Volume 14 / **2026** ISSN 2344-102X
Issue **1** ISSN-L 2344-102X

CYBERSECURITY AND COMMUNICATIONS: MODERN REALITIES

Valeriia Peniuk
Chernivtsi Institute of Trade and Economics of State University of Trade and Economics, Ukraine
penyuk1992@gmail.com
ORCID: 0000-0002-7005-4173

Vasyl Havryliuk
Chernivtsi Institute of Trade and Economics of State University of Trade and Economics, Ukraine
margusha23@yahoo.com
ORCID: 0009-0006-6417-7683

Abstract
The article is devoted to the study that cybersecurity and effective communication have become critically important components of the security and stable functioning of not only governmental structures, but also of business, education, and everyday life. Cybersecurity and communication are closely interconnected, as any exchange of information through digital channels requires protection. Almost daily, companies interact with and attempt to better understand their consumers - learning their personal data, preferences, purchasing frequency, and more - thereby actively collecting personal information. This article explores the relevance of digital threats in the context of business-to-consumer communication. It highlights the specific nature of consumer trust in the digital environment and outlines the components that constitute trust in this space. The concept and prerequisites of cyber threats in the modern world are defined. The study demonstrates why cybersecurity forms the foundation of high-quality communication and long-term relationships with clients in a digital setting, and shows how it influences trust, loyalty, and the reputation of a brand or enterprise. The concept of a "bot farm" is described, and it is recognized as a significant and dangerous threat to modern consumer communications. The article provides examples of the types of information that must be protected when using various communication channels with consumers and clients, including email marketing, social media surveys, messaging platforms, data collection via websites, chatbots, and more. It is emphasized that effective communication - even in the digital realm - enables the formation of a valuable asset: client databases. The article underlines the importance of protecting these databases during the data collection process and argues that database formation is only the initial stage of ensuring digital security.

Key words: cybersecurity; communication; trust; consumer; digital environment

JEL Classification: *D83, L86, O33, K 24.*

Received on*:* 16 April 2026 **Accepted on:** 25 June 2026 **Released on:** 07 July 2026

INTRODUCTION

In the modern digital world, cybersecurity and effective communication have become critically important components of security and stable functioning of both state structures and business, education and everyday life. Cybersecurity and communications are closely related, because any exchange of information through digital channels requires protection.In addition to safeguarding information flows, cybersecurity ensures the reliability and resilience of communication infrastructures that support daily operations. As organizations increasingly rely on cloud platforms, remote working tools, and digital customer touchpoints, the potential surface for cyberattacks expands. This makes proactive risk assessment, continuous system monitoring, and quick incident response essential elements of modern digital management. When communication networks operate securely, organizations can maintain operational continuity and prevent disruptions that could harm financial performance or public confidence.

Moreover, strong cybersecurity measures directly influence the quality of interactions between enterprises and their audiences. Customers expect not only quick and convenient digital services but also full protection of their personal data throughout their online journey. Transparent data-handling policies, encrypted communication channels, and responsible use of digital technologies play a central role in maintaining long-term trust. Businesses that prioritize digital safety not only reduce vulnerability to threats but also enhance their reputation, strengthen customer loyalty, and create a competitive advantage in the increasingly interconnected marketplace.

I. LITERATURE REVIEW

The problems of cybersecurity management in the customer loyalty system were studied and several approaches were proposed to enhance the protection of digital interactions between enterprises and consumers. These proposals include the integration of advanced encryption mechanisms into loyalty platforms, the development of transparent data-

10.4316/EJAFB.2026.14112

Volume 14 / **2026** ISSN 2344-102X
Issue **1** ISSN-L 2344-102X

handling policies, and the adoption of unified standards for monitoring suspicious activity. Additionally, researchers emphasize the necessity of combining technological solutions with organizational measures, such as employee training and periodic security audits, to ensure sustainable protection and maintain customer trust. (Королюк & Чичун, 2023). Information security: organizational and legal frameworks are based on harmonizing regulatory and legal acts with the real challenges of the digital environment. It is important to create clear internal policies of enterprises that regulate access, use and protection of information resources. An effective system of organizational and legal support allows not only to minimize risks, but also to ensure the stability of the functioning of business and state institutions. (Кормич), 2004) developed threatening trends in the use of bot farms to the detriment of the state interests of Ukraine (Юшков, 2021), (Бурячок, et al., 2018) devoted their works to the socio-technical aspect of information and cybersecurity. However, the problem of forming a secure digital environment in the process of communication between a consumer/client and an enterprise that sells a product or service remains insufficiently studied.

