Key Findings:

1. Economic Growth: Digital transformation leads to increased efficiency and productivity in many industries. It enables businesses to reach global markets and innovate their products and services.

2. Changing Work Environment: The rise of remote work and digital communication tools is changing how people collaborate. This shift offers flexibility but also presents challenges in maintaining work-life balance.

3. Cultural Shifts: Digital platforms influence cultural exchange and social interactions. While they promote global connectivity, they can also lead to cultural homogenization and the loss of local identities.

4. Inequality Issues: Access to digital technologies is not uniform across regions. This disparity can widen the gap between different socioeconomic groups, making it crucial to address issues of digital inclusion.

In conclusion, digital transformation is reshaping the world in profound ways. Understanding its economic and socio-cultural impacts is essential for navigating the future effectively. This research highlights the need for policies that promote equitable access to digital resources and support sustainable development in the digital age.

V. Fidyukovich
В.А. Фидюкович
БГЭУ (Минск)
Научный руководитель Я.И. Шавярновская

PROBLEMS OF THE DIGITAL AGE: CYBER DANGER

Проблемы цифровой эпохи: кибер опасность

The purpose of this article is to inform and warn about the cyber threats that companies will face in 2024 due to the shift to remote work and the growing influence of artificial intelligence (AI). The shift to online communications and digital working methods, on the one hand, provides convenience and flexibility, but on the other, it creates conditions for new types of fraud and attacks. This article details how such threats can undermine the security and reputation of companies and what measures can and should be taken. Examples of threats are given, such as deepfakes, which create fake images and voices of employees and allow fraudsters to deceive company executives. It also looks at how AI expands the ability to create and adapt malware and bypass defenses.

The analysis points to the following main threats that enterprises are facing now and will face in the future:

- Cyberattacks using artificial intelligence: AI can create high-quality deepfakes and develop malware that bypasses existing defenses. Organizations are faced with the challenge of countering such sophisticated attacks and detecting fake images and sounds in a timely manner.

- Cloud security breaches: Cloud usage has become widespread, but the risk of unauthorized access to data has also increased. If an attacker gains access to cloud storage, this can lead to the leakage of critical information and, as a result, damage to the company's reputation.
- Ransomware (RaaS): Fraudsters encrypt company data and demand a ransom to unlock it, causing significant financial damage and slowing down the company.
- Supply chain attacks: Attackers target a company's third-party suppliers to gain access to critical systems and data. This is especially important for companies operating in a partner network, as a vulnerability in a supplier can put the entire supply chain at risk.
- Internet of Things (IoT) security threats: In the 5G era, the number of devices connected to the internet increases, which means the attack surface increases. It is important to consider that vulnerable IoT devices can become access points for attackers, potentially compromising a company's critical infrastructure.
- Insider threat: With the rise of remote work, companies are faced with the challenge of monitoring employees outside the office.

The study highlights the need for a comprehensive security approach to help companies protect against these threats. Recommended measures include:

- Implementing multi-factor authentication (MFA) to strengthen account security;
- Regularly updating software to prevent exploitation of vulnerabilities;
- Investing in up-to-date security systems such as antivirus and firewalls;
- Training employees in cybersecurity practices and developing policies to remind them to be careful when using data;
- Continuously monitoring networks and systems to quickly detect suspicious activity.

The article highlights that strengthening security concerns not only the IT sector, but also companies from other industries, as cybersecurity threats are beginning to affect all aspects of social and economic life. It is important to understand that cyber threats are constantly evolving, so it is important to take action today to avoid fraud and losses in the future.

Y. Khlebnikov
Я.А. Хлебников
БГТК (Борисов)
Научный руководитель Е.Л. Потемкина

DIGITAL ECONOMY IN THE REPUBLIC OF BELARUS

Цифровая экономика в Республике Беларусь

The digital economy is based on the use of digital technologies, data, and platforms that create new products, services, and business models. It encompasses not only information and communication technologies but also other industries that apply digital solutions to enhance competitiveness and quality. Key trends include the growth of data