# AXBOROT XAVFSIZLIGINI TA’MINLASHDA MEDIA VA AXBOROT SAVODXONLIGINING AHAMIYATI

**Yusubov Jaloliddin Kadamovich**
*O‘zMU dotsenti, f.f.b.f.d (PhD*

***Annotatsiya.*** *Ushbu maqolada bugungi kunda axborot xavfsizligini ta’minlashda media va axborot savodxonligining ahamiyati ijtimoiy-falsafiy jihatdan tahlil qilingan. Bugungi zamonaviy dunyoda axborot xavfsizligi dolzarb muammo bo‘lib, uni har tomonlama o‘rganish davr talabi bo‘lib bormoqda.*

***Kalit so‘zlar:*** *axborot xavfsizligi, parol, virtual, internet, kiber hujum, enkripsiya*,

Internet texnologiyalarining rivojlanishidan oldin axborotni saqlash nisbatan oson bo‘lgan. Boshqalar bilmasligi kerak bo‘lgan qog‘ozda yozuv shaklidagi, kassetada ovoz shaklidagi yoki boshqa vosita va shakldagi ma’lumotni mustahkam seyfga solib qulflab qo‘yishingizni o‘zi kifoya bo‘lgan. Hukumat idoralari, banklar va boshqa maxfiy xujjatlar bilan ishlovchi tashkilotlarda ham axborot xavfsizligi oson hal qilingan: «o‘ta sirli» tamg‘asi bilan xujjatni seyfga tiqib, seyf turgan xona eshiklarini mustahkam qulflab, binoga bir nechta qorovul tayinlash bilan axborot xavfsizligiga erishilgan. U zamonlar o‘tdi endi.

Hozir juda ko‘p turdagi ma’lumotlar (agar hammasi bo‘lmasa) elektron shaklda internetga ulangan serverlarda saqlanmoqda. Ularning qanchasi shaxsiy, qanchasi maxfiy ekanligi ahamiyatsiz. Muhimi – odamlarning real hayotiga aloqador ma’lumotlar virtual tarmoqdan bitta

[1] Масилова М. Г. Мотивация профессиональной деятельности преподавателей вуза в условиях модернизации высшего профессионального образования (по результатам лонгитюдного исследования, проведенного во ВГУЭС) /М. Г. Масилова // Вестник высшей школы. 2015. № 11. С. 33–38.

parol yoki bitta elektron kalit uzoqligida saqlanmoqda. Kimningdir shaxsiy ma’lumotini o‘g‘irlamoqchi bo‘lgan, yoki qaysidir idoraning sirli xujjatlarini ko‘zdan kechirmoqchi bo‘lganlar hozirgi kunda devor oshishi, qaysidir eshikni buzib kirishi, bir nechta qorovulni dog‘da qoldirishi, seyfni buzishi shart emas. Internet imkoniyatlaridan kelib chiqqan holda bugun shaxsiy ma’lumot ovchisi hatto ma’lumotlar saqlanadigan serverga yaqin joyda turishi ham kerak emas. Boshqa davlat, boshqa qit’adan turib internet orqali yaxshi himoyalanmagan server ma’lumotlarini olish hech gap emas ekanligini ko‘rib turibmiz. Axborot xavfsizligi bo‘yicha eng yaxshi himoyalanishi tan olingan Amerika hukumatining elektron saylovlar tizimiga bo‘lgan kiber xujum buning yaqqol misoli bo‘lishi mumkin.

Qog‘oz va boshqa internetga aloqador bo‘lmagan vositalarda saqlanadigan axborotni ishonchli joyda saqlash kerak. Bunday ma’lumotlar keraksiz bo‘lib qolgan vaziyatda albatta axborotni uni saqlovchi vosita bilan birga jismoniy yo‘q qilish maqsadga muvofiq. Qaysidir maxfiy xujjat kerak bo‘lmay qolsa, uni chiqindiga butunligicha tashlab yubormang. Disk yoki fleshkada maxfiy ma’lumotingizdan qutulmoqchi bo‘lsangiz, shunchaki axborotni o‘chirish bilan cheklanmang. Albatta axborotni uni tashuvchi vosita bilan birgalikda qayta tiklab bo‘lmas holatga keltirib, keyin tashlab yuborish tavsiya etiladi. Har qanday katta parchalarda yirtilgan qog‘ozni birlashtirish, har qanday disk yoki fleshkadan o‘chirilgan ma’lumotni ma’lum texnologiyalar asosida tiklash mumkinligini unutmang.

Internetdagi axborot xavfsizligi esa juda katta mavzu. Bugungi kunda deyarli hammaning hayotiga kompyuterlar, smart telefonlar, onlayn bank kartalari va boshqa vositalar orqali kirib kelgan internet texnologiyalariga bog‘liq axborot xavfsizligini ko‘p uchraydigan muammolar jihatidan bo‘lib ko‘rib chiqamiz.

