

KIBERXAVFSIZLIK VA SHAXSIY MA'LUMOTLARNI HIMOYALASH

Anvarjonova Muhlis Abdurahim qizi

Namangan davlat texnika universiteti talabasi

[tel: +998956261405](tel:+998956261405)

e-mail: muhlisam1403@gmail.com

O'qituvchi: N.Sayidov

Namangan davlat texnika universiteti

Xayrullaxo'jayev Ismoilxo'ja Islomxo'ja o'g'li

Namangan davlat texnika universiteti talabasi

tel: 97-466-01-23

e-mail: xayrillaxojayevismoilxoja@gmail.com

Annotatsiya: Ushbu maqolada kiberxavfsizlikning zamonaviy jamiyatdagi ahamiyati, shaxsiy ma'lumotlarni himoyalash usullari hamda internet tarmog'ida uchraydigan asosiy kiberxavflar haqida so'z yuritiladi. Shuningdek, phishing, viruslar, hakerlik hujumlari kabi tahdidlarning foydalanuvchilarga ta'siri va ulardan himoyalash choralarini tahlil qilingan. Maqolada axborot xavfsizligini ta'minlashning dolzarb masalalari ham yoritilgan.

Kalit so'zlar: kiberxavfsizlik, axborot xavfsizligi, shaxsiy ma'lumotlar, phishing, virus, internet, himoyalash, kiberhujum, autentifikatsiya.

Bugungi kunda axborot texnologiyalarining rivojlanishi natijasida internet tarmog'i inson hayotining barcha sohalariga kirib bormoqda. Insonlar bank xizmatlari, onlayn ta'lim, elektron savdo va ijtimoiy tarmoqlardan keng foydalanmoqda. Shu sababli shaxsiy ma'lumotlarni himoyalash va kiberxavfsizlikni ta'minlash dolzarb masalaga aylandi.

Axborot xavfsizligi buzilishi natijasida foydalanuvchilarning shaxsiy ma'lumotlari tarqalishi, moliyaviy zarar va boshqa salbiy oqibatlar yuzaga kelishi mumkin.

Kiberxavfsizlik — kompyuter tizimlari, tarmoqlar va ma'lumotlarni turli tahdid va hujumlardan himoya qilishga qaratilgan chora-tadbirlar majmuasidir. Kiberxavfsizlikning asosiy vazifasi axborotning maxfiyligi, yaxlitligi va mavjudligini saqlashdan iborat. Hozirgi vaqtda davlat tashkilotlari, banklar va yirik kompaniyalar o'z axborot tizimlarini himoyalash uchun zamonaviy xavfsizlik texnologiyalaridan foydalanmoqda.

Shaxsiy ma'lumotlar deganda ma'lum bir shaxsga tegishli bo'lgan axborotlar tushuniladi. Bularga ism-familiya, telefon raqami, pasport ma'lumotlari, bank karta raqamlari, elektron pochta manzili va login-parollar kiradi. Ushbu ma'lumotlarning himoyalansizligi turli kiberjinoyatlarga sabab bo'lishi mumkin.

Internet tarmog'ida eng ko'p uchraydigan tahdidlardan biri phishing hisoblanadi. Phishing — foydalanuvchini aldash orqali uning maxfiy ma'lumotlarini qo'lga kiritish usulidir. Bunda foydalanuvchiga soxta sayt havolalari yoki elektron xatlar yuboriladi. Foydalanuvchi ushbu havolalarga kirib o'z ma'lumotlarini kiritganda, ma'lumotlar firibgarlar qo'lga tushadi.

Shuningdek, viruslar va zararli dasturlar ham kiberxavfsizlikka katta xavf tug'diradi. Viruslar kompyuter tizimiga zarar yetkazishi, fayllarni o'chirishi yoki foydalanuvchi ma'lumotlarini o'g'irlashi mumkin. Ayrim zararli dasturlar foydalanuvchi qurilmasini boshqarib, maxfiy ma'lumotlarni kuzatadi.

Hakerlik hujumlari ham bugungi kundagi jiddiy muammolardan biridir. Hakerlar turli usullar yordamida tizimlarga noqonuniy kirishga harakat qiladi. Natijada tashkilotlarning muhim ma'lumotlari o'g'irlanishi yoki tizim faoliyati izdan chiqishi mumkin. Shu sababli tashkilotlar xavfsizlik devorlari, antivirus dasturlari va autentifikatsiya tizimlaridan foydalanadi.

Shaxsiy ma'lumotlarni himoyalash uchun foydalanuvchilar bir qator xavfsizlik qoidalariga amal qilishi lozim. Avvalo, murakkab va ishonchli parollardan foydalanish kerak. Parollar harflar, sonlar va maxsus belgilar kombinatsiyasidan iborat bo'lishi tavsiya

etiladi. Bundan tashqari, ikki bosqichli autentifikatsiyani yoqish foydalanuvchi akkauntining xavfsizligini oshiradi.

Noma'lum havolalarni ochmaslik va ishonchsiz dasturlarni yuklab olmaslik ham muhim hisoblanadi. Antivirus dasturlaridan foydalanish qurilmani zararli dasturlardan himoya qilishga yordam beradi. Ma'lumotlarni muntazam zaxiralab borish esa ma'lumotlar yo'qolishining oldini oladi.

Hozirgi davrda kiberxavfsizlik nafaqat alohida foydalanuvchilar, balki davlat xavfsizligi uchun ham muhim ahamiyatga ega. Chunki axborot tizimlariga qilingan hujumlar iqtisodiyot, bank tizimi va davlat boshqaruviga salbiy ta'sir ko'rsatishi mumkin. Shu sababli ko'plab mamlakatlarda kiberxavfsizlikni rivojlantirishga katta e'tibor qaratilmoqda.

Demak, internetdan xavfsiz foydalanish, shaxsiy ma'lumotlarni himoya qilish va zamonaviy xavfsizlik choralariga rioya qilish har bir foydalanuvchi uchun muhim hisoblanadi. Kiberxavfsizlik qoidalariga amal qilish orqali turli tahdid va xavflarning oldini olish mumkin.

FOYDALANILGAN ADABIYOTLAR

1. Abdullayev A. Axborot xavfsizligi asoslari. – Toshkent: O'zbekiston, 2021.
2. Qosimov B. Zamonaviy axborot texnologiyalari. – Toshkent: Fan va texnologiya, 2020.
3. Meliboyev T. Kiberxavfsizlik va axborotni himoyalash usullari. – Toshkent, 2022.
4. Stallings W. Network Security Essentials: Applications and Standards. – Pearson Education, 2019.
5. Whitman M., Mattord H. Principles of Information Security. – Cengage Learning, 2021.
6. O'zbekiston Respublikasi "Shaxsga doir ma'lumotlar to'g'risida"gi Qonuni.
7. O'zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi materiallari.