KIBERXAVFSIZLIK ASOSLARI VA UNING ZAMONAVIY MUAMMOLARI

Salayeva Dilnoza Mirzaqulovna
Jizzax ilg‘or kasbiy mahorat texnikumi
Informatika fani o‘qituvchisi
Qayumova Yulduz Toxirovna
Jizzax ilg‘or kasbiy mahorat texnikumi
Informatika fani o‘qituvchisi
Shodmonqulova Muxabat Rustam qizi
Jizzax ilg‘or kasbiy mahorat texnikumi
Informatika fani o‘qituvchisi

Mavzuning dolzarbligi. Hozirgi kunda jahon miqyosida raqamli texnologiyalar, sun'iy intellekt va internet tarmoqlarining shiddat bilan rivojlanishi insoniyat hayotini tubdan o‘zgartirib yubordi. Axborot kommunikatsiya texnologiyalari (AKT) iqtisodiyot, ta'lim, sog‘liqni saqlash, moliya va davlat boshqaruvining barcha jabhalariga chuqur kirib bordi. Biroq, ushbu global raqamlashuv jarayoni o‘zi bilan birga katta xavf-xatarlarni ham olib keldi. Bugungi kunda kiberjinoyatchilik global muammoga aylanib, nafaqat yirik kompaniyalar, balki oddiy fuqarolarning ham xavfsizligiga tahdid solmoqda.

Shu sababli, kiberxavfsizlikni ta'minlash, shaxsiy va korporativ ma'lumotlarni himoya qilish hamda raqamli gigiyena qoidalariga rioya qilish har bir davlat va shaxs oldida turgan eng muhim vazifalardan biridir. Ushbu loyiha kiberxavfsizlikning nazariy va amaliy jihatlarini ochib berishga qaratilgan.

Ishning maqsadi:

Kiberxavfsizlik tushunchasi va uning asosiy tamoyillarini o‘rganish;

Zamondagi asosiy kibertahdidlar va ularning keltirib chiqaradigan oqibatlarini tahlil qilish;

Axborotni muhofaza qilish usullari va zamonaviy himoya vositalarini yoritib berish.

1-BOB. KIBERXAVFSIZLIKNING NAZARIY ASOSLARI

1.1. Kiberxavfsizlik tushunchasi va uning kelib chiqish tarixi

Kiberxavfsizlik (Cybersecurity) — kompyuter tizimlari, tarmoqlar, dasturiy ta'minotlar va raqamli ma'lumotlarni ruxsat etilmagan kirish, o‘zgartirish, yo‘q qilish yoki shikastlanishdan himoya qilishga qaratilgan texnologiyalar, jarayonlar va amaliyotlar majmui hisoblanadi.

Internet dastlab ilmiy va harbiy maqsadlarda yaratilgan davrlarda xavfsizlik masalalari bu qadar keskin turmagan edi. Biroq tarmoq kengayib, tijorat maqsadlariga xizmat qilisha boshlagach, ma'lumotlarni o‘g‘irlash va tizimlarni ishdan chiqarish holatlari keskin ko‘paydi. Natijada alohida fan va amaliyot sifatida kiberxavfsizlik sohasi shakllandi.

1.2. Kiberxavfsizlikning asosiy uchligi — CIA triadasi

Axborot xavfsizligining poydevori sifatida "CIA triad" (Confidentiality, Integrity, Availability) konsepsiyasi qo‘llaniladi:

Maxfiylik (Confidentiality): Ma'lumotlarga faqatgina tegishli vakolatga ega bo‘lgan shaxslargina kirishini ta'minlash. Maxfiy ma'lumotlarning begona shaxslarga sizib chiqishining oldini olish.

Butunlik (Integrity): Ma'lumotlarning aniqligi, to‘g‘riligi va ularning ruxsatsiz o‘zgartirilishidan yoki soxtalashtirilishidan himoya qilinganligi.

Mavjudlik (Availability): Foydalanuvchilar kerakli paytda ma'lumotlar va tizim resurslaridan to‘liq foydalanish imkoniyatiga ega bo‘lishini kafolatlash (masalan, DDoS hujumlari aynan mavjudlikka qarshi qaratilgan bo‘ladi).