Ma’lumotlarni internet orqali uzatishda foydalaniladigan eng zamonaviy xavfsizlik vositasi – enkripsiya. Bunda foydalanuvchi tomonidan yuborish uchun kiritilgan ma’lumot foydalanuvchi qurilmasining o‘zida enkripsiya qilinadi (inson o‘qishi/ko‘rishi/eshitishi mumkin bo‘lgan shakldan faqat mashina o‘qiy olishi mumkin bo‘lgan shaklda o‘tkaziladi). Enkripsiya qilingan ma’lumot tarmoqda xavfsiz shaklda yetkazilib, qabul qiluvchi server yoki boshqa qurilmada qayta shakllantiriladi (dekripsiya qilinadi). SHu tariqa ikki tomon ma’lumotni xavfsiz shaklda bir-biriga uzatishi mumkin.

Sizning axborot xavfsizligingizda kim bilandir onlayn suhbatingizni uchinchi shaxslar bilmasligi juda muhim hisoblanadi. Saytlar orqali ma’lumot almashganingizda brauzerning SSL sertifikat haqida ma’lumot beruvchi qismiga e’tiborli bo‘ling. Odatda zamonaviy brauzerlar enkripsiyasi yo‘q, SSL sertifikati eskirgan yoki mavjud bo‘lmagan saytlardan foydalanuvchilarni yaxshi ogohlantiradi.

Smart telefoningizga yuklab olayotgan dasturlaringiz va o‘yinlaringizning ishonchliligiga e’tibor bering. Ba’zan o‘zini o‘yin sifatida tanishtirayotgan dasturlar aslida boshqa g‘arazli maqsadlarda ish olib borishi ham hech gap emas. Ko‘ngilsiz holatlarning oldini olish uchun faqat ishonchli manbaalardan dastur va o‘yinlaringizni yuklab olishingiz kerak. Google Play yoki Apple AppStore kabi ishonchli manbaalardan foydalaning. Saytlardan to‘g‘ridan-to‘g‘ri yuklab olingan, yoki sizga messenjerlar orqali yuborilgan o‘yin va dasturlarni telefoningizga o‘rnatmang. Mavjud o‘rnatilgan dasturlaringizni Google Play Protect yoki shunga o‘xshash vositalar yordamida tekshirishingiz mumkin.

Zamonaviy messenjerlarda, xususan Telegram va WatsApp dasturlarida «tomondan-tomongacha enkripsiyalash» imkoniyati bor. Bunda siz va suhbatdoshingiz o‘rtasidagi yozishma, audio yoki video muloqot, almashiladigan fayllar enkripsiya qilinadi va server ishtirokisiz to‘g‘ridan-to‘g‘ri suhbatdoshingizga yetkaziladi. Albatta, bu ham axborotning 100% xavfsizligini ta’minlamaydi. CHunki hammaga ma’lumotni enkripsiyalangan shaklda yuborishda yoki qabul qilishda bo‘lmasligi mumkin.

Xalqimiz ba’zan juda sodda va ishonuvchan. Bu soddalikni internet axborot xavfsizligi kechira olmaydi. Afsuski internetdagi shaxsiy ma’lumotlar xavfsizligidan yaxshi xabardor bo‘lmaslik, zamonaviy bilimlarni o‘zlashtirishga jiddiy qaramaslik oqibatida ayanchli hodisalar uchrab turibdi. Texnologiyalar rivojlangan sari axborotni o‘g‘irlash usullari ham zamonaviylashib,

juda katta kuchga ega bo‘lib bormoqda. Axborotni o‘g‘irlash yoki unga zarar yetkazish bugungi kunda shu darajaga chiqqanki, hatto ba’zi holatlarda sizning parolingiz, SMS tasdiqlash kodingiz ham talab qilinmagan holatda ma’lumotlaringizni yo‘qotishingiz mumkin. Masalan, siz ishonib o‘rnatgan dastur/o‘yin qaysidir rasmingizni sizning soddalingizngizdan foydalanib ko‘chirib olishi mumkin. Qaysidir suhbatdoshingiz sizni aldab u yoki bu turdagi ma’lumotingizni so‘rab olishi mumkin. Siz kutmagan, bilmagan usullar bilan shaxsiy axborot muhitingizga zarar yetkazishlari hech gap emas. Bunga ko‘pincha juda oddiy xatolar, juda keng tarqalgan qoidalarga bilimsizlik tufayli amal qilmaslik sabab bo‘lishi mumkin.

**Foydalanilgan adabiyotlar:**

1.Karimov I.M. Axborot xavfsizligi asoslari. Darslik/ O‘zR IIV Akademiyasi, 2016.
2.Эшбеков Т. Ахборот-психологик хавфсизлик. Ўқув қўлланма. –Т.: ЎзМУ, 2013.
3.Расулов А. Глобал жараёнлар ва маънавият. //Ўзбекистон матбуоти,
4.5-6 сон
5.Саидов У. Глобаллашув ва маданиятлараро мулоқот. –Т. Академия, 2008