DIGITAL ECONOMY AND CURRENT CHALLENGES IN IMPROVING THE QUALIFICATION PREPARATION SYSTEM IN THE FIELD OF INFORMATION SECURITY.

Otakuzieva Zukhra Maratdaevna, Associate Professor, Ph.D.

Tashkent University of Information Technologies named after Muhammad Al-Khwarizmi

Nurov Shokhrukh Shomurodovich Tashkent International University Kimyo, Master business administration

Isroilov Zhavokhirbek Abdugaffor ugli, 3rd year student of the Faculty of Cyber Security, Information Security direction of the Tashkent University of Information Technologies named after Muhammad Al-Khwarizmi

Отакузиева Зухра Маратдаевна, доцент, к.э.н.

Ташкентский университет информационных технологий им.Мухаммада Ал-Хоразмий

Нуров Шохрух Шомуродович Ташкентский международный университет Кимё, Master business administration

Исроилов Жавохирбек Абдуғаффор угли, студент 3-курса факультета Кибербезопасности, направления Информационной безопасности Ташкентского университета информационных технологий им.Мухаммада Ал-Хоразми

АННОТАЦИЯ

Данная статья посвящена вопросу о том, как в условиях цифровой экономики происходят значительные изменения в том, как работает бизнес, и создаются новые проблемы для информационной безопасности. Рассказывается как все более широкое использование цифровых технологий и рост электронной коммерции привели к увеличению спроса на специалистов, обладающих опытом в области информационной безопасности.

Ключевые слова: цифровая экономика, информационная безопасность, кибербезопасность, киберугроза, специалисты в области информационной безопасности.

ABSTRACT

This article is devoted to the question of how in the conditions of the digital economy there are significant changes in the way business works, and new problems for information security are created. It tells how the increasing use of digital technologies and the growth of e-commerce have led to an increase in demand for specialists with experience in the field of information security.

Key words: digital economy, information security, cyber security, cyber threat, information security specialists.

INTRODUCTION

The digital economy has led to significant changes in how businesses operate and created new challenges for information security. The increasing use of digital technologies and the growth of e-commerce has led to an increased demand for professionals with expertise in information security.

To solve these problems, educational institutions and government bodies can collaborate to develop educational programs that meet the needs of the digital economy. This may include creating standardized curricula and certification programs, funding education and development initiatives, and promoting diversity in the field of information security. In addition, companies can invest in employee training and development programs to enhance the qualifications of their current workforce and fill the skills gap in cybersecurity. By solving this task, we can better prepare information security specialists for the demands of the digital economy and ensure that our systems and data are protected from cyber threats.

MAIN PART

There are a number of problems that need to be solve in the information security training system. Here are some of the current challenges:

1. Lack of qualified specialists: There is a shortage of qualified information security specialists. This is due in part to the rapid evolution of technology, making it difficult for educational institutions to keep up with the latest trends and best practices in cybersecurity.
2. Insufficient funding: Another problem arises in the fact that many educational institutions do not have sufficient funding to purchase the necessary equipment and resources to provide a quality volume in the field of information security.
3. Outdated curriculum: Some educational institutions may have outdated curricula that do not reflect the latest developments in cybersecurity. This can

lead to knowledge gaps among graduates who may not have the skills and knowledge needed to address the latest threats and vulnerabilities.
4. Limited practical experience: Many educational programs focus on theory rather than practical experience. This can make it difficult for graduates to apply what they learn to real-world practice.
5. Rapidly changing threat landscape: The information security threat landscape is constantly changing, and it can be difficult for educational institutions to keep up with the latest threats and vulnerabilities. This makes it difficult to provide relevant training that reflects the latest trends and best practices in cybersecurity.

To address these issues, educational institutions and governments should collaboratively develop educational programs that equip students with the skills and knowledge necessary to mitigate the latest threats and vulnerabilities in the field of information security. This may involve investing in newest equipment and resources, updating curricula to reflect the latest trends, and providing opportunities for practical experience through internships and other programs. Additionally, ongoing professional development and training can help information security professionals stay up-to-date with the latest developments and best practices.

Below are some additional details on the challenges of improving the workforce training system in the field of information security in the context of the digital economy:

1. Lack of standardization: There is no standardized educational curriculum or certification program for information security professionals. This can make it difficult for employers to assess the skills and knowledge of job candidates, and educational institutions may find it challenging to develop training programs that meet industry needs.
2. Shortage of cybersecurity skills: The rapid growth of the digital economy has led to a shortage of cybersecurity skills, with more job openings than qualified candidates to fill them. This is a significant problem for companies and governments that rely on information security specialists to protect their systems and data.
3. Limited diversity: The field of information security is not very diverse, with underrepresentation of women and minorities. This can limit the pool of information security professionals and result in a lack of diverse perspectives and approaches to cybersecurity.
4. Changing role of information security: The role of information security specialists is evolving as the digital economy continues to grow. They are no longer solely responsible for network and system security; they must also be knowledgeable about data privacy, regulatory compliance, and risk management.

