36. CYBER SECURITY AND DATA PRIVACY

Romanyuk D.A.

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Maksimchuk R.T. - Senior Lecturer

The importance of cyber security and data privacy is described in the paper. Common threats to computer systems and ways how to minimise risks are mentioned. Worldwide Data Privacy Regulations are presented.

Cyber security and data privacy have become critical issues in the digital age. With the proliferation of technology and the Internet, sensitive information is increasingly vulnerable to cyber attacks and unauthorised access.

Cyber security refers to the protection of computer systems, networks, and sensitive data from theft, damage, or illegal entry. It involves a range of technologies, processes, and practices aimed at securing digital information from potential threats, such as hacking, malware, and phishing attacks.

Data privacy, on the other hand, focuses on protecting the personal information of individuals from misuse and unauthorised access. This includes information such as social security numbers, credit card information, and other sensitive data that could be used to commit identity theft or other forms of fraud.

One of the main threats to computer systems and networks are cyber attacks, which can lead to the theft of personal data, leakage of commercial information or disruption of a website or application. Moreover, new types of threats have emerged recently, such as ransomware attacks, phishing and social engineering, which are used to obtain users' personal data or access sensitive information [1].

To minimise these risks, businesses and individuals must take steps to protect themselves from cyber threats. This includes using strong passwords, regularly updating software, and implementing multi-factor authentication. Additionally, organisations should invest in robust cyber security infrastructure and provide comprehensive training to employees on cyber security best practices.

Data privacy can also be protected through the use of encryption, data access controls and privacy policies. It is essential for organisations to have a clear understanding of the data they collect, how it is stored, and who has access to it. Organisations must also comply with relevant data privacy regulations, such as the General Data Protection Regulation (GDPR) in the European Union (EU) or the California Consumer Privacy Act (CCPA) in the United States [2].

The GDPR applies to all data directly or indirectly related to an identifiable person in the EU that is processed by an individual, company or organisation. Any small business that processes people's personal data within the EU is subject to the GDPR, no matter where in the world the business is based. It is important to note that the GDPR pertains to people within the EU, but not necessarily to EU citizens. This means that any company using the data of EU subjects, even if this company is stationed outside the EU, will need to comply with new ways of protecting data related to identifying information, IP addresses, cookies, health, genetic or biometric data.

The California Consumer Privacy Act A.B. 375 (CCPA) gives California residents an assortment of new privacy rights, starting with the right to be informed about what kinds of personal data companies have collected and why that data was collected.

Businesses are often confused by the terms "data privacy" and "data security" and mistakenly believe that keeping personal and sensitive data secure from hackers means that they are automatically compliant with data privacy regulations. Data security protects data from compromise by external attackers and malicious insiders whereas data privacy governs how the data is collected, shared and used. Traditional cyber security vendors claim that attacks will happen and that there is no way to avoid them. They claim the only thing left to do is to invest in technologies that detect the attack once it has already breached the network and mitigate the damages as soon as possible. With the right technologies in place, most attacks, even the most advanced ones, can be prevented without disrupting the normal business flow.

In conclusion, cyber security and data privacy are critical issues in the digital age. With the increasing amount of sensitive information stored online, it is essential for individuals and organisations to take proactive steps to protect themselves from cyber threats and safeguard personal data. By implementing robust cyber security measures and complying with relevant data privacy regulations, we can ensure that any information remains secure in the digital age.

References:

1. Cyber Security Threats and Attacks [Electronic resource]. – Mode of access: https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know. – Date of access: 28.03.2023.

2. Worldwide Data Privacy Regulations [Electronic resource]. – Mode of access: https://amtrustfinancial.com/blog/small-business/cybersecurity-vs-data-privacy. – Date of access: 28.03.2023.