BG Pulse Journal USA
ISSN:1947-2536 http://www.bgpulseusa.com/index.php/bg

CYBERSECURITY AND PERSONAL DATA PROTECTION

Islomova Ozoda Zokirjon qizi
University of Information Technology and Management
Student, Faculty of Philology and Language Teaching (English)

Abstract: This article presents information on the elements of cybersecurity and methods for protecting computers, servers, mobile devices, electronic systems, networks, and information from malicious attacks. It explains the fundamentals of security, including security principles, important security controls, and cybersecurity best practices. It also offers security programs with recommendations for analyzing user behavior for potential malware and learning how to more effectively detect new infections.

Keywords: Electronics, security, protocols, virus, mobile devices, information, cybersecurity, email, technology, business, cybercrime.

КИБЕРБЕЗОПАСНОСТЬ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация: В данной статье представлены элементы кибербезопасности и способы защиты компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных от вредоносных атак. Эта статья объясняет основы безопасности, включая принципы безопасности, ключевые элементы контроля и лучшие практики в области кибербезопасности. В программах безопасности даны рекомендации по анализу поведения пользователя для выявления потенциально вредоносных программ и улучшения способов обнаружения новых угроз.

Ключевые слова: Электронный, безопасность, протоколы, вирус, мобильный, информация, кибербезопасность, почта, технологии, бизнес, киберпреступ-ность.

INTRODUCTION

In today's rapidly evolving digital world, cybersecurity stands out as one of the most important areas. As the Internet and information technology have deeply penetrated almost all aspects of our lives, the need to protect personal data, financial data, and other important information has become an even more pressing issue. Cybersecurity refers to measures aimed at protecting computer systems, servers, mobile devices, networks, and data from malicious attacks, fraud, data theft, or corruption.

Cybersecurity is currently one of the newly emerging concepts and has various definitions. The main goal of cybersecurity is to maintain the confidentiality, integrity, and availability of information. These three main principles are known as the "CIA" model: Confidentiality, Integrity, and Availability. Confidentiality ensures that only authorized users can access information. Integrity is about maintaining the integrity of data, protecting it from unauthorized modification, deletion, or corruption. Availability is about ensuring that the system or data is available at the right time, meaning that users should be able to access their data even in the event of an attack or failure.

BG Pulse Journal USA
ISSN:1947-2536 http://www.bgpulseusa.com/index.php/bg
BG PULSE JOURNAL



In recent years, cybersecurity and the protection of personal data have become increasingly important not only in the field of technology, but also in social and economic life. Currently, the types of attacks carried out by cybercriminals are increasing. Among them are phishing, viruses, malware, DDoS attacks, data theft and fraud. Phishing is an attack in which fraudsters send fake emails or messages to obtain personal data (login, password, card number, etc.) from users. Malicious programs are designed to enter a computer or network and steal data, damage it or render the device inoperable

LITERATURE REVIEW

Cybersecurity and personal data protection

In recent years, cybersecurity and personal data protection have become increasingly important not only in the field of technology, but also in social and economic life. As the services provided via the Internet and digital technologies expand year by year, ensuring their security remains one of the main tasks. In this article, we will consider the importance of cybersecurity, issues of personal data protection, and key developments in this area.

The rapid development of the Internet in the early 2000s brought about a kind of technological revolution around the world. However, along with this revolution, new threats also emerged. In 2013, secret documents leaked by Edward Snowden revealed that the US National Security Agency (NSA) was conducting large-scale surveillance. This incident further increased distrust among people and states regarding the security of personal data.

By 2017, the widespread spread of the Wanna Cry malware affected hundreds of thousands of computers around the world and caused billions of dollars in economic losses. WannaCry initially

attacked national health systems, government agencies, and large corporations. This incident led to increased attention to cybersecurity, and many countries were forced to reconsider their national cybersecurity policies.

There are many ways to ensure cybersecurity. First, it is important to create strong passwords and change them regularly. Second, it is necessary to use two-factor authentication. This means that when logging in to the system, the user uses not only a password, but also an additional verification method (for example, an SMS code or biometric authentication). In addition, the use of modern antiviruses and firewalls, as well as regular updates of programs, are also important protective measures. Not only technological measures, but also users themselves play an important role in ensuring cybersecurity. Because many attacks rely on the human factor: data is lost due to user distraction, carelessness or lack of knowledge. Therefore, companies and organizations should regularly train their employees in cybersecurity and explain security rules to them.

