

45. Vyshnevskiy, O. S. (2021). Digital platformization of strategic management of Ukrainian economy. *Econ. promisl.*, vol. 3(95), pp. 5-24. <http://doi.org/10.15407/econindustry2021.03.005>.
46. World Energy Outlook 2024. International Energy Agency, Paris.
47. Zhou, F. et al. (2024). Digital Twin-Enabled Smart Maritime Logistics Management in the Context of Industry 5.0. *IEEE Access*, vol. 12, pp. 10920-10931. <https://doi.org/10.1109/ACCESS.2024.3354838>.

Marta Danylovych-Kropyvnytska

ORCID: <https://orcid.org/0000-0003-3963-5524>

PhD in Economics, Associated Professor

Yurii Onyshko

ORCID: <https://orcid.org/0000-0003-4822-3510>

Master's Student in Public Administration

Lviv Polytechnic National University

(Lviv, Ukraine)

E-COMMERCE MARKET IN UKRAINE: CHALLENGES AND PROSPECTS

Abstract

Economic development of countries across the globe is determined by numerous factors, one of which is technological progress. It is technology, primarily Internet and subsequent globalisation, that has affected international trade. Since the early 1960s, businesses have been conducting electronic transactions via primitive computer networks. The birth of e-commerce (EC) is considered to be on 11 August 1994, when CDs were first sold on the US retail platform NetMarket. The e-commerce industry is growing globally and will mostly likely keep growing.

However, along with this development, Internet security has become an issue, i.e. personal data protection from unauthorised access and theft, integrity of business reputation, anti-fraud measures to prevent financial losses, compliance with data protection laws and regulations, and system resilience against cyberattacks. In today's digital world, data security is critical for stable operation of both private and corporate systems.

Keywords: *e-commerce, data security, digital market, data protection, cybersecurity, fraud.*

Modern technologies have transformed the Internet into a developed infrastructure that includes all major information centres, world libraries, databases of scientific and legal information, government and commercial organisations. Today, the Internet can be regarded as a huge market with the potential to reach almost the entire world's population. The rapid development of electronic communications and online advertising has led to revolutionary changes in commerce. The process of buying and selling through various electronic means of communication is called e-commerce.

The e-commerce market is a global platform where online trading transactions for the purchase and sale of goods and services take place. This market has been growing rapidly in recent years and is one of the most progressive and dynamic sectors of the global economy.

According to reports from research organisations, the e-commerce market has high growth forecasts. According to Research and Markets, the global e-commerce market reached a value of \$18.98 trillion in 2022. Its size is expected to increase to \$47.73 trillion by 2030, indicating an annual growth rate of 12.22% (Chevalier, 2023).

The term e-commerce emerged in the 1990s following the development of new software and technologies that transformed the Internet into a commercial environment. The new technologies allowed organizations to exchange information about products and services to influence consumers' purchasing decisions. The interconnectedness facilitated by the Internet allows consumers to engage in various activities online, creating a platform on which companies offer information about themselves and their products. However, with the development of technology, e-commerce has undergone some changes. Initially, companies used electronic technology to facilitate transactions, such as sending documents after an order, while modern e-commerce involves buying and selling goods online. E-commerce platforms are online platforms where consumers can browse and buy various products without visiting physical stores, making them cheap and convenient.

Compliance with data protection regulations is a must for e-

commerce companies operating globally. Privacy policies, including data protection and privacy measures, are increasingly becoming mandatory for companies, especially e-commerce stores. The specific rules for the collection, processing and storage of personal data of customers by businesses in the European Union are based on the General Data Protection Regulation (GDPR). It requires companies to obtain explicit consent from customers before collecting their data.

Given Ukraine's involvement in globalization, e-commerce has become one of the most promising business niches in Ukraine. According to EVO, one of Ukraine's largest product IT companies, the turnover of physical goods and services purchased online in Ukraine as of 2019 was UAH 76 billion, or 6.9% of total retail sales. However, comparing these volumes with global figures, it becomes clear that the Ukrainian e-commerce market is still in its infancy, but is extremely fast-growing. In particular, over the past six years, the average annual growth rate has been 24.7%. At the same time, the well-developed retail segment in Ukraine has maintained a growth rate of 3.9%. According to the State Statistics Service, the number of offline stores (retailers) has been steadily declining since 1990, with their number decreasing at an average annual rate of 3.8%.

The Ukrainian internet environment is showing huge annual growth, even exceeding the overall growth of the global market, but it still has many limitations that, if addressed, could open up even greater potential for expansion. The country's internet penetration rate reached 67% in 2019, while the average for Eastern Europe at the time was 71%. Meanwhile, Iceland, the country with the highest internet penetration, has almost reached full population coverage (99% in 2018). At the same time, the number of Internet users in Ukraine is growing rapidly, as evidenced by the 5.7% annual growth rate in 2019-2020, but the share of consumers who use the Internet and make online purchases is relatively small.

