KIBERXAVFSIZLIK ASOSLARI: SHAXSIY MA`LUMOTLARNI HIMOYA QILISH

Milliy g‘oya va huquq kafedrasi
o‘qituvchisi Yuldasheva Husnidaxon
Qo`qon Davlat Universiteti
Matematika yo`nalishi 2-kurs talabasi
Murodova Ruhshonaxon Akmaljon qizi

Annotatsiya: Ushbu maqolada kiberxavfsizlik tushunchasi va shaxsiy ma’lumotlarni himoya qilishning asosiy tamoyillari yoritiladi. Raqamli makonda foydalanuvchining shaxsiy ma’lumotlari — parollar, bank kartasi ma’lumotlari, shaxsiy suratlar va shaxsga tegishli boshqa axborotlar turli kiberxavflarga duchor bo‘lishi mumkin. Maqolada shaxsiy axborotni himoyalashda kuchli parollardan foydalanish, ikki bosqichli autentifikatsiya, shubhali havolalardan saqlanish hamda ma’lumotlarni zaxiralash kabi amaliy usullar tahlil qilinadi. Shuningdek, internet madaniyati va foydalanuvchining shaxsiy mas’uliyatining ahamiyati ham ko‘rsatib o‘tiladi. Ushbu tadqiqot kiberxavfsizlik savodxonligini oshirishga, foydalanuvchining o‘z ma’lumotlariga ongli yondashuvini shakllantirishga xizmat qiladi.

Annotation: This article examines the concept of cybersecurity and the fundamental principles of protecting personal data. In the digital environment, users’ personal information may be exposed to various cyber threats. The article analyzes protection methods such as using strong passwords, enabling two-factor authentication, avoiding suspicious links, and regularly backing up data. The study aims to improve cybersecurity awareness and promote responsible management of personal information among users.

Аннотатсия: В данной статье рассматриваются понятие кибербезопасности и основные принципы защиты персональных данных. В цифровой среде личная информация пользователя может подвергаться различным киберугрозам. В статье анализируются такие методы защиты, как использование

надежных паролей, двухфакторная аутентификация, осторожность при переходе по подозрительным ссылкам и регулярное резервное копирование данных. Исследование направлено на повышение киберграмотности и ответственности пользователей за сохранность своих данных.

Tayanch so`zlar: kiberxavfsizlik, shaxsiy ma’lumotlar, maxfiylik, xavfsizlik siyosati, parol, ikki bosqichli autentifikatsiya, kiberxavf, fishing, zararli dastur, ma’lumotlarni zaxiralash, tarmoq himoyasi, foydalanuvchi mas’uliyati, internet madaniyati.

Keywords: cybersecurity, personal data, privacy, security policy, password, two-factor authentication, cyber threat, phishing, malware, data backup, network protection, user responsibility, digital literacy.

Ключевые слова: кибербезопасность, персональные данные, конфиденциальность, политика безопасности, пароль, двухфакторная аутентификация, киберугроза, фишинг, вредоносное ПО, резервное копирование данных, защита сети, ответственность пользователя, интернет-культура.

Kiberxavfsizlik - bu kompyuter tizimlari, tarmoqlar, dasturlar va ma'lumotlarni raqamli hujumlardan himoya qilishdir. So‘nggi yillarda kiberhavfsizlik va shaxsiy ma’lumotlarni himoya qilish nafaqat texnologiya sohasida, balki ijtimoiy va iqtisodiy hayotda ham tobora muhim ahamiyat kasb etmoqda. Internet va raqamli texnologiyalar orqali taqdim etiladigan xizmatlar yildan-yilga kengayib borayotgan bir paytda, ularning xavfsizligini ta’minlash asosiy vazifalardan biri bo‘lib qolmoqda. Ushbu maqolada biz kiberhavfsizlikning ahamiyati, shaxsiy ma’lumotlarni himoya qilish masalalari va bu sohadagi asosiy voqealarni ko‘rib chiqamiz. 2000-yillar boshida internetning jadal rivojlanishi butun dunyoda o‘ziga xos texnologik inqilobni yuzaga keltirdi. Biroq, bu inqilob bilan bir qatorda yangi xavf-xatarlar ham paydo bo‘ldi.