II. METHODOLOGY

The purpose of the article is to determine the relationship between the concepts of cybersecurity and communication in the process of communication between a consumer/client and an enterprise that sells a product or service. To achieve this goal, the following tasks have been defined:

- to define the concept of trust in the process of communication between a consumer and an enterprise using digital tools and to determine its components;
- to prove why cybersecurity is the foundation of high-quality communication and long-term relationships with customers in the digital environment;
- to give examples of information that must be protected when using different types of channels of communication between a consumer/client and an enterprise that sells a product or service.

Presentation of the research material and its main results. The information needs of humanity today create a new cultural digital environment (Peniuk, 2023), where modern enterprises are actively resorting to changes and introducing new ways of contact with the consumer. Almost every day, companies contact and try to study their consumers, collect their personal data, study their preferences, frequency of purchases, etc., therefore they actively collect personal information of consumers. If the target audience is confident in the protection of information and personal data, this strengthens the feeling of "trust" in the product or service, and forms confidence in the quality of communications with it. According to the explanatory dictionary, "trust" is an attitude towards someone that arises on the basis of belief in someone's rightness, honesty, sincerity, etc. (Словник.ua, n.d.) From an economic perspective, Турчин, (2012) examines trust as a fundamental category that underpins economic relations and transactions. Кричевська, (2009).) defines trust as an attitude towards economic entities and institutions that expresses the degree of confidence in the compliance of their behavior with ideas about the image of this behavior without actualizing the bases of cost recovery and equivalence. Trust is defined as a subject-subject or subject-object relationship within an economic system based on the confidence that the other party will fulfill all the functions and obligations assigned to it, will act in accordance with certain established norms, and the result of such cooperation will bring some economic, social or moral effect for each of the parties.

If we take into account that the digital environment - an environment that encompasses information and communication technologies, including the Internet, mobile and related technologies and devices, as well as digital networks, databases, content and services, is used to interact with other users and access and publish created content (Меламедова, 2024), then we can make our own definition of the concept of consumer trust in the digital environment. Trust in the digital environment is the user's confidence in the reliability, honesty and predictability of the actions of other participants in digital interaction (in particular, online services, platforms, content and users), which is based on compliance with ethical norms, legal standards and technical security guarantees, and contributes to the formation of stable information, economic or social relations.

The components of trust security in the digital environment cover several key aspects that provide users with confidence in the reliability of interaction, the protection of their data and the integrity of participants in online communication (*Table 1*).

Table 1. The main components of trust in the digital environment

Parts	Description/Characteristics
Technical Security	• Data Protection: encryption, authentication, firewalls, antivirus. • Secure storage and transmission of information: use of HTTPS, VPN, trusted servers. • System updates and vulnerability fixes: regular maintenance.
Privacy and Confidentiality	• Privacy policies: transparently informing the user about data collection and use. • Control over personal data: the ability to adjust the level of openness of personal information. • User consent: use of personal data only after explicit permission.

10.4316/EJAFB.2026.14112

Volume 14 / **2026** ISSN 2344-102X
Issue **1** ISSN-L 2344-102X

Parts	Description/Characteristics
Legal and Ethical Reliability	• Compliance with legislation: compliance with the GDPR, the Ukrainian law "On the Protection of Personal Data" and other acts. • Compliance with ethical standards: honest communication, lack of manipulation, transparency in actions.
Transparency	• Access to information: clear explanation of terms of use, pricing policy, rights and responsibilities. • Openness to changes: informing users about changes in the policy or operation of the service.
Reliability and Reputation	• Reviews and ratings: social proof of trust from other users. • Reputation of the brand or platform: history of work, certifications, partnerships.
User Experience	• Clear interface: ease of use, accessibility of information. • User support: prompt technical assistance, support in resolving issues.

Source: authors based on Corewin (n.d.); Юшков (2021); Бурячок, et. al. (2018); Dumanska et. al (2022)

One of the main dangers in the digital space, what stops quality communication with consumers is cybersecurity (cyber threat) – one of the biggest problems that businesses face today (attacks on backup copies, denial of service, password hacking, use of mobile phone number, etc.). In European countries, over the past five years, the number of victims of cyberattacks has increased from 28% to 80%. That is why cybersecurity measures are being implemented – practical activities aimed at protecting computer systems, corporate networks and personal data from cyberattacks.

Cybersecurity covers the entire range of measures – from password management to security tools based on artificial intelligence and machine learning. Cybersecurity allows you to reliably protect transactions, view content and communicate safely online (Westelecom, n.d.). By adhering to a strict cybersecurity policy, any organization or institution can avoid data leaks, unauthorized access, and other serious threats.

