KIBERXAVFSIZLIK MUAMMOLARI VA YECHIMLARI

Norqobilov Hakimbek Nuriddin o'g'li
Termiz pedagogika instituti
matematika va informatika kafedrasi o'qituvchisi
norqobilovhakimbek98@gmail.com

Annotatsiya: Ushbu tezisda kiberxavfsizlik muammolari ko'rib chiqilib, zamonaviy raqamli muhitda duch kelinadigan eng ko'zga ko'ringan tahdidlar va ularning natijalari tahlil qilinadi. Shuningdek, individual va korporativ foydalanuvchilar, davlat organlari uchun amaliy yechimlar va profilaktik choralar taklif etiladi. Maqolada texnik, tashkilotchi va huquqiy tomonlar uyg'unligi, malaka oshirish va xalqaro hamkorlik zarurligi xususida asosli fikrlar bayon etilgan.

Kalit so'zlar: Kiberxavfsizlik, axborot xavfsizligi, zararli dasturlar, fishing, DDoS, kiberhujumlar, shifrlash, foydalanuvchi hushyorligi, milliy xavfsizlik.

Asosiy qism. Raqamli texnologiyalar hayotimizning ajralmas qismiga aylangan sari axborot va kommunikatsiya tizimlarining xavfsizligi muammosi tobora kuchayib bormoqda. Kundalik faoliyatimiz, moliyaviy operatsiyalarimiz, sog'liqni saqlash ma'lumotlarimiz va davlat boshqaruvi tizimlari — barchasi algoritmlar, serverlar va tarmoqlar orqali amalga oshadi. Shu holat esa ma'lumotlar bilan bog'liq yangi zaifliklarni yuzaga chiqaradi: noxush niyatli shaxslar va guruhlar ma'lumotni o'g'irlash, tizimlarni buzish yoki jamoatchilik ishonchini so'ndirishga yo'naltirilgan turli hujumlarni amalga oshirish imkoniyatiga ega bo'ladi. Kiberxavfsizlik masalasini faqat texnik kasalliklar spektri sifatida ko'rmaslik kerak. Bu, avvalo, inson, tashkilot va davlat darajalarida kompleks yondashuvni talab etadi. Shaxsiy darajada oddiy, lekin samarali qoidalarga rioya qilish — kuchli va noyob parollardan foydalanish, ikki faktorli autentifikatsiyani (2FA) yoqish, operatsion tizim va ilovalarni vaqtida yangilab borish, shubhali havolalardan saqlanish — foydalanuvchini ko'plab muammolardan himoya qiladi. Korporativ bo'lsa, bu masala siyosat, protsedura va texnologiyalar uyg'unligidan iborat: ma'lumotlarga kirishni boshqarish, tizimli xavfsizlik auditlari, uzluksiz monitoring va hodisalar yuz berganda tezkor javob berish mexanizmi bo'lishi lozim.

Zararli dasturlar — bugungi kunda eng ko'p tarqalgan tahdidlardan biri. Viruslar, troyanlar va ransomware (ma'lumotlarni shifrlash orqali haq talab qiluvchi) kabi kodlar korxona yoki shaxsiy kompyuterlar ichiga kirib, ma'lumotlarni bloklashi yoki ochiq-ochiq o'g'irlashi mumkin. Ransomware hujumlari ayniqsa zararli: tibbiyot muassasalari, energetika va moliya sohasidagi tashkilotlar faoliyatini bir necha soat yoki kun davomida to'xtatib qo'yishi mumkin. Shu sababli muntazam zaxiralash

siyosati, ma’lumotlarni offlayn yoki ishonchli bulut xizmati orqali saqlash, hamda ma’lumotlarga kirishni qattiq nazorat qilish kabi choralar zarur.

Fishing — juda oddiy, ammo samarali uslub. Soxta elektron pochta xabarlari, SMS yoki ijtimoiy tarmoqlar orqali yuboriladigan havolalar orqali foydalanuvchilardan login yoki moliyaviy ma’lumotlarni olishga urinishlar kundalikda uchraydi. Ushbu xurujlar bilan kurashish uchun tashkilotlar o‘z xodimlarini muntazam o‘qitishi, soxtalashtirilgan xabarlardan himoyalovchi filtr tizimlarini joriy etishi hamda muomalada shaxsiy ma’lumotlarni talab qiladigan resurslarni rasmiy manbalardan tekshirishni odat qilib olishlari kerak. DDoS hujumlari esa xizmatlarning mavjudligini yo‘qotishga qaratilgan. Internet-resurslarga sun’iy ravishda ortiqcha so‘rovlar yuborilib, ular resurslari band qilinadi. Bu turdagi xurujlar natijasida xizmat ko‘rsatuvchi tashkilotlar mijozlarni yo‘qotishi, biznes jarayonlar uzilishi va obro‘-e’tibor zarar ko‘rishi mumkin. Muqobil yechimlar: yukni tarqatish (load balancing), kontentni yetkazib berish tarmoqlari (CDN), va zarur bo‘lsa bulut asosidagi himoya xizmatlarini jalb etish.

