МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВІННИЦЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЕКОНОМІКИ
ВСП «ВІННИЦЬКИЙ ФАХОВИЙ КОЛЕДЖ ЕКОНОМІКИ ТА ПІДПРИЄМНИЦТВА ЗУНУ»

АКТУАЛЬНІ ПИТАННЯ РОЗВИТКУ НАУКИ, ЕКОНОМІКИ ТА СОЦІУМУ В УМОВАХ ВІЙНИ ТА ПОВОЄННОГО ВІДНОВЛЕННЯ

МАТЕРІАЛИ ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

м. Вінниця, 16-17жовтня 2025 року

ТОМ І
Частина І

Вінниця – 2025

INTEGRATION OF INFORMATION TECHNOLOGIES INTO THE SYSTEM OF DIGITAL MANAGEMENT AS A FACTOR IN ENHANCING THE EFFICIENCY OF THE NATIONAL ECONOMY

Inna Sysoieva,
Doctor of Economics, Professor
Vinnytsia Educational and Scientific Institute of Economics
West Ukrainian National University
Oleh Pohrishchuk,
PhD in Economics, Associate Professor
Vinnytsia Educational and Scientific Institute of Economics
West Ukrainian National University

Today, the world is at the epicenter of a large-scale digital transformation that is radically reshaping the nature of economic activity and management approaches. Information technologies (IT) have evolved from tools of technical optimization into a key factor of enterprise competitiveness, prompting organizations to rethink traditional business models and develop modern digital management strategies. The implementation of technological innovations in management systems not only automates routine operations but also enhances the quality of managerial decision-making, accelerates business processes, and minimizes potential risks. During 2000-2024, cyber threats have undergone significant evolution – from widespread virus attacks to sophisticated, targeted incidents that increasingly employ artificial intelligence, phishing, social engineering, and cryptographic fraud (Fig.1). In the early 2000s, DDoS attacks, trojans, and financial fraud were the most prevalent types, whereas between 2011 and 2015, cyberattacks became more personalized and primarily targeted corporate networks. The period of 2016-2020 was marked by the massive spread of ransomware and a surge in cyber espionage, resulting in multibillion-dollar financial losses worldwide. Since 2021, cybercriminals have increasingly utilized neural networks and deepfake technologies, making attacks more advanced, automated, and difficult to detect. The widespread use of Internet of Things (IoT) devices and cloud technologies has significantly expanded the attack surface, while the number of DDoS incidents has grown by almost 40%. In the near future, quantum computing, AI-based cybersecurity systems, and stricter regulatory frameworks are expected to play a crucial role in combating digital threats. Thus, an

effective cybersecurity strategy should be built upon a multi-layered defense system, automated threat detection tools, and adaptive data recovery mechanisms, enabling enterprises and government institutions to reduce digital risks and protect critical infrastructure [1].

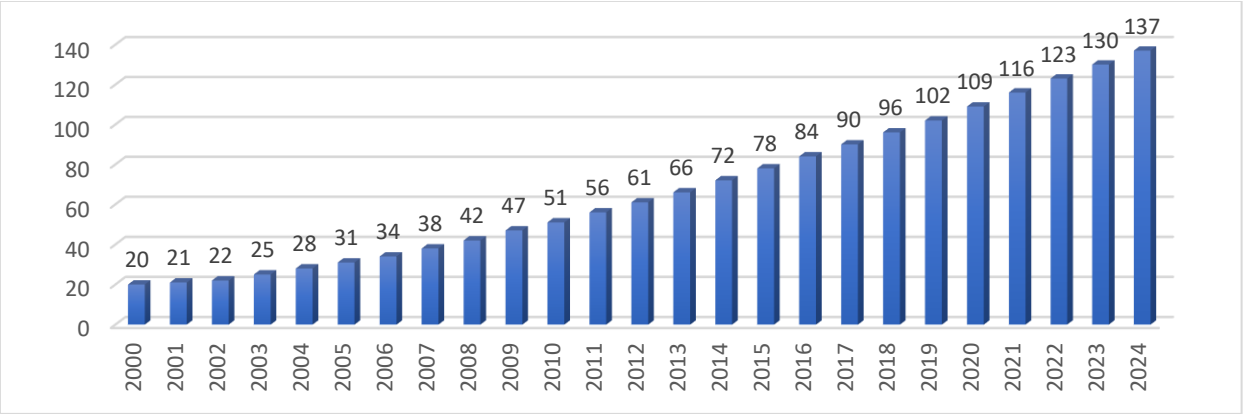

Fig. 1. Dynamics of the growth of cyber threats (2000-2024)