Within just one month of the introduction of martial law, the number of cyberattacks on government institutions and businesses in Ukraine increased almost threefold compared to the same period in 2021, and as a result, enterprises were taught to respond to cyberthreats and introduce effective cyber protection tools into the enterprise management system (Королюк, & Чичун, 2023). According to the State Special Communications Service, most of these attacks were unsuccessful and did not cause damage to critical information infrastructure. Most often, hackers target state and local authorities, security and defense structures, private companies of various profiles, the financial sector, telecommunications infrastructure, IT companies, the media, as well as resources documenting Russian war crimes in Ukraine. In the first month and a half of the war, more than half of the cyber threats were attempts to collect data or distribute malware. According to a 2021 Microsoft report, Ukraine was one of the main targets of cyberattacks in the world - almost 20% of global threats were directed at it, second only to the United States (Kyivstar Hub, 2024). One of the large-scale cyberattacks on a large customer base was the cyberattack on Kyivstar in December 2023. As a result, about 24 million subscribers were left without communication, the network was completely turned off, and hackers managed to destroy 40% of the infrastructure. Although the company assures that there was no leakage of customer data, financial investments in the company's cybersecurity were still made.

No less important and dangerous threat to modern communications with consumers is the work of so-called "bot farms". As Юшков (2021) notes bot farms are companies that massively create fake social media users and write thousands of comments on their behalf. If we do not take into account global dangers at the country level, we can note that bot farms are often used in trade or services to increase the image and attractiveness of a company or product. They imitate likes on social networks, comment on the level of services provided or the quality of the product and promote their ideas to the masses. Therefore, consumers, in turn, either resort to such influence and make a purchase, or understand that it is worth trying another product and drawing their own conclusions. Such a practice reduces the level of trust in companies and worsens relations with consumers.

Cybersecurity is the foundation of quality communication and long-term customer relationships in the digital environment, as it directly affects trust, loyalty and reputation of the brand/company. Here's why:

1. Protection of personal data is the basis of trust. Customers provide companies with access to their personal data (contacts, payment details, purchase history, etc.). If this data falls into the hands of attackers through weaknesses in the system, it leads to loss of trust, customer churn and legal consequences. Reliable cybersecurity ensures that data is protected and the company is trustworthy.

2. Reputational stability. Even one data leak or cyberattack can cause enormous damage to the reputation of a business. Customers are reluctant to cooperate with those who cannot guarantee security. A systematic approach to cybersecurity builds a sustainable positive reputation of the brand as a reliable partner.

3. Increased loyalty. When users are confident in the security of the service, they are more likely to return, spend more, and recommend it to others. Loyalty is based not only on the product, but also on the feeling of security when interacting with the brand.

4. Competitive advantage. In a world where cyber threats are constantly growing, companies that invest in cybersecurity stand out from their competitors. Security becomes part of the value proposition and branding.

10.4316/EJAFB.2026.14112

Volume 14 / **2026** ISSN 2344-102X
Issue **1** ISSN-L 2344-102X

5. Compliance with legislation. Companies that comply with data protection requirements (GDPR, Ukrainian regulations, etc.) demonstrate their responsibility and respect for customer rights, which also helps to strengthen trust.

According to Чира (2023) today there are many options for promoting a product or service and/or communicating with a target audience. For example, sending information by e-mail, conducting surveys on social networks, messengers, collecting information on your own website, in chat bots, etc. Therefore, it is especially important to protect personal data and communication with consumers (Table 2).

Table 2. Examples of information that must be protected when using different types of communication channels

Communication channel	Usage example	What should be protected
Emails	Newsletter, order confirmation, customer support	- Customer addresses
		- Email content
		- Mail servers
Messengers (Viber, WhatsApp, Telegram)	Real-time customer communication	- Correspondence
		- Account access
		- Attachments and files
Phone calls	Hotline, consultations, support service	- Phone numbers
		- Call records
		- VoIP infrastructure
Online chats / chat bots	Live chat with a consultant on the website	- User data (TIN, addresses, requests)
		- Message history
		- Personal data
		- API connections to CRM or databases
Social Networks (Facebook, Instagram)	Messages, comments, advertising	- Account data
		- Messages
		- Photos
E-commerce platforms	Messages in user accounts	- Order data
		- Payment information
		- Purchase history
SMS and push notifications	Promotions, order notifications	- Phone numbers
		- Message content
		- Delivery channels
Video conferences (Zoom, Meet)	Online presentations, webinars, support	- Conference access
		- Recordings
		- Access links

Source: authors based on Corewin (n.d.), Юшков (2021), Бурячок, et. al. (2018), Dumanska et. al (2022)

In addition, in today's digital communications environment, companies should pay significant attention to building a comprehensive cyberthreat monitoring system that allows them to detect suspicious activity at an early stage. Tracking atypical user behavior patterns on social networks and on the company's web resources is especially relevant, which may indicate the intervention of botnets or automated scripts aimed at manipulating public opinion or discrediting the brand. Timely response to such manifestations helps not only prevent reputational losses but also increase the transparency and responsibility of digital interaction with consumers (Popelo et al., 2026).

