kriptografiyada haqiqiy burilish 1985 yilda N. Koblits va V. Miller ilmiy ishlari [2] chop etilgandan so‘ng yuz berdi. Shu damdan boshlab mashhur jahon kriptologlari elliptik kriptografiya bilan shug’ullana boshladilar.

Faktorlash va EECh gruppasida diskret logarifmlash murakkabliklarini taqqoslama tahlili EEChlarning bahslashuvdan holi afzalliklarini namoyon etdi [3,4]. 1-jadvalda taqqoslama ma’lumotlar keltirilgan (ma’lumotlar tub maydonda diskret logarifmlash muammosi uchun ham oson hisoblanadi).

1-jadval

Kriptotahlil murakkabliklari bo‘yicha ma’lumotlar

Almashtirish moduli uzunligi	EECh gruppasida kriptotahlil murakkabligi	RSA modulini faktorlash murakkabligi
192 bit	$2^{95,82} \approx 10^{29,21}$	$2^{40,41} \approx 10^{12,32}$
256 bit	$2^{127,82} \approx 10^{39}$	$2^{40,56} \approx 10^{14,5}$
512 bit	$2^{255,82} \approx 10^{78}$	$2^{65,15} \approx 10^{19,86}$
1024 bit	$2^{511,82} \approx 10^{156}$	$2^{88,47} \approx 10^{27}$

XXI asrning boshidan boshlab nosimmetrik kriptografiyaning an’anaga aylanib qolgan kriptotizimlardan bardoshliligi EECh gruppasida diskret logarifmlash muammosining murakkkabligiga asoslangan tizimlarga o‘tish boshlangani ko‘zga tashlandi.

Foydalanilgan adabiyotlar ro‘yxati:

1. Akbarov D.E. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanishlari. Toshkent. “O‘zbekiston markasi “, 2009. - 432 b.

2. O‘z DSt 1092:2009 «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari».

3. Брюс Шнаер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ - Москва: ТРИУМФ, 2002.

4. Xasanov X.P. Takomillashgan diamatritsalar algebralari va parametrli algebra asosida kriptotizimlar yaratish usullari va algoritmlari. - Toshkent, 2008. 208 b.

ENSURING A SAFER DIGITAL FUTURE, THE IMPORTANCE OF CYBERSECURITY EDUCATION

(PhD) Mukhtarov Farrukh Mukhammadovich
The Ferghana Branch Tashkent university of information technologies
fmm1980@rambler.ru

Annotation: This article discusses the importance of cybersecurity education in today's digital world. It defines cybersecurity education and explains its benefits, such as reducing the risk of cyber attacks, protecting sensitive data, and minimizing the damage caused by a cyber attack. The article also provides a list of common cyber threats, such as phishing attacks, malware, and ransomware.

Keywords: cybersecurity education, information security, digital literacy, cyber threats, phishing attacks, malware, ransomware, cyber attack, security posture.

The digital world is constantly evolving, and with it, so do the cybersecurity threats that we face. In today's interconnected world, everyone is at risk of being targeted by cybercriminals, regardless of their age, background, or technical expertise. This is why cybersecurity education is more important than ever before. Cybersecurity education is the process of teaching people about the risks of the digital world and how to protect themselves from those risks. It encompasses a wide range of topics, including common cyber threats, how to create strong passwords and keep them safe, how to be safe online, how to protect your devices and data from unauthorized access, and how to respond to a cyber attack.

The digital world is constantly evolving, and with it, so do the cybersecurity threats that we face. In today's interconnected world, everyone is at risk of being targeted by cybercriminals, regardless of their age, background, or technical expertise. This is why cybersecurity education is more important than ever before.

Cybersecurity education is the process of teaching people about the risks of the digital world and how to protect themselves from those risks. It encompasses a wide range of topics, including:

Common cyber threats:

Phishing attacks: Phishing attacks are attempts to trick people into revealing sensitive information, such as passwords or credit card numbers, by sending fraudulent emails or text messages that appear to be from a legitimate source.

Malware: Malware is malicious software that can damage or disable computers or steal data. Malware can be spread through email attachments, infected websites, or USB drives.

Ransomware: Ransomware is a type of malware that encrypts a victim's files and then demands a ransom payment in exchange for the decryption key.

How to be safe online:

Be careful about what information you share. Only share personal information with websites and apps that you trust.

Be careful about what websites you visit. Avoid clicking on links in emails or on social media from unknown senders.

Keep your software up to date. Software updates often include security patches that can help to protect your devices from known vulnerabilities.

Use a firewall and antivirus software. A firewall can help to block unauthorized access to your computer, and antivirus software can help to detect and remove malware.

How to protect your devices and data from unauthorized access:

- Use strong passwords and keep them safe.
- Enable two-factor authentication (2FA) on all of your accounts. 2FA adds an extra layer of security by requiring you to enter a code from your phone in addition to your password when logging in.
- Keep your software up to date.

