increasing. If we look at digital fraud as a separate country, with a damage of 6 trillion dollars in 2021, it would be the country with the third most powerful economy in the world after the USA and China [1]. By 2025, cybercrime will cost the world economy up to 10,5 trillion dollars annually. Back in 2015, this amount was estimated at 3 trillion dollars, that is, in 10 years, the threat grew 3,5 times. Thus, cyber security is a key component of digital trust in international e-commerce, its basis. Buyers should be confident that their personal information is protected when interacting with the seller's company online. This approach determines the implementation of strict security measures to protect against cyber threats, the use of encryption to protect confidential data and ensure the safe storage of all customer data.

Digital trust is critical in today's digital world to the success of businesses engaged in e-commerce and defines the limits of its change. Digital transformation is a challenging task. Countries that have reached the highest level of digital maturity had to solve complex cultural, organizational, technical problems, and only taking into account all these factors made these transformations successful. In order to become today's digital leaders in specific areas of the economy, it is necessary to guarantee the reliability of digital trust in international trade in the presence of a cyber threat to the information environment.

For Ukraine, the problem of digital trust and cyber security has not only a monetary dimension - from the very beginning, Russian armed aggression has also been conducted in cyberspace. Therefore, it is extremely important for us to understand the trends and challenges for cyber security in order to guarantee economic security. If we talk about the level of knowledge of cyber threats among ordinary citizens, the situation here is even more complicated. In October 2022, a study within the project «Digital emergency support of civil society in Ukraine» [2] demonstrated that 64% of surveyed Ukrainians fell into crisis situations related to online security; the level of digital skills of 55% of respondents was below average.

According to the World Economic Forum [3], digital trust is defined as expectations of individuals that digital technologies and services will protect the interests of all stakeholders and support societal expectations and values. More specifically, digital trust involves building a strong online reputation, increasing trust and transparency, and delivering an exceptional customer experience. This includes implementing security measures to protect against cyber threats, being transparent about how customer data is collected and used, and ensuring a smooth and seamless online experience.

The four pillars of digital trust are security, transparency, reliability and user engagement, and companies must prioritize them to improve their digital reputation and build long-term customer loyalty. Digital trust also has a significant impact on customer behavior, brand reputation and customer loyalty. Companies must therefore invest in robust security measures and transparent data collection and use policies to ensure customer data is protected and privacy is preserved. Finally, companies should use technologies such as artificial intelligence and data reliability to monitor data accuracy and improve data security and control while managing legal data rights [4].

Under such realities, the model of zero trust has become the new normal. «Never trust, always verify» is a key tenet of the Zero Trust architecture, which gained popularity after the start of the pandemic

and companies moving to hybrid clouds for remote work [5]. The zero-trust model takes as an axiom the fact that every user in the system is considered a threat, requiring constant verification and confirmation of necessary access. Incidentally, these are also the basic building blocks of digital trust and zero-trust implementation models (Fig. 1).

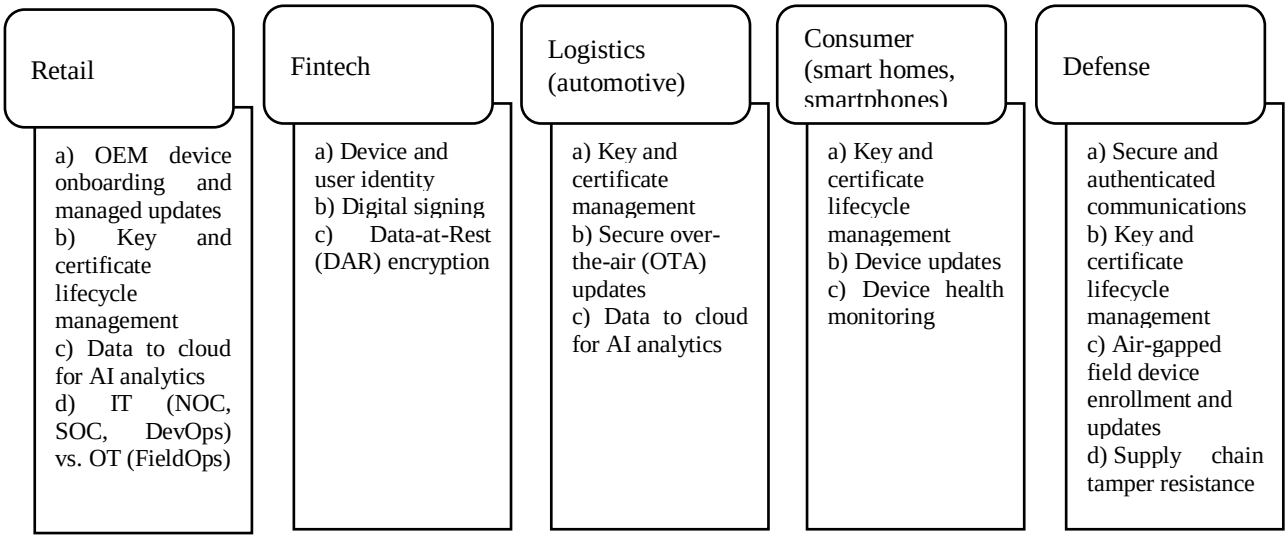


Figure 1 - The primary challenges to digital trust in e-commerce [5]

In practice, multi-factor authentication models are often used on various services when, in addition to the password, we are asked for additional confirmation (code from SMS, email, etc.). This is the concept that will become the only acceptable for organizations that want to protect their data and exist safely in the digital environment.