Ukraine is the 65th largest e-commerce market with revenue of USD 1.1 billion in 2021, ahead of Lithuania and behind Algeria. The classification of the main types of e-commerce in Ukraine is presented in Table 2.7.

The largest player in the Ukrainian e-commerce market is rozetka.com.ua. In 2021, the store's revenue was USD 246 million.

Rozetka.com.ua is followed by apple.com and makeup.com.ua as the second and third largest stores with USD 77 million and USD 46 million in revenue, respectively. Overall, the top three account for 35% of online revenue in Ukraine. Each of the segments is represented by an oligopolistic market model: each segment is controlled by several large firms, but there is a clear leader or group of leaders. Their pricing policy is usually a benchmark for smaller market participants, but not the ultimate limit, as small players are more flexible and have the potential to capture niches and gaps in large segments (Stan rynku e-commerce...).

E-commerce businesses collect and store huge amounts of personal and financial data from their customers. This data is vulnerable to hacking and cyberattacks, which can lead to fraudsters obtaining information and breaches of data protection regulations. Ensuring robust cybersecurity measures and compliance with data protection laws, such as the General Data Protection Regulation (GDPR) in the European Union, is crucial for e-commerce companies.

Potential data protection issues in the global e-commerce market include:

- ✓ The risk of data breaches: hackers can infiltrate e-commerce platforms and gain unauthorised access to customers' personal and financial information, which can lead to financial losses and undermine consumer confidence.

- ✓ Lack of adequate encryption measures to protect sensitive data in transit. If e-commerce platforms do not use strong encryption protocols, attackers can intercept and manipulate data, compromising customer privacy and security.

- ✓ Inadequate security measures: Many e-commerce platforms do not employ strong security measures to protect customer data. Weak passwords, outdated software, and a lack of regular security audits leave them vulnerable to attack.

- ✓ Lack of consumer awareness: Consumers often overlook the importance of reading privacy policies and terms of service before sharing their personal information online. This lack of awareness leaves them vulnerable to data misuse by e-commerce platforms.

Table 2.7

Types of e-commerce in Ukraine

Species	Characteristics	Representatives
E-commerce from business to consumer (B2C)	It involves the online sale of goods or services directly from businesses to individual consumers. It includes various online shopping platforms (online marketplaces, retailer websites and online classifieds).	Rozetka, Prom.ua, OLX
E-commerce for business (B2B)	It refers to online transactions that involve the exchange of goods, services or information between businesses through electronic platforms, allowing companies to optimise procurement processes, enter into contracts and collaborate with suppliers or partners online.	EVO
Consumer-to-consumer e-commerce (C2C)	It involves the sale of goods/services online between individual consumers using special platforms that connect buyers and sellers directly, without intermediaries. You can sell used items, offer services, or even rent real estate.	OLX
Online Marketplace	Online marketplaces are platforms that bring together many sellers and buyers, offering a wide range of goods and services in one place. They are intermediary platforms that provide an efficient environment for transactions.	Prom.ua, Rozetka, Zakupki.ua
Digital goods and services	It involves the online sale and distribution of digital products/services: buying and downloading software, e-books, music, films and online subscriptions.	Litres, Electronic Catalogue
Mobile commerce (M-commerce)	They are carried out via mobile devices (smartphones, tablets). Many of the EC platforms in Ukraine have developed mobile applications or optimised their web versions for mobile platforms.	

Source: compiled by the authors

✓ Cross-border data transfer: Global e-commerce involves the transfer of customer data between different jurisdictions. This poses certain challenges, as different countries may have different data protection laws and regulations. E-commerce companies must ensure compliance with these laws to protect customer data.

✓ Third-party sharing: E-commerce platforms often share customer data with third-party service providers for various purposes. However, a lack of transparency in this practice and insufficient safeguards to protect data shared with third parties can lead to unauthorised access or misuse.

✓ Unsecured payment systems: the use of unsecured payment systems can lead to potential theft or fraud of customer financial information. E-commerce platforms should implement secure payment gateways and adhere to industry standards to protect customer payment data (Socha & Lubowicka, 2023).

The anonymous nature of online transactions and the possibility of cross-border financial flows have made e-commerce an attractive route for money laundering. Criminals can use e-commerce platforms to disguise the illicit origin of funds through seemingly legitimate transactions. This problem requires robust anti-money laundering measures and cooperation between e-commerce companies, financial institutions and law enforcement agencies. Money laundering in the global e-commerce market poses several significant challenges. Historically, anti-money laundering efforts have focused primarily on the financial services sector, which is worth more than USD 400 trillion. However, the development of e-commerce has created new challenges. One of these challenges is the lack of personal contact and physical interaction with sales assistants that are typically present in traditional stores. The lack of face-to-face transactions makes it difficult to detect and prevent money-laundering activities (Straight, 2022).

