KIBERXAVFSIZLIK: INTERNETDA O'ZINI QANDAY HIMOYA QILISH MUMKIN

Andijon davlat chet tillari istituti,
Roman – german va slavyan tillari fakulteti,
Kompyuter lingvistikasi yo'nalishi 101 – guruh talabasi
Alisherova Nozimaxon Jumansher qizi
Ilmiy maslahatchi: ***Xomidova M.***

Annotatsiya: Ushbu maqolada kiberxavfsizlik tushunchasi, uning zamonaviy jamiyatdagi ahamiyati va internet foydalanuvchilarini kutayotgan asosiy xavf-xatarlar yoritiladi. Shuningdek, maqolada fishing, zararli dasturlar, ma'lumotlar o'g'irlanishi kabi tahdidlar tahlil qilinib, ulardan himoyalanishning samarali usullari bayon etiladi. Internetdan foydalanishda shaxsiy ma'lumotlarni himoya qilish, kuchli parollardan foydalanish, ikki bosqichli autentifikatsiya va xavfsizlik dasturlarining ahamiyati alohida ta'kidlanadi. Kiberxavfsizlikni ta'minlash nafaqat texnik, balki ijtimoiy muammo ekanligi ko'rsatib beriladi.

Kalit so'zlar: *Kiberxavfsizlik, internet xavfsizligi, shaxsiy ma'lumotlar, fishing, zararli dasturlar, autentifikatsiya, antivirus, tarmoq xavfsizligi, raqamli texnologiyalar*

Аннотация: В данной статье рассматривается понятие кибербезопасности, её значение в современном обществе, а также основные угрозы, с которыми сталкиваются пользователи интернета. Кроме того, в статье анализируются такие угрозы, как фишинг, вредоносные программы и кража данных, и излагаются эффективные способы защиты от них. Особое внимание уделяется защите персональных данных, использованию надёжных паролей, двухфакторной аутентификации и средств безопасности при работе в интернете. Подчёркивается, что обеспечение кибербезопасности является не только технической, но и социальной проблемой.

Ключевые слова: *Кибербезопасность, интернет-безопасность, персональные данные, фишинг, вредоносные программы, аутентификация, антивирус, сетевая безопасность, цифровые технологии*

Abstract: This article discusses the concept of cybersecurity, its significance in modern society, and the main threats faced by internet users. It also analyzes such risks as phishing, malware, and data theft, and outlines effective methods of protection against them. Special attention is paid to the protection of personal data, the use of strong passwords, two-factor authentication, and security software when using the internet. It is emphasized that ensuring cybersecurity is not only a technical issue but also a social one.

Keywords: *Cybersecurity, internet security, personal data, phishing, malware, authentication, antivirus, network security, digital technologies*

Bugungi kunda internet inson hayotining ajralmas qismiga aylangan. Bank xizmatlari, ta’lim, ish faoliyati va ijtimoiy tarmoqlar keng ravishda onlayn muhitga o‘tdi. Shu bilan birga, kiberxavfsizlik muammolari ham ortib bormoqda. Ayniqsa, so‘nggi yillarda akkaunt o‘g‘irlash, firibgarlik va ma’lumotlar sizib chiqishi holatlari ko‘paymoqda.

Internet foydalanuvchilari turli xil xavf-xatarlarga duch keladi. Eng keng tarqalganlari quyidagilar:

- **Fishing (phishing)** — soxta saytlar yoki xabarlar orqali shaxsiy ma’lumotlarni qo‘lga kiritish
- **Zararli dasturlar (malware)** — viruslar, trojanlar orqali tizimga zarar yetkazish
- **DDoS hujumlari** — serverlarni ortiqcha yuklash orqali ishlamay qolishiga olib kelish
- **Ijtimoiy muhandislik** — inson ishonchidan foydalanib ma’lumot olish

Bu tahdidlar nafaqat shaxsiy foydalanuvchilar, balki tashkilotlar uchun ham katta xavf tug‘diradi.

Fishing (Phishing)

Fishing — bu foydalanuvchini aldab uning shaxsiy ma’lumotlari (parol, bank karta raqami va boshqalar)ni qo‘lga kiritishga qaratilgan kiberhujum turidir. Odatda u soxta elektron pochta, havola yoki veb-saytlar orqali amalga oshiriladi.

Zararli dasturlar (Malware)

Zararli dasturlar kompyuter tizimiga zarar yetkazish yoki ma’lumotlarni o‘g‘irlash uchun yaratilgan dasturlardir. Ularga quyidagilar kiradi:

- viruslar
- trojanlar
- spyware (josus dasturlar)
- ransomware (ma’lumotlarni bloklab pul talab qiluvchi dasturlar)

Parol buzish hujumlari

Kiberjinoyatchilar foydalanuvchilarning parollarini maxsus dasturlar yoki oddiy taxmin qilish usuli orqali buzishga harakat qiladilar. Oddiy va qisqa parollar bunday hujumlar uchun juda oson nishon bo‘ladi.Internetda o‘zini himoya qilish usullari

Kuchli parollar yaratish

Parollar kamida 8–12 belgidan iborat bo‘lib, unda katta va kichik harflar, raqamlar hamda maxsus belgilar bo‘lishi tavsiya etiladi.

Ikki bosqichli autentifikatsiya

Ikki faktorli autentifikatsiya foydalanuvchi hisobini yanada ishonchli himoya qiladi. Bu usulda tizimga kirish uchun nafaqat parol, balki qo‘shimcha tasdiqlash kodi ham talab qilinadi.

Antivirus dasturlaridan foydalanish

Antivirus dasturlari zararli fayllarni aniqlash va ularni yo‘q qilish orqali kompyuterni himoya qiladi. Tizimni muntazam yangilab borish ham muhim hisoblanadi.

Shubhali havolalardan ehtiyot bo‘lish

Noma’lum manbalardan kelgan xabarlar yoki havolalarni ochmaslik kerak. Ayniqsa bank yoki shaxsiy ma’lumotlar so‘ralgan xabarlar ehtiyotkorlik bilan tekshirilishi lozim.

Dasturlarni yangilab borish

Operatsion tizim va dasturlarni yangilab turish xavfsizlik zaifliklarini bartaraf etadi.

Kiberxavfsizlik bugungi raqamli jamiyatning eng muhim masalalaridan biridir. Internetdan xavfsiz foydalanish uchun har bir foydalanuvchi oddiy xavfsizlik qoidalariga amal qilishi zarur. Kuchli parollar yaratish, antivirus dasturlaridan foydalanish, shubhali havolalardan ehtiyot bo‘lish va ikki bosqichli autentifikatsiyani yoqish orqali ko‘plab kiberxavflarning oldini olish mumkin.

Shunday qilib, internetdan ongli va ehtiyotkor foydalanish shaxsiy ma’lumotlar xavfsizligini ta’minlashda muhim ahamiyatga ega.

FOYDALANILGAN ADABIYOTLAR:

1. Kurose J., Ross K. Computer Networking: A Top-Down Approach. Pearson Education, 2017.

2. Stallings W. Network Security Essentials: Applications and Standards. Pearson, 2018.

3. Whitman M., Mattord H. Principles of Information Security. Cengage Learning, 2021.

4. O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi rasmiy materiallari.

5. Internet xavfsizligi bo‘yicha xalqaro tavsiyalar (Cybersecurity Guidelines).

6. Sodiqov M. Kiberxavfsizlik va axborot himoyasi. – Toshkent, 2023.

7. Stallings W. Cryptography and Network Security: Principles and Practice. – Pearson, 2020.