Changing the usual technologies: eSIM, access keys instead of passwords. SIM-cards as physical objects, which we have been used to since the beginning of mobile communication, may very soon disappear into oblivion. The so-called eSIM technology instead of a physical chip offers a digital code that can be transferred from an old phone to a new one. The technology became available as early as 2017, but Apple's decision to release the iPhone 14 in the US without a physical SIM card slot will force millions of people to start using eSIM in 2023. This will make it easier to have multiple profiles with numbers from different operators at the same time, and also eliminate the risk physical loss or theft of the SIM card [4].

Below are five strategic digital trust safeguards to ensure transparency, privacy and security:

1. AI-based data monitoring: Use artificial intelligence algorithms to verify the accuracy, authenticity and reliability of data [6] in real-time, while detecting missing or unexpected data, this will ensure data is used as intended and help maintain trust.

2. Data trusts: Use data trusts to manage data for others by acting as a trusted third party that verifies, controls and protects data while managing legal data rights on behalf of its beneficiaries. This will increase digital trust, making data management and sharing more reliable and easier.

3. Blockchain technologies: use blockchain as a means of digital trust, applying it to digital fingerprints, identification, assets and smart contracts; to overcome technological limitations and ensure trust, use quantum-resistant encryption methods and maintain cryptographic flexibility [7].

4. Customer trust: Communicate openly with customers about how their data is handled, who controls it and how it is used; involve customers in the process and be careful in choosing third-party operators to trust data.

5. Investment in talent and infrastructure: Invest in talent to develop and implement digital strategies such as AI-based monitoring and blockchain-enabled trust mechanisms; in addition, invest in infrastructure so that your organization has the necessary technology and systems to support digital trust.

Digital trust is a key aspect of modern business to build a strong foundation of trust. One of the possible ways to reduce risks and increase the confidence of buyers in online trade is the introduction of cyber security guarantees at the state level into the seller-buyer chain. The state, in cooperation with the private sector, forms an effective model of relations in the field of cyber security, based on trust, by implementing the following measures:

1) regulation at the legislative level of the issue of public-private partnership in the field of cyber security;

2) stimulation of the development of domestic software products, in particular open source software, which will be used as a priority for the processing and protection of state information resources, as well as at critical information infrastructure facilities;

3) implementation of the program for the development of the market of goods and services in the field of cyber security, which will include stimulation of its development and international recognition;

4) development of a system for evaluating the latest technologies that have a direct impact on the country's cyber resilience, creating tools (standards, protocols, certificates, etc.) for evaluating the effectiveness of using the latest technologies to combat cyber attacks;

5) introduction of pilot mentoring programs for improving the qualifications of specialists of state bodies that directly perform the functions of ensuring cyber security and cyber protection, by involving private sector specialists certified according to international standards;

6) promoting the implementation of a cyber security culture in business structures, which consists in constantly increasing the cyber awareness of their managers and employees;

7) mutual recognition of the results of cyber security compliance assessment and certification carried out by relevant bodies both in Ukraine and abroad;

8) implementation of a mechanism for assessing the losses of business entities as a result of cyber attacks for the possibility of their compensation and as an element of the further implementation of the cyber insurance system [8].

Thus, ensuring digital trust in international e-commerce with cyber security guarantees forms: trust in digital resources; development of information infrastructure; popularization and implementation of cyber security and cyber protection measures; the need to develop new national standards in the field of cyber security regarding the safety of the use of gadgets; electronic trust services based on a qualified website authentication certificate for the conclusion of purchase contracts; necessary prerequisites (normative, organizational, technological) for authentication of users of digital services using electronic identification technologies and/or electronic trust services; efficiency of the system of protection of personal data of citizens.

## REFERENCES


1. Cyber security Almanac 2022: 100 Facts, Figures, Predictions And Statistics. Cybersecurity Ventures. URL: https://cybersecurityventures.com/cybersecurity-almanac-2022/ (accessed 24.02.2024)

2. Five digital security trends in 2023. MEDIA-DK. URL: https://cutt.ly/3wNiXYGi (accessed 24.02.2024) (in Ukrainian)

3. Earning Digital Trust: Decision-Making for Trustworthy Technologies.World Economic Forum. URL: https://cutt.ly/AwNiXpco (accessed 24.02.2024)

4. What Is Digital Trust and Why Does It Matter for Business? Mapsted. URL: https://mapsted.com/blog/what-is-digital-trust (accessed 24.02.2024)

5. The road ahead for a trusted IOT. Digicert. URL: https://cutt.ly/LwNiXqJj (accessed 24.02.2024)

6. Guseva, O. Yu., Kazarova, I. O., Dumanska, I. Y., Gorodetskyy, M., Melnichuk, L. V., Saienko, V. H. Personal Data Protection Policy Impact on the Company Development. *WSEAS Transactions on Environment and Development*, 2022. Vol. 18, P. 232-246.

7. Dumanska, I., Vasylkivskyi, D., Hrytsyna, L., Khmelevskyi, O., Kharun, O. The Impact of Blockchain Technology on the Scenario Development of a Logistics Enterprise. *IJCSNS International Journal of Computer Science and Network Security*, 2022. Vol. 22. №. 11. P. 692-700.

8. The Cyber Security Strategy of Ukraine project (2021-2025). National Security Council of Ukraine. URL: https://cutt.ly/0wNiZPTI (accessed 24.02.2024) (in Ukrainian)



***Dumanska Ilona Yu.*** - Doctor of Economic Sciences, Professor, Professor at the International Economic Relations Department, e-mail: dumanskaiy@gmail.com.