The achievement of these criteria is possible provided the timely development of science-based economic activities within the industrial sector, i.e. technologies V and VI technological orders. With a view to implement the tasks set out in the Republic of Belarus, a number of normative and legal documents have been developed, the main ones of which are presented below:

1. Decree 381 «On digital development» of November 29, 2023;
2. Decree 40 «On cybersecurity» of 14 February 14, 2023.
3. State program «Digital development of Belarus» for 2021–2025.

1. Moving from the fourth to the fifth industrial revolution involves integrating people and machines, shifting the focus from technological progress to the social aspect of a company's activities. At this point the employees of organizations become an «investment» asset, in this case, there is a win-win strategy: by investing in the skills of the organization's staff, companies achieve their own purposes. In Industry 5.0 cyber-physical systems play a central role, so the transformation affects them too: they combine computing resources with physical objects, but with the addition of human factor, becoming cyber-social systems.

2. The Republic of Belarus has an exhaustive potential for realizing the prospects of Industry 5.0 in the future, which is justified by the combination of significant support from the state, development of human resources and specialization of Belarusian industry in industries with a developed manufacturing base. Implementation of cyber-physical systems will make the Republic of Belarus a global economic competitor, especially in terms of intelligent resource management for the development of innovative high value-added products and services using cyber-physics systems.

3. As a result of work, the following conclusions can be made: Industry 5.0 would allow to solve a number of problems that arose within the framework of Industry 4.0, due to fundamental differences, which are based on humanization of companies' activities and sustainable development.

M. Muslivchik
М. А. Мусливчик
БГТУ (Минск)
Научный руководитель К. Ф. Михасенко

DIGITAL PRIVACY AND DATA SECURITY IN THE INFORMATION AGE

Цифровая конфиденциальность и безопасность данных в информационную эпоху

In the modern world, internet access has become an integral part of daily life for the majority of the population. We use social networks, make online purchases, store personal photos in the cloud, and communicate through messengers. Yet, do we fully comprehend the associated dangers of the digital realm?

A prime example is the cookie consent banner that appears upon visiting a website. We mechanically click the «Accept» button without considering where our data goes and for what purpose. This raises a critical question: what portion of our lives remains outside the internet's reach, and how much does it already know about us?

The aim of this work is to encourage individuals to reflect on the protection of their personal data online and to propose straightforward and effective methods for digital self-defense.

Digital Privacy is a human right to control the collection, storage, and use of one's personal data. This includes not only obvious information such as passport details, medical records, and banking information but also browser history, messenger conversations, and even behavioral patterns (e.g., time spent online or frequency of website visits).

Data Security, in contrast, constitutes a set of measures designed to protect this data throughout its entire lifecycle, preventing its loss and unauthorized use.

Many users operate under the assumption that they have «nothing worth stealing». However, even basic data – name, email address, date of birth – can be leveraged by malicious actors. This information can be used to create a highly accurate psychological and behavioral profile of an individual, which can then be exploited for targeted advertising and fraudulent activities.

Furthermore, no one is immune to data breaches. In such events, if you reuse the same password across multiple services, attackers can gain access to your other accounts simply by matching the compromised email and password combination.

The volume and sophistication of cyberattacks grow daily, affecting even large corporations and government institutions. While achieving complete protection is nearly impossible, anyone can significantly mitigate these risks by adhering to several fundamental principles:

1. Scrutinize Terms of Service and Privacy Policies. Make an effort to understand what data a website or application requests and for what specific purpose.

2. Utilize Partial Consent and Configure Privacy Settings. Do not grant a website or application unnecessary access to your contacts, camera, or geolocation. Enable only the permissions that are strictly necessary for its core functionality.

3. Create Temporary and Anonymous Accounts. Use these for registration on platforms that you do not intend to use on a long-term basis.

4. Employ Strong and Unique Passwords. These should be complex, incorporating numbers, symbols, and a mix of upper- and lower-case letters. For convenient management, it is highly recommended to use a secure password manager.

5. Enable Two-Factor Authentication (2FA) on all critical services (e.g., email, social networks, banking platforms). This can protect your account from being compromised even if your password is leaked.

In conclusion, digital privacy and data security are not merely IT concepts but are essential tools for safeguarding the personal lives of every modern individual. Every online action carries potential consequences. Therefore, it is imperative to develop digital literacy, adopt a conscious approach to technology use, and remember: your data is your

asset. Maintaining vigilance will ensure that your life online becomes not only more comfortable but also significantly more secure.

References

1. Azure Data Security and Encryption Best Practices // Microsoft Learn. – URL: https://learn.microsoft.com/en-us/azure/security/fundamentals/data-encryption-best-practices (date of access: 22.10.2025).

2. 10 Data Security Best Practices in 2025 // GeeksforGeeks. – URL: https://www.geeksforgeeks.org/data-security-best-practices/ (date of access: 01.11.2025).

A. Nevdakh
А. С. Невдах
БГЭУ (Минск)
Научный руководитель Н. А. Михайлова

SAFEGUARDING PERSONAL DATA OF STUDENTS AND TEACHERS IN THE DIGITAL EDUCATIONAL ENVIRONMENT USING THE EXAMPLE OF THE REPUBLIC OF BELARUS

Защита персональных данных студентов и преподавателей в цифровой образовательной среде на примере Республики Беларусь

The purpose of this study is to analyse legal and organizational mechanisms for personal data protection in the educational environment of the Republic of Belarus, assess their effectiveness in practice and identify possible problem areas in the context of active digitalisation of education.

Digital technologies have changed the way we study and teach. Today, students and teachers use online platforms, electronic journals, and video lessons every day. These tools make education more flexible and accessible. However, they also create new risks. Personal data: names, grades, and health information can be stolen or misused. That is why it is very important to protect this data. In Belarus, schools and universities must follow special laws to keep personal information safe and respect the rights of students and teachers.

The Law of the Republic of Belarus from May 7, 2021, No. 99-Z «On Personal Data Protection» is the main law that controls how personal data is protected. According to Article 4, personal data can only be used if the person agrees, unless the law says otherwise. Special types of personal data: health details, biometric data, and information about someone's marital status – are protected even more strictly.

In Belarus, the National Center for Personal Data Protection (NCPD) is responsible for protecting personal data. NCPD checks if the laws are followed, carries out inspections, and gives clear explanations and ready-made solutions for different areas,