Kiberhujumlarning yagona texnik yo‘nalishi bilan cheklanib qolmasligi hamda ular ijtimoiy va siyosiy oqibatlarga olib kelishi muhim. Davlatlararo kiberhujumlar, kiberterrorizm va axborot urushi kontseptsiyalari mavjud bo‘lib, ular strategik infratuzilmalar — energetika, transport, moliya va sog‘liqni saqlash tizimlariga zarar yetkazishi mumkin. Shu boisdan milliy darajada kiberxavfsizlik siyosatini ishlab chiqish va mustahkamlash lozim. Bu siyosatda qonunchilik, standartlar, krytografik talablar va favqulodda vaziyatlarga javob protokollari aniq belgilanishi kerak.

Innovatsion yondashuvlar bilan ham samarani oshirish mumkin. Sun’iy intellekt va mashinaviy o‘rganish texnologiyalari yordamida anomaliyalarning onlayn aniqlanishi, tahdidlarni oldindan bashorat qilish va avtomatlashtirilgan javob mexanizmlari joriy etilmoqda. Blokcheyn texnologiyalari esa ma’lumotlarning butligini ta’minlash va tranzaksiyalarni manipulyatsiyadan himoya qilishda foydali bo‘lishi mumkin. Biroq bunday texnologiyalarni qo‘llashda ham xatarlarga e’tibor qaratish talab etiladi: masalan, sun’iy intellektni hujumni o‘rganish va javobni optimallashtirish uchun ishlatish mumkin, lekin tizimni o‘ziga xos zaifliklardan himoya qilish zarur.

Kiberxavfsizlik sohasida inson kapitalini rivojlantirish muhim omil hisoblanadi. Mutaxassislar yetishmovchiligi ko‘plab mamlakatlarda jiddiy muammo. Shu bois, ta’lim muassasalari va kasb-hunar markazlarida axborot xavfsizligi bo‘yicha kurslar, amaliy mashg‘ulotlar va qayta tayyorlash dasturlari kengaytirilishi kerak. Korxonalar esa o‘z xodimlarini muntazam o‘qitib, inkubatsiya va stajirovka dasturlari orqali yangi iste’dodlarni o‘z tizimiga jalb etishi lozim.

Milliy va xalqaro hamkorlik ham samarali kurashda muhim rol o‘ynaydi. Kiberxavfsizlik tahdidlarining ko‘plab holatlari chegaradan oshib ketadi; shu sababli

tajriba almashish, umumiy standartlar va favqulodda vaziyatlarda tezkor ma’lumot almashish mexanizmlarini yaratish zarur. Davlatlararo lug‘atlar va normativ hujjatlar, shuningdek, xususiy sektor va nodavlat tashkilotlar ishtirokida jamoaviy himoya choralari ishlab chiqilishi kerak. Amaliy jihatdan, tashkilotlar uchun tavsiya etiladigan asosiy qadamlar quyidagilar: xavfni baholash va yillik auditlarni joriy etish; ma’lumotlarga kirishni qat’iy boshqarish; ma’lumotlarni shifrlash va zaxiralash; hodisa yuz berganda tezkor javob berish guruhini tayyorlash; va xodimlarni muntazam ravishda xavfsizlik bo‘yicha o‘qitish. Shuningdek, shaffof kommunikatsiya siyasati ham muhim: agar xuruj sodir bo‘lsa, tashkilot mijozlar va regulyatorlarga holat haqida jo‘natma berishi, hamda vaziyatni bartaraf etish bo‘yicha chora-tadbirlarni ommaga tushuntirishi zarur.

Xulosa

Xulosa qilib aytganda, kiberxavfsizlik — bu doimiy e’tibor va resurs talab qiladigan jarayon. Texnologiyalar tez o‘zgararkan, tahdidlar ham rivojlanadi; biroq asosiy tamoyillar — oldindan tayyorgarlik, inson omilini kuchaytirish, zamonaviy texnologiyalardan oqilona foydalanish va xalqaro hamkorlik — barqaror natijalar beradi. Raqamli dunyoning imkoniyatlaridan xavfsiz foydalanish istagida bo‘lgan jamiyat va tashkilotlar uchun bu omillar birgalikda ishlashi muhimdir.

Foydalanilgan adabiyotlar ro‘yxati:

1. To‘rayev Sh., Qodirova M., “Axborot xavfsizligi asoslari”, Toshkent, Universitet nashriyoti, 2021.
2. Shukurov U., “Kiberxavfsizlik va zamonaviy tahdidlar”, Innovatsiya nashriyoti, 2020.
3.Schneier B., “Applied Cryptography”, Wiley, 2015.
4.West D., “Cybersecurity and National Security”, Brookings Institution Press, 2018.
5.O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi rasmiy sayti (mitc.uz).
6.Kaspersky va Symantec kompaniyalarining yillik tahdidlar hisobotlari.