KIBERPSIXOLOGIYA: TAHDIDLAR VA ODAMLAR ISHONUVCHANLIGIDAN FOYDALANISH JARAYONI

Mahmudov Murodjon Alisher o‘g’li
O‘zDJTU Xalqaro jurnalistika fakulteti talabsi

Annotatsiya. *Ushbu maqolada kiberpsixologiya tushunchasi, raqamli makonda online tahdidlar, soxta havolalar va xabarlar, shaxsiy ma’lumotlarni muhofaza qilish va foydlanuvchilarda axborot savodxonligini oshirish borasida ma’lumotlar va tavsiyalar berib o‘tilgan.*

Kalit zo‘zlar: *inqilob jarayoni, kiberpsixologiya, kiberxavfsizlik, kiberhujum, hakerlar, axborot xavfsizligi, tahdidlar, zararli viruslar.*

Абстрактный. *В статье дана информация и рекомендации по концепции киберпсихологии, интернет-угрозам в цифровом пространстве, поддельным ссылкам и сообщениям, защите персональных данных и повышению информационной грамотности пользователей.*

Ключевые слова: *революционный процесс, киберпсихология, кибербезопасность, кибератака, хакеры, информационная безопасность, угрозы, вредоносные вирусы.*

Abstract. *This article provides information and recommendations on the concept of cyberpsychology, online threats in the digital space, fake links and messages, protecting personal data, and increasing information literacy among users.*

Key words: *revolutionary process, cyberpsychology, cybersecurity, cyberattack, hackers, information security, threats, malicious viruses*.

KIRISH

XXI asrda raqamli inqilob jarayoni inson hayotining deyarli barcha sohalariga ta’sir ko‘rsatmoqda. Axborot texnologiyalarining jadal rivojlanishi bilan birga inson psixologiyasida bevosita ta’sir ko‘rsatish imkoniyatlari ham kengaydi. Axborotlarning to‘liq himoyalanmaganligi, yoxud, shaxsiy ma’lumotlarni o‘g’irlash – kiberjoniyatlar soni bugungi kunda oshib bormoqda. Axborot jamiyatida bu kabi muammolar turli yo‘llar bilan yuzaga keladi. Chunki, odamlar keng ko‘lamli va bir xil bo‘lgan axborot mahsulotlaridan foydalanadilar. Masalan, reklamalar, ijtimoiy tarmoqlar (Telegram, Instagram), o‘zaro axborot almashinuvi. Shu sababli, axborot jamiyati muammolarini hal qilishda yangi tadqiqot yondashuviga ehtiyojlar yuzaga kelmoqda.

ADABIYOTLAR TAHLIL VA METODLAR

Kiberpsixologiya – psixologiyaning bir tarmog’i bo‘lib, odamlar tomonidan ijtimoiy xizmatlardan foydalanish turlari, usullari va tamoyillarini o‘rganish metodologiyasi, nazariyasi va amaliyotini birlashtiradi. Kiberpsixologiya zamonaviy jamiyatda muhim rol o‘ynaydi, chunki internet hayotning ajralmas qismiga aylangan. Ushbu soha odamlarning internetdan xavfsiz va samarali foydalanishiga yordam beradi. Kiberpsixologiyaning asosiy yo‘nalishlari:

1. Ijtimoiy tarmoqlarda o‘zini tutish – kiberpsixologiya odamlarning ijtimoiy tarmoqlarda qanday munosabatda bo‘lishini, qanday profil yaratishini, qanday ma’lumotlarni baham ko‘rishini va boshqalarni o‘rganadi.
2. Internetda xatti-harakatlar – ushbu yo‘nalish internetdagi turli xil xatti-harakatlarni, masalan, onlayn xarid qilish, o‘yin o‘ynash, ma’lumot izlash va boshqalarni tahlil qiladi.
3. Kiberbullying va virtual zo‘ravonlik – kiberpsixologiya internetdagi tajovuzkorlik, masalan, kiberbullying, haqoratlash va shantaj kabi holatlarni nazorat qiladi.
4. Onlayn muloqot – kiberpsixologiya odamlarning internet orqali muloqot qilish usullarini, masalan, xabar almashish, video suhbatlar va boshqalarni o‘rganadi.
5. Kiberuzluksizlik va kiberaddiksiya – internetga qaramlik, internetdan haddan tashqari foydalanish va ularning salbiy ta’sirlarini tahlil qiladi.