An important aspect of ensuring cyber resilience is also the formation of a culture of digital hygiene among company employees. It is the human factor that often becomes the weakest link in the cyber defense system: using unreliable passwords, ignoring authentication rules, careless opening of phishing messages - all this creates opportunities for attackers. Regular training, internal audits, and cyberattack simulations can significantly reduce risks and create an environment where security becomes an integral part of the corporate culture. Ultimately, only a combination of technological tools, effective organizational policies, and conscious personnel behavior provides a solid foundation for long-term and secure customer relationships.

III. RESULTS AND DISCUSSION

The results of the study confirm that the formation of a secure digital environment during the interaction of the enterprise with the consumer is a key condition for the development of modern communication strategies. Analysis of threats arising in the process of digital communications showed that the most critical challenges today are personal data leaks, cyberattacks on communication platforms, manipulative activities of botnets, as well as a low level of digital literacy of both consumers and company employees. The complex of these factors significantly affects the level of trust in the brand and the effectiveness of marketing activities implemented in the digital environment.

10.4316/EJAFB.2026.14112

Volume 14 / **2026** ISSN 2344-102X
Issue **1** ISSN-L 2344-102X

The study found that consumers are increasingly evaluating the quality of interaction with the brand not only by the functionality of the product or service, but also by the level of protection of their personal data. This allows us to assert that cybersecurity is becoming one of the defining criteria for the competitiveness of the enterprise. Companies that systematically implement information protection policies, use modern encryption protocols and demonstrate transparency in working with data have a much higher chance of forming long-term and mutually beneficial relationships with their customers.

An important result was the discovery of a direct connection between the reputational stability of the enterprise and its ability to provide reliable information protection. Companies that have at least once become victims of public data leaks or manipulations by bot farms face long-term consequences: reduced loyalty, a drop in sales, a negative information background and an increase in the cost of restoring trust. At the same time, companies that effectively communicate their cyber protection measures demonstrate more stable indicators of interaction with consumers and enjoy higher reputational support. Analysis of the activities of botnets has shown that their influence goes far beyond political or social manipulation. In the business world, bot farms are increasingly used to create a positive or negative image of a company. The mass layering of fake comments, artificially inflated “likes” or views create a misleading impression of the quality of goods or services. In the long term, such practices undermine the overall level of trust in digital platforms, as consumers begin to doubt the reliability of any content, which, in turn, negatively affects all market participants.

The results also showed that effective cybersecurity management is possible only if technical, organizational and behavioral measures are combined. Technical solutions ensure infrastructure protection, organizational policies define rules and procedures for working with information, and personnel training forms a security culture that prevents the most common human errors. Companies that implement a comprehensive approach demonstrate higher resilience to cyber threats and the ability to adapt to a rapidly changing digital environment. However, as Corewin (n.d.) notes, overly strict security measures can frustrate users and lead to unsafe practices.

Thus, the results of the study confirm: the security of communications in the digital space is a fundamental condition for building trust, loyalty and a positive reputation of the enterprise. In modern conditions, it is no longer enough to offer a quality product - it is necessary to ensure reliable and transparent digital interaction, which guarantees the protection of each stage of communication with the consumer.

IV. CONCLUSION

Thus, effective communication, even in the digital world, provides an opportunity to form a certain asset - customer databases that store critical information: personal data of users, transaction histories, logistical operations, business analytics, etc. They are not only a source of operational efficiency, but also the basis for building trust between the company and customers, partners, and society at large. Database security encompasses measures, tools, and policies to protect databases from unauthorized user access, misuse, theft, or loss. This includes controlling access to the database, protecting data within the database, and protecting data during its movement or access. Effective database security standards protect the organization's valuable information assets, which, in turn, helps maintain customer trust and avoid financial and reputational losses caused by data leaks. However, enterprises need to remember that measures aimed at maximizing data security often disappoint users and hinder their productivity. This can lead to users bypassing security measures, which can ultimately compromise security. For example, requiring complex and frequently changed passwords helps protect accounts from compromise, but it can also frustrate users, leading to unsafe practices such as password reuse or writing them down. To avoid these problems, organizations need to balance database security measures with the impact on user interactions.

