

**IJTIMOIIY TARMOQLARDA AXBOROT XAVFSIZLIGI**

Ro‘zmatova Sadoqatxon

Annotatsiya: *Ijtimoiy tarmoqlar zamonaviy hayotimizning ajralmas qismiga aylangan. Bugungi kunda deyarli har bir inson o‘z fikrini bildirish, do‘stlari va tanishlari bilan muloqot qilish, yangiliklardan xabardor bo‘lish, turli ma‘lumotlarni almashish uchun ijtimoiy tarmoqlardan foydalanadi. Ushbu platformalar insonlar orasidagi masofani qisqartiradi, bilim va tajriba almashinuvini osonlashtiradi, shuningdek, biznes va ta‘lim sohalarida yangi imkoniyatlar yaratadi. Biroq, ijtimoiy tarmoqlarning keng tarqalishi bilan birga, ularda axborot xavfsizligi masalalari ham dolzarblashmoqda. Axborot xavfsizligi — bu shaxsiy va jamoat ma‘lumotlarini himoya qilish, ularning noto‘g‘ri qo‘llarga tushishining oldini olish va onlayn faoliyatni xavfsiz tarzda olib borishni ta‘minlashdir. Ushbu maqolada ijtimoiy tarmoqlarda axborot xavfsizligining ahamiyati, mavjud xavf-xatarlar, ularni oldini olish usullari hamda foydalanuvchilarning mas‘uliyati haqida batafsil so‘z boradi.*

Kalit so‘zlar: *ijtimoiy tarmoqlar, biznes, ta‘lim, muloqot, muammolar, yechim, dasturlar, kompyuterlar, jamoa.*

Ijtimoiy tarmoqlarda axborot xavfsizligi muammolari turli ko‘rinishlarda namoyon bo‘ladi. Eng ko‘zga ko‘ringan muammolardan biri shaxsiy ma‘lumotlarning o‘g‘irlanishi hisoblanadi. Foydalanuvchilar o‘zlari haqidagi shaxsiy ma‘lumotlarni, shu jumladan ism-familiya, tug‘ilgan sana, yashash joyi, telefon raqami, elektron pochta manzili kabi ma‘lumotlarni ijtimoiy tarmoqlarga joylashtiradilar. Bu ma‘lumotlar esa firibgarlar va kiberjinoyatchilar tomonidan osongina qo‘lga olinib, turli zararli maqsadlarda ishlatilishi mumkin. Masalan, shaxsiy ma‘lumotlar yordamida firibgarlar moliyaviy firibgarliklarni amalga oshirishi, identifikatsiya o‘g‘irligi orqali firibgarliklarni sodir etishi yoki hatto shaxsning obro‘sigacha putur yetkazishi mumkin. Firibgarlik va aldovlar ijtimoiy tarmoqlarda keng tarqalgan yana bir xavf hisoblanadi. Soxta akkauntlar yaratish,



foydalanuvchilarni aldash maqsadida yolg'on ma'lumotlar tarqatish, pul yoki boshqa qimmatbaho narsalarni so'rash kabi firibgarlik usullari keng qo'llaniladi. Ushbu holatlar ko'pincha foydalanuvchilarning ishonchiga tayangan holda amalga oshiriladi va natijada ular moliyaviy zarar ko'rishi, shaxsiy ma'lumotlari o'g'irlanishi yoki onlayn obro'lari zarar ko'rishi mumkin. Bundan tashqari, firibgarlar tomonidan tarqatilgan zararli dasturlar va havolalar orqali kompyuterlar va mobil qurilmalar viruslar bilan zararlanadi, bu esa foydalanuvchilarning shaxsiy ma'lumotlarini o'g'irlanishiga olib keladi.[1]