Personal data protection is the foundation of our security

Personal data is being transmitted over the Internet in huge volumes. Nowadays, the average Internet user enters their confidential data into dozens of applications and websites every day. The European Union's General Data Protection Regulation (GDPR), which came into force in 2018, was a significant step towards protecting this personal data. The GDPR changed policies and procedures related to personal data not only in European countries, but also around the world. For example, companies were required to clearly inform users about how they store and process data.

By 2021, Facebook and other social media platforms were hit with large fines due to problems with the privacy of users' personal data. These incidents showed that protecting personal data is of great importance not only for users, but also for companies. In many countries, special cybersecurity centers have been established, which work to identify and prevent threats in the cyberspace at the national level.

Cybersecurity occupies a special place in the business sector. For companies, protecting the personal data of customers is not only a legal obligation, but also important for their reputation and reliability. If a company's data is leaked, this will not only lead to financial losses, but also to a loss of customer trust. As the development of digital technologies has become an integral part of human development, the issue of cybersecurity is gaining strategic importance on a global scale. In the modern technological environment, it is an urgent task to protect personal, corporate and state information resources, ensure information security and develop systematic measures against cybercrime. Analysis shows that in creating a cybersecurity infrastructure, along with improving technical tools and algorithms, the human factor, i.e. increasing the digital literacy of users, plays an important role.

DISCUSSION)

Developing cybersecurity in Uzbekistan

Uzbekistan is also taking a number of important steps in the field of cybersecurity. The Resolution of the President of the Republic of Uzbekistan "On ensuring information security in the Republic of Uzbekistan", approved in 2019, was aimed at strengthening the national cybersecurity system. In addition, in 2020, the Ministry of Information Technologies and Communications of Uzbekistan developed a national cybersecurity strategy.

Currently, various applications and programs are being introduced in our country to ensure the security of personal data, in particular, the "e-signature" system and new technologies that guarantee the security of electronic services. This process is creating a solid foundation for Uzbekistan's transition to a digital economy.

As the development of digital technologies has become an integral part of human progress, the issue of cybersecurity is gaining strategic importance on a global scale. In the modern technological environment, it is an urgent task to protect personal, corporate and state information resources, ensure information security and develop systematic measures against cybercrime. Analyses show that in creating a cybersecurity infrastructure, along with improving technical tools and algorithms, the human factor, namely increasing the digital literacy of users, plays an important role.

CONCLUSION

Today, cybersecurity and personal data protection issues are becoming increasingly important for every Internet user. With thousands of cyberattacks occurring every year, global rules for protecting personal data are becoming increasingly stringent. Uzbekistan is also actively working in this direction, developing national security strategies. We, as ordinary users, must use the most modern tools to protect our data. Because this is an important part not only of our personal security, but also of national cybersecurity. In practice, the possibilities of ensuring cybersecurity are expanding with the help of modern antivirus systems, cryptographic algorithms, network segmentation, firewalls, and analytical tools based on artificial intelligence.

At the same time, international experience shows that ensuring cybersecurity requires multilateral cooperation and an approach based on international standards, rather than individual actions. For example, standards such as ISO/IEC 27001 help organizations manage information security in a systematic way. Thus, ensuring information security and cybersecurity is emerging as the foundation of today's and future digital transformation. When scientific research and technological advances are combined with legal and institutional measures, robust mechanisms for protecting society from cyber threats emerge. This, in turn, is an important factor in ensuring the sustainable development of the digital economy and the security of the global information space.

REFERENCES:

1. Andress, J., & Winterfeld, S. (2014). Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. Elsevier.
2. Stallings, W. (2019). Network Security Essentials: Applications and Standards. Pearson Education.
3. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization.
4. Kaspersky Lab. (2023). Cybersecurity trends and predictions. Retrieved from: www.kaspersky.com.
5. Symantec Corporation. (2022). Internet Security Threat Report. Retrieved from: www.broadcom.com/company/newsroom/press-releases.
6. Kaspersky Lab. (2023). Basic cyber security for business. URL: www.kaspersky.ru.
7. Pechnikov, S.A. (2020). Information security in the digital age. Moscow: Nauchnyi mir.

8. Cybersecurity & Infrastructure Security Agency (CISA). (2024). Cyber Essentials. Retrieved from: www.cisa.gov.
9. Agency of cyber security of the Republic of Uzbekistan (2023). Kiberugrozy i zashchita personalnyx dannyx. Tashkent.
10. Termiz State University study guide. (2024). Fundamentals of information security. We sweat.