Axborot-kommunikatsiya texnologiyalarining keskin rivojlanishi natijasida yangi paydo bo‘lgan bu soha insonlarning internet, texnologiyalar, sun’iy intellekt, ijtimoiy tarmoqlar, videoo‘yinlar kabi raqamli muhitdagi xatti-harakatlari, hissiyotlari va psixologik holatlarini o‘rganadi. Umumiy qilib aytganda, kiberpsixologiyaning asosiy maqsadi insonning texnologiyalar bilan sog’lom muvozanatda yashashi, ulardan ortiqcha foydalanmasdan, ruhiy va jismoniy salomatlikni saqlab qolishidir.

Biroq, internet asrida shiddat bilan o‘sib borayotgan jarayon ma’lumotlarni muhofaza qilishni to‘liq ta’minlay olmayapti. Har qanday shaxslarning yoki tashkilotlarning ma’lumotlarini himoya qilish muhim hisoblanadi. Bu borada axborot xavsizligi tushunchasi ilgari suriladi. Axborot xavfsizligi (inglizcha “Information security”) – axborot va tegishli infratuzilmani, shuningdek ma’lumot egalariga yoki foydalanuvchilariga zarar yetkazish bilan bog’liq tasodifiy yoki qasddan ta’sirlardan himoya qilish, ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlashdir. Ilgarigi xavf maxfiy xabar va hujjatlarni o‘g’irlash bo‘lgan bo‘lsa, hozirgi vaqtda asosiy e’tibor shaxsiy ma’lumotlar to‘plamiga qaratilgan. Bundan maqsad, moddiy foyda olish, noqonuniy yo‘l bilan boylik orttirish bo‘lib qolmoqda.

Tahdidlarni quyidagi mezonlar asosida sinflarga ajratish mumkin:

– axborot xavfsizligining asosiy tashkil etuvchilariga nisbatan bo‘ladigan tahdidlar (axborotga murojaat qilish imkoniyatiga qarshi, axborotning yaxlitligini buzishga qaratilgan, axborotning maxfiyligini oshkor qilishga qaratilgan tahdidlar);

– axborot tizimining tashkil etuvchilariga nisbatan bo‘ladigan tahdidlar (berilgan ma’lumotlar, dasturlar, apparat qurilmalari va tizimni qo‘llab quvvatlovchi infrastruktura);

– tahdidni amalga oshirish usuli bo‘yicha (tabiiy, texnogen, tasodifiy, g’arazli maqsadda);

– tahdid manbaining axborot tizimiga nisbatan joylashgan o‘rni bo‘yicha (ichki yoki tashqi).

Hakerlar – avvallari bu so‘z kompyuter dasturlarini tezda yoza oladigan, yoki qurumlarni tezda sozlay oladigan dasturchilarga nisbatan ishlatilgan. Biroq, bugungi kunga kelib, bu jinoyat bilan bog’liq atamalar ro‘yxatiga kiritildi. Ular o‘z manfaatlari yo‘lida lavozimlarini suiste’mol qilishdi. Ular foydalanuvchilarga turli virusli havolalar yuborishadi. Hozirda ular turli nomlar bilan ijtimoiy tarmoqlarda “aylanib yuribdi”. Jumladan, “tug’ilgan kunga/to‘yga taklifnoma”, “majburiy ijrodan xat”, “bu rasmdagi sizmi” kabi bir qancha e’tiborni jalb qiladigan so‘zlar bilan yozilgan bo‘ladi. Bu jarayonda ular mobil qurilmadagi ma’lumotlar bazasiga kirib oladilar. Shundan so‘ng jabrlanuvchilarning shaxsiy bank kartalari, hisob raqamlari, mablag’lari, aloqa kontaktlarini o‘zlashtirib olishadi va virusni butun tarmoqlarga tarqatishadi. Ba’zi hollarda ular notanish raqamlardan qo‘ng’iroq qilib sizning hisob raqamlaringiz haqida ma’lumotlarni aytishadi va kimdir ulanishga harakat qilayotgani haqida ogohlantirish berishadi. Aslida esa bu ularning o‘zlari bo‘lishadi. Shaxslar telefonlariga yuborilgan sms xabarnomasini aytishlari bilan aloqa yakunlanadi va ma’lumotlar egasi haqiqiy qurbonga aylanadi. Bu jarayonda ular mobil qurilmadagi ma’lumotlar bazasiga kirib oladilar. Shundan so‘ng jabrlanuvchilarning shaxsiy ma’lumotlar bazasi va aloqa kontaktlarini o‘zlashtirib, virusni butun tarmoqlarga tarqatishadi.