Kiberhujumlar ham ijtimoiy tarmoqlarda axborot xavfsizligiga katta tahdid soladi. Xakerlar turli metodlardan foydalangan holda foydalanuvchilarning akkauntlarini buzishga harakat qiladilar. Bu usullarga parollarni buzish, phishing (aldovchi elektron xabarlar orqali ma'lumotlarni olish), zararli dasturlarni tarqatish kiradi. Kiberhujumlar natijasida foydalanuvchilarning shaxsiy ma'lumotlari, moliyaviy ma'lumotlari va onlayn faoliyati nazoratdan chiqib ketadi, bu esa jiddiy zararlar keltirishi mumkin. Yolg'on va noto'g'ri ma'lumotlarning tarqalishi ijtimoiy tarmoqlarda keng tarqalgan muammolardan yana biridir. Ijtimoiy tarmoqlardagi tezkor va keng qamrovli axborot almashuvi noto'g'ri ma'lumotlar, mish-mishlar va yolg'on xabarlarining tez tarqalishiga imkon beradi. Bu esa jamiyatda tushunmovchiliklar, ijtimoiy tarangliklar, hatto zo'ravonlik holatlarining yuzaga kelishiga olib kelishi mumkin. Shuningdek, noto'g'ri ma'lumotlar siyosiy barqarorlikka ham salbiy ta'sir ko'rsatishi mumkin.[2]

Ijtimoiy tarmoqlarda axborot xavfsizligini ta'minlash uchun bir qator muhim choralarga rioya qilish zarur. Eng avvalo, foydalanuvchilar o'z shaxsiy ma'lumotlarini ehtiyotkorlik bilan ulashishlari kerak. Shaxsiy ma'lumotlarni faqat ishonchli do'stlar va tanishlar bilan, zarur hollarda va ehtiyotkorlik bilan bo'lishish axborot xavfsizligini ta'minlashga yordam beradi. Shuningdek, foydalanuvchilar o'z akkauntlarini himoya qilish uchun murakkab, oson taxmin qilib bo'lmaydigan parollardan foydalanishlari, parollarni muntazam yangilab borishlari muhimdir.[3]

Ikki faktorli autentifikatsiya tizimini yoqish ijtimoiy tarmoqlarda xavfsizlikni oshirishning samarali usullaridan biridir. Ushbu tizim foydalanuvchi



akkauntiga kirishda paroldan tashqari qo'shimcha tasdiqlash bosqichini talab qiladi, bu esa akkaunt buzilishining oldini oladi. Bundan tashqari, noma'lum va shubhali havolalar, xabarlar va ilovalarga ehtiyotkorlik bilan qarash kerak. Firibgarlar ko'pincha zararli havolalar orqali foydalanuvchilarning qurilmalariga viruslar yoki zararli dasturlarni o'rnatishga harakat qiladilar. Shuning uchun bunday havolalarga bosishdan oldin ularning xavfsizligini tekshirish lozim. Maxfiylik sozlamalarini to'g'ri o'rnatish orqali foydalanuvchilar o'z ma'lumotlarini kimlar ko'rishi mumkinligini nazorat qilish imkoniyatiga ega bo'ladilar. Ijtimoiy tarmoqlarning ko'pchilik platformalarida maxfiylik sozlamalari mavjud bo'lib, ular yordamida foydalanuvchi o'z profilini, postlarini, do'stlar ro'yxatini va boshqa ma'lumotlarni faqat ma'lum doirada ko'rishga ruxsat berishi mumkin. Bu esa shaxsiy ma'lumotlarning noto'g'ri qo'llarga tushishining oldini oladi. Qurilmalarni va ilovalarni muntazam yangilab borish ham axborot xavfsizligini ta'minlash uchun muhimdir. Yangilanishlar ko'pincha xavfsizlikni oshirishga qaratilgan bo'lib, yangi aniqlangan zaifliklarni bartaraf etadi. Shuningdek, antivirus dasturlaridan foydalanish va ularni doimiy ravishda yangilab borish kompyuter va mobil qurilmalarni zararli dasturlardan himoya qiladi. Axborot xavfsizligi madaniyatini shakllantirish va foydalanuvchilarni bu borada xabardor qilish ham muhim ahamiyatga ega. Ko'pgina foydalanuvchilar axborot xavfsizligi qoidalarini bilmaydi yoki ularga rioya qilmaydi, bu esa ularni firibgarlik va kiberhujumlarga nisbatan zaif qiladi. Shu sababli, axborot xavfsizligi bo'yicha muntazam o'quv va targ'ibot ishlarini olib borish, foydalanuvchilarni soxta ma'lumotlar va firibgarliklardan himoyalashga o'rgatish zarur. Axborot xavfsizligi nafaqat individual foydalanuvchilar uchun, balki butun jamiyat uchun muhimdir. Shaxsiy ma'lumotlarning himoyasi odamlarning shaxsiy hayotini saqlashga, moliyaviy zarar ko'rmaslikka va onlayn faoliyatni xavfsiz tarzda olib borishga yordam beradi. To'g'ri va ishonchli axborot tarqatish jamiyatda ijtimoiy barqarorlikni ta'minlaydi, noto'g'ri ma'lumotlarning tarqalishini kamaytiradi. Shu sababli, axborot xavfsizligini ta'minlash ijtimoiy tarmoqlarda ishonchli va samarali muloqot uchun zarurdir. Ijtimoiy tarmoqlar operatorlari va davlat organlari ham axborot