2013-yilda Edvard Snouden tomonidan fosh etilgan maxfiy hujjatlar AQSH Milliy xavfsizlik agentligi (MXA) keng ko‘lamli kuzatuvlar olib borayotganini ochib berdi. Bu hodisa insonlar va davlatlar o‘rtasida shaxsiy ma’lumotlar xavfsizligiga nisbatan ishonchsizlikni yanada kuchaytirdi. 2017-yilga kelib, WannaCry zararli

dasturining keng ko‘lamda tarqalishi butun dunyo bo‘ylab yuz minglab kompyuterlarga zarar yetkazdi va milliardlab dollar miqdorida iqtisodiy yo‘qotishlarga sabab bo‘ldi. WannaCry dasturi dastlab milliy sog‘liqni saqlash tizimlariga, davlat muassasalariga va yirik korporatsiyalarga hujum qildi. Bu hodisa kiberxavfsizlikka bo‘lgan e’tiborning yanada kuchayishiga olib keldi va ko‘plab mamlakatlar o‘zlarining kiberxavfsizlik sohasidagi milliy siyosatini qayta ko‘rib chiqishga majbur bo‘ldilar.

Shaxsiy ma’lumotlarni himoya qilish - xavfsizligimizning poydevori

Shaxsiy ma’lumotlar internet orqali juda katta hajmlarda uzatilmoqda. Hozirgi kunda oddiy internet foydalanuvchisi kuniga o‘nlab ilova va veb-saytlarga o‘zining maxfiy ma’lumotlarini kiritadi. 2018-yilda kuchga kirgan Yevropa Ittifoqining Ma’lumotlarni himoya qilish bo‘yicha umumiy reglamenti (GDPR) bu shaxsiy ma’lumotlarni himoyalash yo‘lidagi muhim qadam bo‘ldi. GDPR nafaqat Yevropa mamlakatlarida, balki butun dunyoda shaxsiy ma’lumotlar bilan bog‘liq siyosat va tartib-qoidalarni o‘zgartirdi. Misol uchun, kompaniyalardan foydalanuvchilarga ma’lumotlarni qanday saqlashlari va qayta ishlashlari haqida ochiq-oydin xabar berishlari talab etildi.

2021-yilga kelib, Facebook va boshqa ijtimoiy tarmoq platformalari foydalanuvchilarning shaxsiy ma’lumotlari maxfiyligiga oid muammolar tufayli yirik jarimalarga duchor bo‘ldi. Bu voqealar shuni ko‘rsatdiki, shaxsiy ma’lumotlarni himoya qilish nafaqat foydalanuvchilar uchun, balki kompaniyalar uchun ham juda muhim ahamiyatga ega ekan.

Bugungi raqamli dunyoda shaxsiy ma'lumotlarni himoya qilish juda muhim. Har kuni milliardlab ma'lumotlar almashinadi va har bir foydalanuvchi o'z shaxsiy ma'lumotlarini xavfsiz saqlash uchun choralar ko'rishi zarur. Kiberxavfsizlikning yetishmasligi natijasida katta moliyaviy yo'qotishlar, obro'sizlik va hatto huquqiy muammolar yuzaga kelishi mumkin. Bu maqola orqali o'quvchilar kiberxavfsizlikning ahamiyati va shaxsiy ma'lumotlarni himoya qilishning muhimligini tushunishlari mumkin. Shuningdek, maqola ularni o'zlarining raqamli xavfsizligini ta'minlash uchun zarur choralarni ko'rishga undaydi. Bugungi kunda kiberxavfsizlikka oid tahdidlar kun

sayin ortib bormoqda va ularning xarakteri ham o'zgarib turadi. Eng ko'p uchraydigan kiber tahdidlar quyidagilardir:

•Fishing hujumlari: Soxta elektron pochta yoki veb-saytlar orqali foydalanuvchilardan shaxsiy ma'lumotlarni olish.