- Be careful about what apps you install on your devices. Only install apps from trusted sources.
- Use a VPN when connecting to public Wi-Fi networks. A VPN encrypts your traffic, making it more difficult for attackers to intercept your data.

If you think you have been the victim of a cyber attack, there are a few things you should do: Change your passwords immediately, contact your bank or credit card company if you think your financial information may have been compromised, report the attack to the appropriate authorities.

You may also want to consider hiring a cybersecurity expert to help you investigate the attack and recover from any damage. By following these tips, you can help to protect yourself from cyber threats and keep your devices and data safe. Cybersecurity education is important for everyone, but it is especially important for children and young adults. Children and young adults are more likely to use the internet and social media on a regular basis, and they may be less aware of the cybersecurity risks that they face. Cybersecurity education can help children and young adults to develop the skills and knowledge they need to stay safe online.

Cybersecurity education is also important for businesses and organizations of all sizes. Businesses and organizations are increasingly reliant on technology to operate, and they store a great deal of sensitive data, such as customer information and financial data. Cybersecurity education can help businesses and organizations to protect their data from cyber attacks and to minimize the damage that can be caused by a successful attack.

There are many different ways to get cybersecurity education. There are online courses, books, articles, and even video games that can teach you about cybersecurity. There are also many organizations that offer cybersecurity training programs and workshops.

No matter how you choose to get it, cybersecurity education is an essential part of staying safe in the digital world. By taking the time to learn about cybersecurity, you can protect yourself, your family, and your business from cyber threats.

Here are some specific benefits of cybersecurity education:

- Reduces the risk of cyber attacks: Cybersecurity education can help people to identify and avoid common cyber attacks, such as phishing emails and malware-infected websites.
- Protects sensitive data: Cybersecurity education can help people to protect their sensitive data, such as passwords, credit card numbers, and social security numbers, from unauthorized access.
- Minimizes the damage caused by a cyber attack: If a cyber attack does occur, cybersecurity education can help people to minimize the damage and recover quickly.
- Improves overall security posture: Cybersecurity education can help people to develop a more security-conscious mindset and to make better decisions about their online behavior.

Cybersecurity education is an investment in our digital future. By educating ourselves about cybersecurity, we can make the internet a safer place for everyone.

Cybersecurity education is an essential part of staying safe in the digital world. By taking the time to learn about cybersecurity, you can protect yourself, your family,

and your business from cyber threats. Cybersecurity education is an investment in our digital future. By educating ourselves about cybersecurity, we can make the internet a safer place for everyone.

Literature:

1. Blythe, J., & Shoesmith, D. (2019). Cybersecurity education in schools: An exploratory study into the current state and challenges. Computers & Education, 129, 78-88.

2. Ikeda, M., Nakamura, T., & Takeuchi, A. (2015). The importance of educating users on information security behaviors: Empirical study of individual's computer use at two Japanese universities. Computers & Security, 49, 315-327.

3. Muxtarov , F., Turdimatov , M., & Mominova , M. (2023). UMUMIY O'RTA TA'LIMGA KIBERXAVFSIZLIK FANINI TIZIMLI ISLOH QILISHNING USTUVOR YO'NALISHLARI. Engineering Problems and Innovations.

4. Muxtarov, F., & Sadirova, X. (2023). KORXONADA AXBOROT XAVFSIZLIGINI TA'MINLASHNING ZAMONAVIY USULLARI. *Engineering Problems and Innovations*.

5. Papastergiou, M., Nikolakopoulou, V., & Gerodimos, R. (2017). Cybersecurity education in Greece: A survey on school practices and stakeholder opinions. Journal of Information Security Education, 10(1), 40-49.

AUGMENTED REALITY IN ROBOTICS: MERGING WORLDS FOR THE FUTURE

Jomurodov Dustmurod Mamasolievich,
Ulashev Asror Nasriddinovich
Jizzakh branch of National University of Uzbekistan
jomurodovd77@gmail.com

Abstract : This article explores the use of augmented reality (AR) in robotics. Explores interactive programming lessons, allowing students to interact with virtual robots in real time, changing code and seeing the results of their actions. Simulation of real scenarios of robot operation in a virtual environment is also discussed, which simplifies the understanding of the principles of operation and programming of robots. These innovations make learning more interactive, enhancing learning and developing robotics programming skills.

Keywords: augmented reality, robotics, programming, training, virtual robots, interactive lessons, simulation, visualization, education.

Augmented Reality (AR) is a technology that allows you to integrate virtual objects and information into the real world. The application of this technology is expanding into many areas, including medicine, education, the gaming industry, and, of course, robotics [3]. Integrating augmented reality into robotics offers exciting