The main threats that can lead to money laundering through the e-commerce market:

✓ Lack of strict customer verification processes: Many e-commerce platforms have weak customer verification procedures, allowing fraudsters to exploit the system and move illicit funds undetected.

✓ The use of cryptocurrencies for anonymous transactions:

Money launderers use the decentralised nature and anonymity of cryptocurrencies to hide their illegal activities, making it difficult to track and detect suspicious transactions.

- ✓ Weak anti-money laundering framework: The e-commerce industry lacks a comprehensive and standardised anti-money laundering framework, which hinders the effective prevention and detection of money laundering.

- ✓ Complex cross-border transactions: Global e-commerce involves cross-border transactions, which increases the complexity of monitoring and regulating financial flows. Money launderers take advantage of this complexity, making it difficult to trace the origin and destination of illicit funds.

- ✓ Use of third-party payment systems: money launderers often use third-party payment systems to transfer illicit proceeds through legitimate platforms, bypassing traditional banking channels and making suspicious activity more difficult to detect (Clean Money is a Click Away...).

Another major challenge in this market is online fraud, which is an ever-evolving threat as fraudsters develop new tactics and strategies to evade detection and circumvent security measures. This makes it a challenge for businesses and regulators to stay ahead of the latest threats and develop robust defences. The most common types of online and e-commerce fraud include:

- ✓ Phishing.

Phishing – fraudsters send emails or messages that look like they come from a legitimate company or organisation, such as a bank or online store, to trick consumers into handing over sensitive information such as passwords or credit card numbers.

- ✓ Identity theft.

Identity theft is when a fraudster steals someone's personal information, such as name, date of birth, social security number or driver's licence number, to impersonate that person and access their financial accounts or make fraudulent purchases.

- ✓ Credit card fraud.

Credit card fraud is where criminals use stolen or fake credit card information to make unauthorised purchases online.

- ✓ Account takeover fraud.

Account takeover fraud occurs when a fraudster gains access to

someone's online account, such as a bank account or email, by stealing login credentials through phishing or other methods.

✓ Chargeback fraud.

Chargeback fraud occurs when someone makes a purchase using a credit card, receives a product or service, and then disputes the charge with the credit card company, claiming that they never received the product or service or that it was defective, in order to get their money back. Unlike the friendly fraud described below, chargeback fraud involves an intentional act of fraud.

✓ Friendly fraud.

Friendly fraud occurs when a customer makes a legitimate purchase, but then disputes the charge to their credit card, claiming that the purchase was fraudulent. Sometimes this is done to avoid paying for the goods or to avoid the process of returning the goods or getting a refund.

North America and Europe are the regions most affected by online payment fraud, partly due to the widespread adoption of digital payment methods in these regions, as well as the developed technological infrastructure and high levels of online connectivity. The losses are expected to reach \$50bn and \$35bn by 2025, respectively.

In North America, the prevalence of online payment fraud is influenced by numerous factors, including the widespread use of credit and debit cards, as well as the growing popularity of mobile payments and e-commerce, as the region is home to many large financial institutions and technology companies that are attractive targets for cybercriminals.

Asia Pacific is the largest market for online payment fraud, with losses expected to reach \$54 billion by 2025 due to the rapid adoption of digital payment methods in the region and a large population that is increasingly connected to the internet.

Machine learning and artificial intelligence are increasingly being used to combat online fraud, with spending on these technologies expected to reach \$11.3 billion by 2025. These are two key tools in the fight against online fraud due to their ability to analyse large amounts of data and identify patterns and anomalies that traditional fraud detection methods may miss. Machine learning and artificial intelligence can be used to identify suspicious transactions, detect

anomalies in user behaviour, and analyse data from multiple sources to detect fraudulent activity in real time (Online and ecommerce fraud statistics...).

The e-commerce market is constantly evolving and changing, driven by new technologies, consumer behavior and global trends. Understanding these trends is essential for companies seeking to succeed in this space. According to the authors, the global trends affecting the EU market are:

- ✓ The development of e-commerce: more and more people are using mobile devices to shop online, which has led to the growth of the mobile segment of the e-commerce market, which is expected to reach 50% of all purchases in 2025.

- ✓ Personalization: Consumers want their shopping experience to be personalized, which has led to an increase in the use of artificial intelligence (AI) and machine learning (ML) to personalize product recommendations, marketing campaigns and other aspects of the experience.

- ✓ Social e-commerce: social media is becoming an increasingly important marketing and sales channel, with the social segment of the market expected to reach 30% of the global shopping market share.