TAHLIL VA NATIJALAR

Shu o‘rinda kiberxavfsizlikda eng ommalashgan 5 ta zararli dasturlar haqida ma’lumot berib o‘tiladi:

1. Troyan virusi: zararli dasturiy ta’minot turi, foydalanuvchilar fayl zararli bo‘lsa ham, sog‘lom faylni yuklab olyapman deb o‘ylashadi. Fayl bajarilgandan so‘ng, troyan virusi tajovuzkorga jabrlanuvchining tizimiga kirish huquqini berib, ularga ma’lumotlarni o‘g‘irlash yoki ko‘proq zararli dasturlarni o‘rnatish kabi zararli harakatlarni amalga oshirish imkonini beradi.

2. Worm (qurt): o‘zini ko‘paytirish va boshqa tizimlarga yuborish orqali o‘zini tarqatish uchun mo‘ljallangan zararli dastur turi. Qurtlar juda ko‘p zarar yetkazishi mumkin,

chunki ular tez tarqalib, juda ko‘p resurslarni sarflashi mumkin, bu esa tizimlarni ishdan chiqarishi mumkin.

3. Ransomware: ushbu turdagi zararli dastur jabrlanuvchining fayllarini shifrlaydi, so‘ngra fayllar shifrini ochish uchun to‘lovni talab qiladi. Bu jabrlanuvchi uchun juda qimmatga tushadigan hujum bo‘lishi mumkin, chunki ular to‘lovni to‘lamaguncha o‘zlarining asosiy fayllariga kira olmasligi mumkin.

4. Spyware: jabrlanuvchilar haqida ulardan yashirincha ma’lumotlarni to‘plash uchun mo‘ljallangan zararli dastur. Ushbu ma’lumotlar jabrlanuvchini kuzatish yoki uning shaxsini o‘g‘irlash uchun ishlatilishi mumkin.

5. Wiper zararli dasturi: fayllarni o‘chirish yoki tizimni ishlamay qoldirish uchun mo‘ljallangan zararli dastur. Ushbu turdagi zararli dasturlar ko‘pincha tajovuzkor, imkon qadar ko‘proq zarar yetkazmoqchi bo‘lgan hujumlarda qo‘llaniladi.

Himoyalanish bo‘yicha ko‘rsatmalar:

Login va parollarni murakkab tarzda tuzish. Shaxsning axborot kommunikatsiya tizimiga tanishtirish jarayonida qo‘llaniladigan belgilar ketma-ketligi bo‘lib, u qanchalik murakkab bo‘lsa shaxsiy tizimga kirish qiyin kechadi;

Pin-kod raqamlarini ketma-ketligini turli xil raqamlardan tashkil topishi. Hakerlar tomonidan 4 ta bir xil raqamlar ma’lumotlarni o‘g’irlash jarayonini osonlashtiradi va tezlashtiradi. Chunki, ular psixologiyani ham yaxshi bilishadi;