Constructed using the source [2**]**

In 2024, cybersecurity has become one of the key tools in countering digital threats, as the number and complexity of cyberattacks continue to increase (Fig. 2). Businesses and government institutions are actively implementing multi-factor authentication (MFA), encryption, AI-powered threat detection systems, and regular security audits to protect sensitive data. Research shows that encryption reduces the risk of data breaches by 85%, MFA decreases unauthorized access incidents by 75%, and audits improve threat detection efficiency by 70%. The use of artificial intelligence and machine learning enables real-time monitoring and predictive threat detection, while the integration of firewalls, IDS systems, and cloud-based solutions enhances protection and reduces the number of successful attacks. However, cybercriminals continue to refine their methods– using deepfake scams, AI-driven phishing attacks, and potentially dangerous quantum technologies. Therefore, an effective security strategy must combine multi-layered protection, intelligent threat detection systems, and continuous employee training. In the future, the main directions of cybersecurity development will include zero-trust architecture, biometric authentication, and quantum-resistant encryption, which will ensure a higher level of resilience to digital

risks.

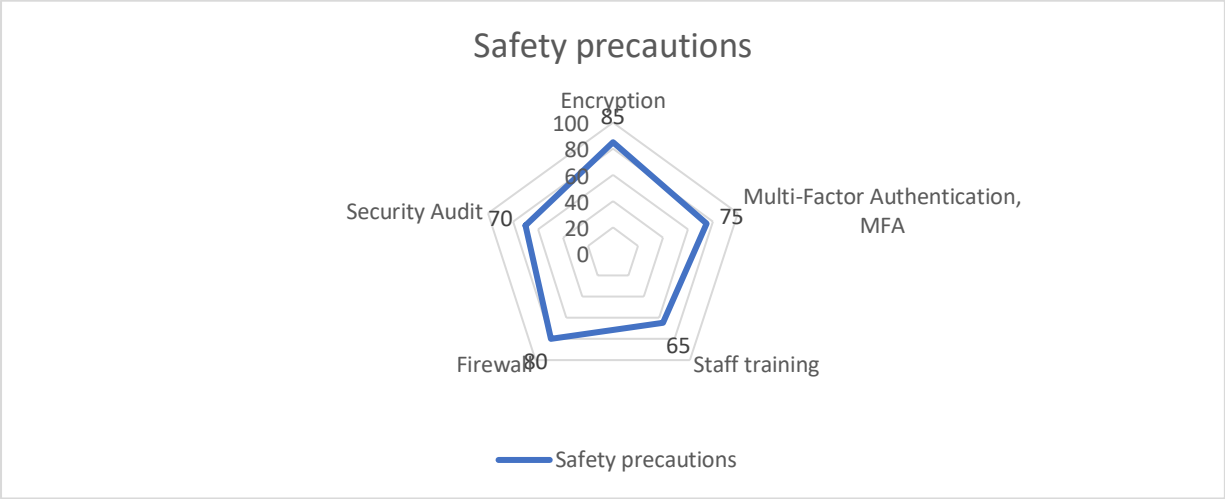

Fig. 2. The impact of cybersecurity measures on reducing attacks (2024)
Constructed using the source [2]

Figure 3 illustrates the growing number of cyberattacks in Ukraine, showing a steady rise in digital threats in recent years. This upward trend is driven by geopolitical tensions, the rapid expansion of digital infrastructure, and increasingly sophisticated cybercriminal tactics. The main attack types include DDoS, phishing, ransomware, and state-sponsored cyber espionage, targeting both public and private sectors. The escalation of cyber threats underscores the urgent need for stronger protection measures such as multi-factor authentication (MFA), AI-based threat detection, and advanced data encryption. In response, Ukraine is enhancing cybersecurity through public–private cooperation, alignment with international standards, and the implementation of proactive defense strategies.

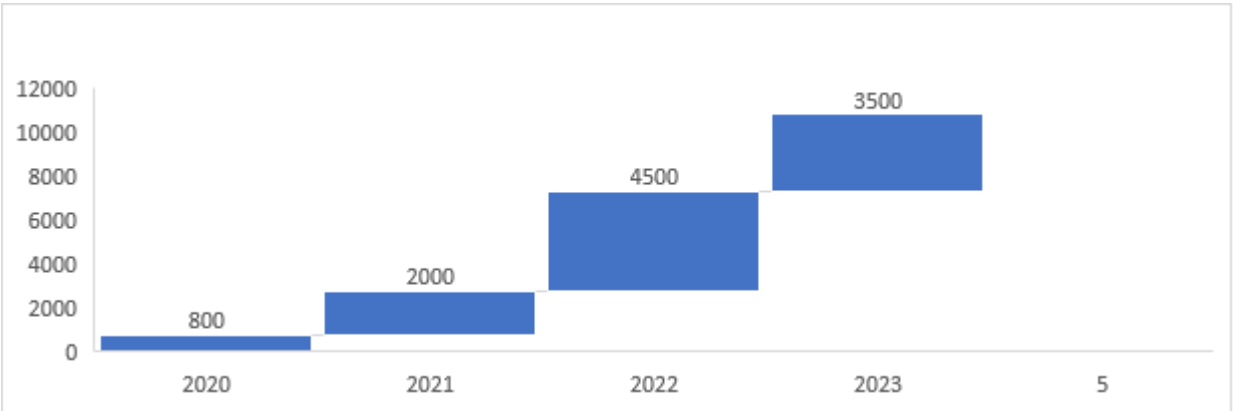

Fig.3. Number of cyberattacks in Ukraine

Constructed using the source [2]