Promoting diversity in the field of information security is essential to ensure that the workforce in cybersecurity reflects the diversity of the communities they serve. Here are several ways to promote diversity in the field of information security:

1. Informational and outreach programs: Educational institutions, industry associations, and government bodies can create informational and outreach programs targeted at underrepresented groups, such as women and minorities. These programs can provide mentorship, training, and networking opportunities to encourage more people from diverse backgrounds to pursue careers in information security.
2. Scholarships and grants: Financial barriers can hinder many individuals from pursuing careers in information security. Governments, educational institutions, and industry associations can provide scholarships and grants to help underrepresented groups access education and training in the field of information security.
3. Mentorship and coaching: Organizations can offer mentorship and coaching programs to help individuals from underrepresented groups develop their skills and knowledge in information security. This can help them overcome barriers and succeed in a field where they may face unique challenges.
4. Emphasis on interpersonal skills: Employers can emphasize the importance of interpersonal skills, such as communication and collaboration, when hiring information security professionals. This can attract candidates from diverse backgrounds who may not have traditional technical education but possess other valuable skills in this field.
5. Role models and representation: Representation matters, and organizations can promote diversity by showcasing and celebrating the achievements of information security professionals with diverse backgrounds. By elevating role models and encouraging diversity in leadership positions, organizations can encourage more individuals from underrepresented groups to pursue careers in information security.

In general, promoting diversity in the field of information security requires coordinated efforts from educational institutions, industry associations, government bodies, and employers. By providing informational and outreach programs, scholarships and grants, mentorship and coaching, emphasizing interpersonal skills, and promoting role models and representation, we can create a more diverse and inclusive workforce that is better prepared to address the challenges of the digital economy.

Underrepresented groups in the field of information security, such as women and minorities, may face a range of challenges that can hinder their career progression and success in this field. Here are some of the problems they may encounter:

1. Stereotypes and biases: Stereotypes and biases can hinder serious consideration of underrepresented groups in information security. Women and minorities may be perceived as less competent or less technical than their peers, leading to a lack of opportunities for career advancement or recognition.

2. Lack of role models: A shortage of role models and mentors with similar experiences can hinder underrepresented groups' ability to succeed in information security. This can lead to feelings of insecurity or isolation in the workplace.
3. Hiring practices: Hiring practices based on traditional credentials or experience can disadvantage underrepresented groups who may not have had the same opportunities or access to resources as their colleagues. This can impede their entry into the field or advancement in their careers.
4. Limited networking opportunities: Networking is crucial for career growth in information security, but underrepresented groups may not have the same access to networking opportunities as their colleagues. This can restrict their access to job opportunities, mentorship, and other resources that can help them succeed in the field.
5. Hostile work environment: Women and minorities may encounter a hostile work environment, including harassment or discrimination, which can hinder their sense of safety and hinder their career success.

CONCLUSION

Addressing the aforementioned problems requires coordinated efforts from employers, educational institutions, and industry associations to create a more inclusive and supportive environment for underrepresented groups in the field of information security. This may include providing mentorship and networking opportunities, promoting diversity in hiring practices, and fostering a safe and respectful workplace culture. By tackling these issues, we can help make the field of information security accessible to all and provide a more diverse and talented workforce to address the challenges of the digital economy.

REFERENCES

1. Actual Problems of Information Law: Textbook / Edited by I. L. Bachilo, M. A. Lapina. - Moscow: Yustitsiya, 2016. - 532 p.
2. Begishev, I. R. Crimes in the Field of Digital Information Handling: Monograph / I. R. Begishev, I. I. Bikeev. - Kazan: Izd-vo "Poznanie" Kazanskogo Innovatsionnogo Universiteta, 2020. - 300 p.
3. Cybercrime: Criminological, Criminal Law, Criminal Procedure, and Forensic Analysis: Monograph / Scientific Editor I. G. Smirnova; Responsible Editor O. A. Egerieva, E. M. Yakimova. - Moscow: Yurlitinform, 2016. - 312 p.
4. Countering Cybercrime in the Aspect of National Security Provision: Monograph / P. V. Agapov, S. V. Borisov, D. V. Vagurin, A. L. Korenyuk, V. V. Merkuryev, A. E. Pobegailo, A. I. Khaluillin. - Moscow: Academy of the Prosecutor General's Office of the Russian Federation, 2014. - 136 p.

Websites:

1. Is the Internet That Scary? "Gazeta.Ru" on the Real Cyber Threats. URL: http://www.gazeta.ru/tech/2014/11/05_a_6289085.shtml (accessed: 10.08.2021).
2. Hi-Tech Crime Trends 2020/2021. Cyber Threats, Trends, and Forecasts. URL: https://www.groupib.ru/blog/trends20_21 (accessed: 10.08.2021).
3. Kaspersky Security Bulletin: 2017 Review. URL: https://securelist.ru/ksb-review-of-the-year2017/88142/ (accessed: 10.08.2021).