If a company chooses digital channels to promote its products, ensuring the cybersecurity of communications with consumers should be an important strategic component of its activities. Forming and filling customer databases is only the initial stage of digital security. Much more critical is the continuous monitoring of the state of the information system and taking measures to prevent the leakage of confidential data. In today's conditions, this is one of the key priorities for business management, which seeks to maintain consumer trust, ensure the stability of business processes, and meet the requirements of the digital age.

REFERENCES

1. Corewin. (n.d.). 13 найкращих практик для безпеки баз даних. CoreWin Blog.. Retrieved from: https://corewin.ua/blog/what-is-database-security/ (accessed 27.10.2025) (in Ukrainian).
2. Dumanska, I., Vasylkivskyi, D., Hrytsyna, L., Khmelevskyi, O. & Kharun, O. (2022). The Impact of Blockchain Technology on the Scenario Development of a Logistics Enterprise. IJCSNS International Journal of Computer Science and Network Security,.22 (11), 692-700. Retrieved from: https://elar.khmnu.edu.ua/server/api/core/bitstreams/dd08c115-d1ae-4d64-851a-237d936dbaec/content
3. Peniuk, V. O. (2023). Vplyv internet-tekhnolohii na komunikatyvnu kulturu suspilstva. *Mizhnarodnyi naukovyi zhurnal "Internauka", Seriia: "Ekonomichni nauky"*, 6 https://doi.org/10.25313/2520-2294-2023-6-8979 (in Ukrainian).
4. Popelo, O., Zhavoronok, A., & Cosmulese, C. G. (2026). Trends in the financial and digital space. Socio-economic relations in the digital society, 2(60), 74-84. https://doi.org/10.55643/ser.2.60.2026.649
5. Westelecom. (n.d.). Основи кібербезпеки для бізнесу. Retrieved October 25, 2025, from https://westelecom.ua/blog/osnovy-kiberbezopasnosti-dla-biznesa

10.4316/EJAFB.2026.14112

Volume 14 / **2026** ISSN 2344-102X
Issue **1** ISSN-L 2344-102X

6. Бурячок, В. Л., Толубко, В. Б., Хорошко, В. О., & Толюпа, С. В. (2018). Інформаційна та кібербезпека: соціотехнічний аспект: підручник. Львів. https://spadok.org.ua/books/Buryachok-Osnovy-info-ta-ciberbezpeky.pdf
7. Кормич, Б. А. (2004). Інформаційна безпека: організаційно-правові основи. Київ: Кондор.. http://doi.org/10.34025/2310-8185-2023-4.92.03
8. Королюк, Ю. Г., & Чичун, В. А. (2023). Менеджмент кібербезпеки в системі лояльності покупців. Вісник Чернівецького торговельно-економічного інституту. Економічні науки, 4(92), 39–53. https://doi.org/10.34025/2310-8185-2023-4.92.03
9. Кричевська, Т. О. (2009). Логіко-історичний аналіз довіри в контексті соціально-економічних відносин. , ПОЛІТЕКОНОМІЯ, 330.1, 5-18 Retrieved from: https://etet.org.ua/docs/ET_09_3_05_uk.pdf (accessed 01.11.2025) (in Ukrainian).
10. Кричевська, Т. О. (2009). Логіко-історичний аналіз довіри в контексті соціально-економічних відносин. *Економічна теорія*, (3), 5–18.
11. Меламедова, О. О. (2024). Цифрове освітнє середовище педагога НУШ (теоретичний кейс, математична галузь). Vseosvita. https://vseosvita.ua/library/tsyfrove-osvitnie-seredovyshche-pedahoha-nush-teoretychnyi-keis-matematychna-haluz-825681.html
12. Словник.ua. (n.d.). *Довіра*. https://slovnyk.ua/index.php?swrd=довір'я
13. Турчин, Л. Є. (2012). Сутність поняття «довіра» як економічної категорії. Ефективна економіка, (5). http://www.economy.nayka.com.ua/?op=1&z=1173
14. Чирак, І. М. (2023). *Економіка соціальних медіа: навчальний посібник*. Тернопіль: ЗУНУ. http://dspace.wunu.edu.ua/handle/316497
15. Юшков, А. Г. (2021). Загрозливі тенденції використання ботоферм на шкоду державним інтересам України: механізми запобігання та протидії. Інформація і право, 3(38), 90–98. https://doi.org/10.37750/2616-6798.2021.3(38).243812

10.4316/EJAFB.2026.14112