Future trends point toward zero-trust security models, quantum encryption, and real-time monitoring systems, which will be key to improving resilience against emerging digital threats. Figure 4 shows the distribution of cyberattacks by type in 2023. The majority of incidents were ransomware attacks (40%), which encrypt data and demand payment for decryption. Phishing accounted for 30%**,** using social engineering to steal confidential information. DDoS attacks represented about 20%**,** overwhelming servers and disrupting online services. The remaining 10% consisted of spyware and IoT-related attacks, which threaten network integrity and data privacy.

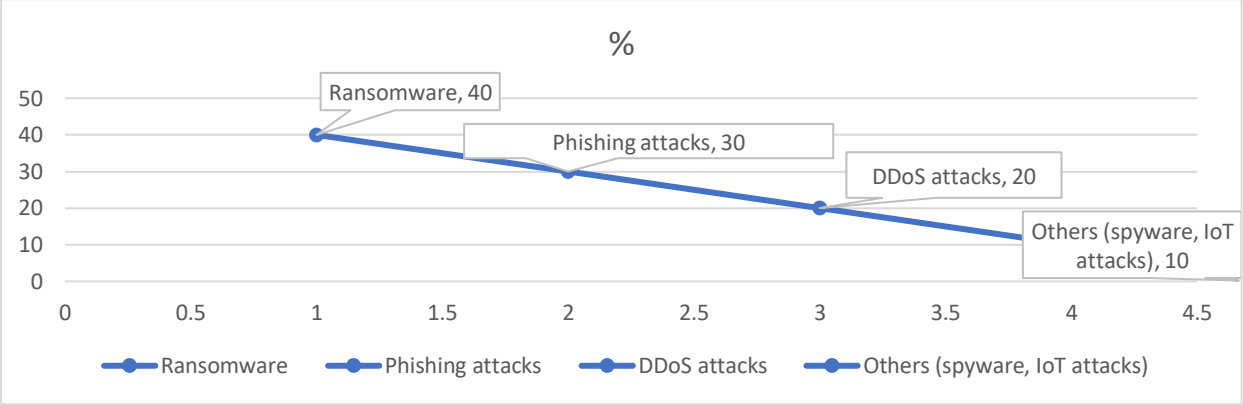

Fig.4. The share of different types of cyberattacks in the total number of incidents in 2023
Constructed using the source [3]

The study confirms that information technology (IT) is a key driver of business management efficiency, enabling process automation, cost reduction, and better strategic decisions. After IT implementation, labor productivity grows by about 50%, and data processing time decreases by 60%, proving the crucial impact of digital tools.

Major management risks include cybersecurity threats (40%), data leaks (25%), outdated software (15%), and human errors (10%). Effective mitigation requires multi-layer protection, data encryption, network monitoring, and digital literacy training.

The introduction of ERP, CRM, AI, and analytics systems enhances resource use, decision-making, and customer engagement. Future trends focus on quantum computing, AR/VR technologies, and advanced AI algorithms for predictive management.Thus, the synergy of digital technologies and strategic management

determines business competitiveness today. Sustainable digital transformation depends on innovation adoption, digital culture development, and strong cybersecurity.

References:

1. Sysoieva I., Pukas A., Pohrishchuk O., Pohrishchuk B., Tsikhanovska O., Lyzun M. *Artificial Intelligence as an Organized Assembly of Information Technologies for the Goals of Sustainable Development.* // *14th International Conference on Advanced Computer Information Technologies (ACIT)*. – Ceske Budejovice, Czech Republic, 2024. – С. 259–263. – DOI: 10.1109/ACIT62333.2024.10712621.
2. Oberig IT. *Trends in cybersecurity in 2023 and year review.* – 2023. – Режим доступу: https://oberig-it.com/statti/tendencziyi-kiberbezpeky-u-2023-roczi-ta-oglyad-roku/. – Дата звернення: 06.10.2025.

3 H-X Technology. *Cyber Threats Forecast 2024.* – 2024. – Режим доступу: https://www.h-x.technology/ua/blog-ua/cyber-threats-forecast-2024-ua. – Дата звернення: 06.10.2025.