Har bir raqamli parollari turlicha bo‘lishi kerak. Bankdagi hisob raqami, bank kartalarining parollari yoki kirish kodlarining parollari barchasi turlicha bo‘lsin. Agar sizning ma’lumotlaringiz hujumga uchrasa, parollarni topish jarayoni qiyinlashadi;

Autentifikatsiyalash – kompyuter tizimi foydalanuvchisini haqiqiy yoki haqiqiy emasligini aniqlash jarayoni. Bu jarayonda tizim insonning haqiqiyligini aniqlaydi. Identifikatsiyadan farqi shundaki, identifikatsiya jarayonida shaxs yoki tizim foydalanuvchisining kimligi aniqlanadi, autentifikatsiyada esa identifikatsiya qilingan shaxs yoki foydalanuvchining haqiqatan ham o‘sha ekanligini isbotlanadi;

Parollarni imkoni bo‘lsa barmoq usuli orqali himoyalash. Bu nafaqat sizning ma’lumotlaringiz xavfsizligi, balki, o‘zingizda ham ichki xotirjamlikni bildirib turadi;

Ikki bosqichli autentifikatsiyash – Oddiy parolga qo‘shimcha ravishda yana bir tasdiqlovchi bosqich qo‘shiladi. akkauntingizni ikki qatlamda himoya qiladi. Agarda hakerlar sizning kirish parolingizni bilsa ham, akkauntingizga kira olmaydi;

Mobil qurilmangizdagi ilovalarni yangilab turing. Agar sistemangizda nosozlik bo‘lsa, ishlash jarayoni kuchsiz bo‘lsa viruslar o‘rnashishi shunchalik oson kechadi.

XULOSA

Kiberhujumlar kundan-kunga murakkablashmoqda, ammo oddiy qoidalarni muntazam qo‘llash orqali siz o‘zingiz va ma’lumotlaringizni ancha samarali himoya qilishingiz mumkin. Bu asrda zamonaviy axborot xavfsizligi faqat texnik vositalar bilan emas, balki inson omili bilan ham chambarchas bog’liq. O‘zingiz shubhali deb bilgan havolalarni ochmang. Ular “Siz sovrin yutdingiz”, “Tekinga yuting”, “Iphone” yoki “Avtomobil” aksiyasi ishtirokchisiga aylandigiz” kabi mazmunda havolalar, qimmatbaho buyumlar qo‘yilgan tanlovlarda ishtirok etish bo‘yicha taklifnomalar, yoki turli mazmunda apk. fayllari yuborilganda hech qachon ochmang va tarqalishini butkul oldini oling. Ko‘plab kiberhujumlar aynan insonlarning ishonuvchanligi, ehtiyotsizligi yoki psixologik manipulyatsiyaga uchrashi orqali amalga oshiriladi. Axborot xavfsizligi — bu har bir foydalanuvchining mas’uliyati.

Inson psixologiyasi va hissiyotlariga ta’sir qilish imkoniyatidadir: qo‘rqitish, shoshiltirish, yolg‘on ma’lumot bilan chalg‘itish, rasmiylikka o‘xshatish kabi usullar bu jarayonlarda keng qo‘llaniladi. Odamlar e’tiborsizligi, axborot savodsizligi, yoki haddan tashqari ishonuvchanlik kabi holatlar esa bunday hujumlar muvaffaqiyatiga xizmat qiladi. xborot xavfsizligini mustahkamlash texnik vositalar bilan cheklanmasdan, inson omiliga asoslangan yondashuvlarni ham qamrab olishi lozim. Insonlar ishonuvchanligini suiiste’mol qiluvchi tahdidlarga qarshi kurashda eng kuchli qurol — bu xabardorlik va bilimdir.

FOYDALANILGAN ADABIYOTLAR

1. Рахуба О.А “Киберпсихология: возникновение и становление”
2. “Kiberxavfsilikka qarshi yetti tahdid”. Orifjon Dusyarov. Xabar.uz
3. “Axborot xavfsizligiga bo‘ladigan tahdidlar”. Akbarova M.R. “Экономика и социум” №6(85) 2021
4. Wikipediya.uz Autentifikatsiya