3. Постановление Совета Министров Республики Беларусь 2 февраля 2021 г. № 66 о Государственной программе «Цифровое развитие Беларуси» на 2021–2025 годы [Электронный ресурс]. – Режим доступа: https:// pravo.by/ – Дата доступа 14.10.2024.

4. Парк высоких технологий сегодня [Электронный ресурс]. – Режим доступа: https://www.park.by/ – Дата доступа 14.10.2024.

5. Переход экономики в цифровой формат в Беларуси [Электронный ресурс]. – Режим доступа: https://edn.by/ – Дата доступа 14.10.2024.

A.A. Lebedeva, S.A. Slassi Moutabir
Belarusian National Technical University
Minsk, Belarus

CYBERSECURITY BASICS

Abstract. In our modern world, information is a rather valuable resource, which makes us think about protecting it. Cybersecurity is a critical area for protecting information and data on the Internet. A successful cyberattack can result in the irretrievable loss or modification of important data, thus making it of great importance to follow the cybersecurity regulations.

А.А. Лебедева, С.А. Сласси Мутабир
Белорусский национальный технический университет
Минск, Беларусь

ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

Аннотация. В нашем современном мире информация является довольно ценным ресурсом, что заставляет нас задуматься о ее защите. Кибербезопасность – важнейшая область защиты информации и данных в Интернете. Успешная кибератака может привести к безвозвратной потере или изменению важных данных, поэтому важно соблюдать основные правила кибербезопасности.

In the modern world, where digital technologies are rapidly developing, when an increasing amount of personal and corporate information is stored and transmitted electronically, data protection issues are becoming more relevant than ever.

Cybersecurity is actions that help protect computers, networks, and

data from unauthorized access, use, destruction, alteration, or disclosure. It should be understood that there is a similar in meaning definition — information security. Information security refers to the protection of data from various threats, regardless of whether they are conventional or electronic [1].

We need cybersecurity to protect our personal and work information, as well as so that we can safely use the Internet and not worry about it. Protection includes risk management, compliance with laws, and reducing the chances of possible attacks.

The significance of cybersecurity tends out to be of high importance. First of all, it is worth noting that every year there is an increase in the number of cyberattacks, and their complexity is constantly increasing. Hackers use a variety of methods, ranging from phishing and viruses to complex attacks, such as DDoS (distributed denial of service) [4]. They usually use them to gain access to protected information. With regard to lost data, leakage or loss of information can have serious consequences for both organizations and individuals, including financial losses, reputational damage and legal problems.

Let's take a closer look at the most basic types of cyberattacks. Firstly, I would like to highlight phishing. In this case, users may receive a message or a link to a site already with a virus that is able to see your saved passwords or other important data. The bottom line is that the attacker pretends to be a trusted and reliable person. Phishing also happens in the form of a phone call where a thief tries to pry out your data [5]. If we consider viruses such as worms and Trojans, they destroy data completely, most likely without the possibility of return. DdoS attacks load servers and as a result, sites become inaccessible to users. There are programs that can damage the device and demand a ransom for restoration. It should be mentioned that **decent carefulness help avoid** getting caught in a simple manipulation and give away personal information with somebody`s own hands. It may also be that a third person is secretly added to the dialogue between two people and imperceptibly takes away information. It is enough to follow a couple of simple steps to protect against all the threats presented, for example, do not forget to update the software and train users. As technology continues to evolve, it is important to be informed and vigilant in cyberspace [3].

It is a very big misconception to think that personal data is not interesting to intruders and does not need cybersecurity. They absolutely do not care if a person or an enterprise are prominent or far-famed. All devices connected to the Internet are affected. This is because all cyberattacks are automated and aimed at obtaining any information available to them.

What does everyone need to know to avoid becoming a victim of

cyberattacks? It is important to control who has access to systems and data. Strong passwords, two-factor authentication and biometric technologies help protect access to important information. The use of firewalls, antivirus software and intrusion detection systems allows to monitor and block suspicious activity on the network. Data encryption is an important measure to protect data both at rest and during transmission. It prevents unauthorized users from accessing the data. People are the most vulnerable part of the cybersecurity system. Conducting regular training and informing employees about the risks and methods of protection can significantly reduce the likelihood of successful attacks. Having a clear plan of action in case of a cyberattack or incident empowers users to minimize damage and quickly restore the normal operation of the system [2].

We can note that the basics of cybersecurity include an understanding of current threats and protection methods. Awareness of possible risks allows users to make more informed and logical decisions. An important aspect of cybersecurity is training. Providing educational programs aimed at raising awareness of cyber threats is critical to reducing risks. Employees of organizations should be informed about potential threats and trained to respond to incidents correctly. Such measures significantly reduce the likelihood of successful attacks. Investments in the latest cybersecurity solutions may be justified in terms of minimizing potential losses from cyberattacks [3].

In conclusion, it is important to understand that cybersecurity is a process that continues all the time. Threats are changing, so to revamp security measures it is needed to update protection strategies. Regular security checks, updating rules and working with experts will help maintain a high level of protection.

Thus, the fundamentals of cybersecurity relate to different areas, and successful protection requires a comprehensive approach that includes training, technology and continuous improvement of protection methods. In the context of digital transformation and the increasing number of cyber threats, each of us must be responsible for our own safety and the safety of others in the virtual space.

References

1. Чем отличается кибербезопасность от информационной безопасности [Электронный ресурс] : tsecurity.com. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/knowledge-base/chto-takoe-ki berbezopasnost/. – Дата доступа: 30.09.2024

2. Вредоносное ПО [Электронный ресурс] : Kaspersky.ru. – Режим доступа: https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security. – Дата доступа: 02.10.2024

3. Why is Cybersecurity Critical? [Electronic resource] : Knowledgehut.com. – Mode of access: https://www.knowledgehut.com/blog/security/cyber-security-fundamentals. – Date of access: 04.10.2024

4. 16 common types of cyberattacks and how to prevent them [Electronic resource] – Mode of access: https://www.techtarget.com/searchsecurity/tip/6-common-types-of-cyber-attacks-and-how-to-prevent-them. – Date of access: 04.10.2024

5. Different Types of Phishing Attacks [Electronic resource] – Mode of access: https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks. – Date of access: 04.10.2024

У.В. Маннанов, Г.Ж. Аллаева
Ташкентский государственный технологический университет
Ташкент, Узбекистан

ОСОБЕННОСТИ УСТОЙЧИВОГО РАЗВИТИЯ ПРЕДПРИЯТИЙ ТЭК В УСЛОВИЯХ ФОРМИРОВАНИЯ ЦИФРОВОЙ ЭКОНОМИКИ

Аннотация. В статье рассмотрены основные факторы устойчивого развития предприятий топливно-энергетического комплекса в контексте формирования цифровой экономики. Рассмотрены основные понятия цифровой среды, определены закономерности устойчивого развития предприятий энергетического сектора.

U.V. Mannanov, G.Zh. Allayeva
Tashkent State Technological University
Tashkent, Uzbekistan

PATTERNS OF SUSTAINABLE INNOVATIVE DEVELOPMENT OF FUEL AND ENERGY SECTOR ENTERPRISES IN THE CONTEXT OF THE FORMATION OF THE DIGITAL ECONOMY

Abstract. The article considers the main factors of sustainable development of enterprises of the fuel and energy complex in the context of the formation of the digital economy. The basic concepts of the digital environment are considered, the patterns of sustainable development of energy sector enterprises are determined.