2-BOB. ZAMONAVIY KIBERTAHDIDLAR VA XAVFLAR

2.1. Fishing (Phishing) va ijtimoiy muhandislik

Zamonavimizda kiberjinoyatchilar faqatgina texnik usullardan emas, balki inson omilidan foydalangan holda hujum qilishni afzal ko‘rmoqdalar. Ijtimoiy muhandislik (Social Engineering) insonlarni aldash, ularda qo‘rquv yoki ishonch uyg‘otish orqali kerakli ma'lumotlarni (parollar, bank kartasi raqamlari) qo‘lga kiritishga asoslangan.

Fishing — bu soxta saytlar, xabarlar yoki elektron xatlar orqali foydalanuvchilarni aldab, shaxsiy ma'lumotlarini shilib olish usulidir. Ko‘pincha mashhur bank yoki servis niqobi ostida yuboriladi.

2.2. Zararli dasturlar (Malware)

Kompyuter tizimlariga zarar yetkazish uchun yaratilgan dasturlar quyidagi turlarga bo‘linadi:

Virus va troyanlar: Tizimga yashirincha kirib, fayllarni buzadi yoki ma'lumotlarni o‘g‘irlaydi.

Ransomvar (Ransomware): Foydalanuvchining barcha fayllarini shifrlab qo‘yadi va ularni ochish uchun tovon puli (kutubxona yoki kriptovalyuta orqali) talab qiladi.

Josus dasturlar (Spyware): Foydalanuvchining klaviaturada tergan matnlarini yoki ekranidagi ma'lumotlarni kuzatib boradi.

3-BOB. AXBOROTNI MUHOFAZA QILISH VA HIMOYA VOSITALARI

3.1. Texnik himoya choralari

Tizimlarni himoya qilish uchun quyidagi texnika va dasturiy vositalar qo‘llaniladi:

Fayrvollar (Firewalls): Tarmoq trafigini nazorat qiluvchi va shubhali ulanishlarni to‘sib qo‘yuvchi to‘siqlar.

Antivirus tizimlari: Zararli dasturlarni o‘z vaqtida aniqlab, yo‘q qiluvchi vositalar.

Shifrlash (Encryption): Ma'lumotlarni maxsus algoritmlar asosida o‘zgartirib, begona shaxslar o‘qiy olmaydigan holatga keltirish.

3.2. Tashkiliy va shaxsiy himoya qoidalari

Har bir foydalanuvchi rioya qilishi lozim bo‘lgan qoidalar:

Kuchli parollardan foydalanish: Har bir hisob uchun har xil, uzun va murakkab (harflar, raqamlar va maxsus belgilar qatnashgan) parollar yaratish.

Ikki bosqichli autentifikatsiya (2FA): Hisobga kirishda qo‘shimcha ravishda SMS kod yoki maxsus dastur tasdiqini talab qilishni yoqib qo‘yish.

Dasturiy ta'minotni yangilab borish: Operatsion tizim va barcha dasturlarning so‘nggi xavfsizlik yangilanishlarini o‘rnatish.

XULOSA

Xulosa qilib aytganda, kiberxavfsizlik zamonaviy dunyoda har bir inson, tashkilot va davlatning barqaror faoliyat yuritishining asosiy kafolati hisoblanadi. Texnologiyalar rivojlangani sayin kibertahdidlar ham murakkablashib bormoqda.

Shu bois, kibermakonda hushyorlikni oshirish, raqamli savodxonlikni keng targ‘ib qilish hamda muhofaza choralarini o‘z vaqtida ko‘rish barchamizning burchimizdir.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

O‘zbekiston Respublikasining «Kiberxavfsizlik to‘g‘risida»gi Qonuni. Toshkent, 2022-yil.

Karimov I.A. *«Yuksak intellektual avlodni tarbiyalash — mamlakat taraqqiyotining garovi»*. Toshkent: «O‘zbekiston», 2018.

Raxmonov S.X. *«Axborot xavfsizligi asoslari»*. O‘quv qo‘llanma. Toshkent, 2023.

Stallings W. *«Computer Security: Principles and Practice»*. Pearson, 2020.

Rasmiy internet resurs:www.gov.uz