- ✓ Growth of emerging markets: China, India and Southeast Asia are becoming increasingly important to the EU market, driving the growth of cross-border e-commerce and the popularity of local e-commerce platforms.

- ✓ Leapfrog in logistics and distribution: The popularity of express and same-day delivery has led to innovations in logistics and delivery, as well as the proliferation of last-mile delivery services.

- ✓ Increased focus on sustainability: Consumers are increasingly concerned about the environmental impact of their purchases, which has led to an increase in demand for eco-friendly e-commerce products and services.

- ✓ Growing popularity of alternative payment methods: Consumers are increasingly using alternative payment methods such as digital wallets and cryptocurrencies as safe and convenient methods of paying for EC.

Today, the Ukrainian Internet segment is growing in almost all areas. Our country's Internet economy is represented by the

computer and communications industries, the advertising and media industry, Internet services, and e-commerce.

Ukraine's e-commerce market has a huge potential for growth. However, there are a number of challenges and obstacles that need to be addressed in order to fully utilize this potential. The main challenges and obstacles hindering the development of the Ukrainian e-commerce market are as follows:

- ✓ Lack of trust and security: Building trust and ensuring security are major concerns for both consumers and businesses in the e-commerce sector. Many Ukrainian consumers are hesitant to make online purchases due to concerns about the security of personal and financial information.

- ✓ Inadequate logistics and delivery infrastructure: efficient and reliable logistics and delivery services are essential for the success of any e-commerce market. In Ukraine, there are problems with infrastructure, transport networks and last-mile delivery capabilities.

- ✓ Limited means of payment: the dominance of cash payments and limited adoption of digital payment methods in Ukraine pose challenges for online businesses. Encouraging the use of electronic payments and expanding the range of payment options could accelerate the development of the e-commerce market.

- ✓ Regulatory framework: the lack of comprehensive and clearly defined regulations on e-commerce creates uncertainty for businesses and consumers. A clear legal framework is needed to regulate online transactions, protect consumer rights and promote fair competition in the market.

- ✓ Limited digital skills and awareness: many citizens and businesses in Ukraine lack the digital skills and knowledge necessary to fully participate in online commerce. Promoting digital education and training programs can empower citizens and allow businesses to effectively tap into the potential of e-commerce.

Several strategies can be implemented to overcome these challenges and obstacles:

- A) Improving digital infrastructure: the government should invest in improving internet connectivity and providing broad access to high-speed internet throughout the country. This will allow more businesses and consumers to participate in the e-commerce market.

- B) Improving payment systems: steps should be taken to promote

digital payment methods, ensure transaction security and build trust between buyers and sellers. Collaboration with financial institutions and fintech companies can be helpful in this regard.

C) Promote consumer confidence and protection: implement measures to protect consumer rights, ensure the security of transactions, and promote transparent pricing and product information. This can be achieved by introducing and enforcing e-commerce rules and standards.

By seizing opportunities and addressing challenges, the Ukrainian e-commerce market has the potential to grow significantly in the coming years. Further efforts to improve infrastructure, increase trust and security, and support small businesses will be key to realizing this potential.

References:

1. *Stephanie Chevalier. Retail e-commerce sales worldwide from 2014 to 2027. Available at: <https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/> (accessed September 21, 2024).*
2. *Stan rynku e-commerce v Ukraini: Mykyta Artemchuk pro tendentsii, vyklyky ta tochky dlia rozvytku [The state of the e-commerce market in Ukraine: Mykyta Artemchuk on trends, challenges and points for development] Available at: <https://web-promo.ua/ua/blog/stan-rynku-e-commerce-v-ukrayini-mikita-artemchuk-pro-tendenciyyi-viklyki-ta-tochki-dlya-rozvytku/> (accessed October 13, 2024).*
3. *Paweł Socha, Karolina Lubowicka. Privacy compliance in ecommerce – a comprehensive guide. Available at: <https://piwik.pro/blog/privacy-compliance-in-ecommerce/> (accessed October 19, 2024).*
4. *Brian Straight. Money launderers find safe havens amid e-commerce boom. Available at: <https://www.freightwaves.com/news/money-launderers-find-safe-havens-amid-e-commerce-boom> (accessed August 20, 2024).*
5. *Clean Money is a Click Away: The Money Laundering Risks of E-Commerce. Available at: <https://www.protiviti.com/us-en/whitepaper/clean-money-click-away-money-laundering-risks-e-commerce> (accessed October 23, 2024).*
6. *Online and ecommerce fraud statistics that are predicting the future of fraud June 8, 2023 Available at: <https://stripe.com/resources/more/online-and-ecommerce-fraud-statistics#online-and-ecommerce-fraud-statistics> (accessed October 25, 2024).*