• Zararli dasturlar: Kompyuter va mobil qurilmalarga zarar yetkazadigan va ma'lumotlarni o'g'irlash yoki yo'q qilishga mo'ljallangan dasturlar.

•Huquqiy chora-tadbirlar: Kiber jinoyatchilikka qarshi huquqiy choralarni kuchaytirish va huquq-tartibot organlari bilan hamkorlik qilish.

•Texnologik yangiliklar: Xavfsizlikni oshirish uchun yangi texnologiyalar va algoritmlar yaratish va ulardan foydalanish.

•Tashkilotlar uchun xavfsizlik siyosati: Har bir tashkilot uchun xavfsizlik siyosatini ishlab chiqish va uni qat'iy rioya qilish.

Ma'lumotlar xavfsizligi tushunchasi- Ma'lumotlar xavfsizligi deganda tabiiy yoki sun'iy xarakterdagi tasodifiy yoki qasddan qilingan ta'sirlardan axborot va uni qo'llab-quvvatlovchi infrastrukturaning himoyalanganligi tushuniladi. Bunday ta'sirlar axborot sohasidagi munosabatlarga, jumladan, axborot egalariga, axborotdan foydalanuvchilarga va axborotni muhofaza qilishni qo'llab- quvvatlovchi infrastrukturaga jiddiy zarar yetkazishi mumkin.

Bugungi kunda kiberxavfsizlik va shaxsiy ma’lumotlarni himoya qilish masalalari har bir internet foydalanuvchisi uchun dolzarb ahamiyat kasb etmoqda. Har yili minglab kiberhujumlar sodir etilayotgani bois, shaxsiy ma’lumotlarni himoya qilishning global qoidalari tobora qat’iylashib bormoqda. O‘zbekiston ham bu yo‘nalishda faol harakat qilib, milliy xavfsizlik strategiyalarini ishlab chiqmoqda. Biz, oddiy foydalanuvchilar sifatida, o‘z ma’lumotlarimizni himoya qilish uchun eng zamonaviy vositalardan foydalanishimiz lozim. Chunki bu nafaqat shaxsiy xavfsizligimizning, balki milliy kiberxavfsizlikning ham muhim qismi hisoblanadi.Xulosa sifatida shuni aytish mumkinki, kiberxavfsizlik bugungi dunyoda har bir inson va tashkilot uchun muhim masaladir. Shaxsiy ma'lumotlarni himoya qilish uchun kuchli parollar yaratish, ikki bosqichli autentifikatsiyani qo'llash, yangilanishlarni muntazam bajarish, antivirus

dasturlaridan foydalanish va zaxira nusxalarini yaratishkabi choralar muhimdir. Bundan tashqari, tahdidlar haqida xabardorlikni oshirish va xavfsizlik siyosatini rivojlantirish ham zarurdir. Bu choralar kiberxavfsizlikni ta'minlashda muhim rol o'ynaydi va shaxsiy ma'lumotlaringizni himoya qiladi.

Foydalanilgan adabiyotlar ro‘yxati

1. Karimov, B. Kiberxavfsizlik asoslari. — T.: “Fan va texnologiya”, 2022.
2. Абдурахмонов, С. Информационная безопасность и защита данных. — Ташкент: “Узбекистон”, 2021.
3. Stallings, W. Network Security Essentials: Applications and Standards. — Pearson Education, 2020.
4. Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. — John Wiley & Sons, 2015.
5. European Union Agency for Cybersecurity (ENISA). Cybersecurity Guidelines and Best Practices. — 2023.
6. Official Website: National Cyber Security Centre — https://www.ncsc.gov.uk
7. Symantec Security Reports. Global Internet Threat Report. — 2022.