xavfsizligini ta'minlashda katta rol o'ynaydi. Ular foydalanuvchilarning shaxsiy ma'lumotlarini himoya qilish, kiberjinoyatchilikka qarshi kurashish va axborot xavfsizligi standartlarini joriy etish uchun samarali choralar ko'rishi kerak. Shu bilan birga, qonun hujjatlari va tartib-qoidalar yordamida onlayn makonda qonunbuzarliklarning oldini olish muhimdir.[4]

Har bir foydalanuvchi axborot xavfsizligi madaniyatini shakllantirishda o'zining mas'uliyatini anglab, unga rioya qilishi lozim. O'z ma'lumotlarini himoya qilish, ehtiyotkorlik bilan onlayn faoliyat yuritish va boshqalarni ham bu borada ogoh qilish orqali ijtimoiy tarmoqlarda xavfsiz va ishonchli muhit yaratish mumkin. Shu tariqa, raqamli jamiyatning barqaror rivojlanishiga hissa qo'shiladi.

Xulosa:

Xulosa qilib aytganda, ijtimoiy tarmoqlarda axborot xavfsizligi bugungi kunda juda dolzarb va muhim masala hisoblanadi. Shaxsiy ma'lumotlarning o'g'irlanishi, firibgarliklar, kiberhujumlar va noto'g'ri ma'lumotlarning tarqalishi xavf-xatarlaridan himoyalaniş uchun foydalanuvchilar ehtiyotkorlik bilan harakat qilishlari, kuchli parollardan foydalanishlari, ikki faktorli autentifikatsiya tizimini yoqishlari, maxfiylik sozlamalarini to'g'ri o'rnatishlari va shubhali havolalarga ehtiyotkorlik bilan qarashlari zarur. Shu bilan birga, axborot xavfsizligi bo'yicha ta'lim va targ'ibot ishlarini kuchaytirish, ijtimoiy tarmoqlar operatorlari va davlat organlari tomonidan samarali chora-tadbirlarni amalga oshirish muhimdir. Axborot xavfsizligini ta'minlash orqali ijtimoiy tarmoqlar insonlar orasidagi muloqotni yanada xavfsiz, ishonchli va samarali qiladi hamda raqamli jamiyatning barqaror rivojlanishiga xizmat qiladi. Har bir foydalanuvchi o'ziga yuklatilgan mas'uliyatni anglab, axborot xavfsizligi madaniyatini rivojlantirishga hissa qo'shishi kerak. Shunday qilib, ijtimoiy tarmoqlarda xavfsiz va samarali faoliyat yuritish mumkin bo'ladi.

FOYDALANILGAN ADABIYOTLAR:

1. Mamatova Ya. "Ijtimoiy tarmoqlarda axborot hujumlari va tahdidlar" — 2024 yil
2. Nurmatov O. "Axborot xavfsizligi asoslari" — 2023 yil



3. Karimova D. "Ijtimoiy tarmoqlarda shaxsiy ma'lumotlarni himoya qilish" — 2022 yil
4. Tursunov S. "Axborot xavfsizligiga bo'ladigan tahdidlar" — 2023 yil
5. Islomova N. "Raqamli makonda axborot xavfsizligini ta'minlash" — 2024 yil
6. Qodirov B. "Kiberxavfsizlik va ijtimoiy tarmoqlar" — 2023 yil
7. Rasulova M. "Axborot-kommunikatsiya texnologiyalari va xavfsizlik" — 2022 yil