KIBERXAVFSIZLIK VA RAQAMLI MA'LUMOTLARNI HIMOYA QILISHDA ZAMONAVIY YONDASHUVLAR

Abdumannonova Guljahon Iqboljon qizi
guljahonabdumannonova@gmail.com
Farg`ona Davlat Universiteti
Filologiya va tillarni o`qitish chet tillari fakulteti
24.108-guruh talabasi

Annotatsiya. Ushbu maqolada kiberxavfsizlikning asosiy tushunchalari, hozirgi zamon raqamli tahdidlarining turlari va ularga qarshi kurashishda qo‘llanilayotgan zamonaviy texnologiyalar ko‘rib chiqiladi. Shuningdek, shaxsiy va korporativ ma’lumotlarni himoya qilish usullari tahlil qilinadi. Kiber makonda xavfsizlikni ta’minlashda sun’iy intellekt, kriptografiya, “Zero Trust” arxitekturasi kabi yangi texnologik yondashuvlar o‘rganiladi.

Kalit so`zlar: kiberxavfsizlik, raqamli tahdidlar, axborot xavfsizligi, ma’lumotlarni himoya qilish, sun’iy intellekt, kriptografiya.

Annotation. This article explores the fundamental concepts of cybersecurity, the types of modern digital threats, and the advanced technologies used to combat them. It also analyzes methods of protecting personal and corporate data. The study examines new technological approaches such as artificial intelligence, cryptography, and Zero Trust architecture to ensure security in cyberspace.

Keywords: cybersecurity, digital threats, information security, data protection, artificial intelligence, cryptography.

Kirish

Raqamli inqilob jamiyatning barcha sohalariga ta’sir ko‘rsatmoqda. Ayniqsa, axborot texnologiyalarining jadal rivojlanishi kiber makonda yangi muammolarni yuzaga keltirdi. Bugungi kunda kiberxavfsizlik nafaqat texnik muammo, balki ijtimoiy, iqtisodiy va siyosiy masala sifatida ham qaralmoqda.

Axborot texnologiyalaridan foydalanuvchi har bir foydalanuvchi – xoh jismoniy, xoh yuridik shaxs bo‘lsin – o‘zining raqamli ma’lumotlarini himoya qilish zaruriyatini his qilmoqda. Ma’lumotlarning yo‘qolishi, o‘g‘irlanishi yoki o‘zgartirilishi nafaqat alohida foydalanuvchiga, balki butun tizimga jiddiy zarar yetkazishi mumkin. Shu sababli, zamonaviy axborot muhitida xavfsizlik masalalari birinchi darajali ahamiyat kasb etmoqda.

Kiberxavfsizlikning asosiy maqsadi – raqamli ma’lumotlarning butligini, maxfiyligini va mavjudligini ta’minlashdir. Hozirgi paytda kiber tahdidlar turlicha

ko‘rinishda yuzaga chiqmoqda va ularning oldini olish uchun yangidan-yangi texnologik yondashuvlar talab etiladi.

Kiberxavfsizlik tushunchasi va muammolari

Kiberxavfsizlik — bu kompyuter tizimlari, tarmoqlar, dasturiy ta'minot va foydalanuvchilarni raqamli tahdidlardan, ya'ni zararli harakatlar, ruxsatsiz kirishlar, ma’lumotlarni o‘g‘irlash yoki yo‘qotish kabi holatlardan himoya qilishga qaratilgan chora-tadbirlar majmuidir. Bu atama ko‘p hollarda “axborot xavfsizligi” bilan sinonim tarzda ishlatiladi, biroq kiberxavfsizlik ko‘proq raqamli muhitga tegishli bo‘lgan xavflarga nisbatan qo‘llaniladi.

Kiberxavfsizlik masalasi tobora dolzarb bo‘lib bormoqda. Bunga sabab — internet tarmog‘ining kengayishi, korxona va tashkilotlarning raqamli platformalarga o‘tishi, hamda onlayn xizmatlardan foydalanishning ortib borayotganidir. Ayniqsa, moliyaviy xizmatlar, sog‘liqni saqlash tizimlari, ta’lim platformalari va davlat boshqaruvi tizimlarida raqamli xavfsizlik yuqori ahamiyatli.

Jahon banki va boshqa xalqaro tashkilotlarning ma’lumotlariga ko‘ra, har yili kiberjinoyatlar natijasida yuzaga keladigan moddiy zararlar milliardlab dollarni tashkil qiladi. McAfee va Center for Strategic and International Studies (CSIS) hisobotlariga ko‘ra, global iqtisodiyotga kiberhujumlar 1 trillion dollarga yaqin zarar yetkazmoqda.

Kiberjinoyatchilar tomonidan qo‘llaniladigan vositalar va uslublar tobora murakkablashib bormoqda. Endilikda oddiy zararli dasturlar bilan emas, balki sun’iy intellekt yordami bilan avtomatlashtirilgan hujumlar ham sodir etilmoqda. Natijada an’anaviy himoya vositalari, masalan, faqatgina antivirus dasturlari yoki parollar orqali himoya qilish, endilikda yetarli darajada samarali emas.

Yana bir jiddiy muammo – foydalanuvchilarning axborot xavfsizligi madaniyatining yetarli darajada shakllanmaganidir. Ko‘pchilik oddiy parollar ishlatadi, noma’lum manbalardan havolalarni ochadi, shaxsiy ma’lumotlarni osonlik bilan tarqatadi. Bu esa kiberjinoyatchilarning ishini yengillashtiradi.

Kiberxavf turlari va ularning xususiyatlari

Kiberxavf — bu raqamli infratuzilmaga tahdid soluvchi har qanday zararli harakat yoki xatti-harakatdir. Kiberxavf turlarining xilma-xilligi sababli ularga qarshi kurashish jarayoni ham murakkab va keng qamrovli bo‘lishi lozim. Quyida eng ko‘p uchraydigan va xavfli hisoblangan tahdid turlari keltirilgan:

1.Phishing (soxtalashtirish)

Phishing — foydalanuvchini aldash yo‘li bilan uning maxfiy ma’lumotlarini (login, parol, bank kartasi rekvizitlari) qo‘lga kiritishga qaratilgan hujumdir. Ko‘pincha elektron pochta orqali yuborilgan soxta xabarlar yordamida amalga oshiriladi. Foydalanuvchi uni rasmiy tashkilotdan kelgan deb o‘ylab, havolaga bosadi yoki ma’lumot kiritadi, natijada ularning ma’lumotlari jinoyatchilar qo‘lida.

2.DDoS (Distributed Denial of Service) hujumlar

DDoS hujumlar — server yoki tarmoq resurslarini haddan tashqari yuklash orqali ularni ishdan chiqarishga qaratilgan hujumlardir. Ular ko‘pincha turli manbalardan bir vaqtning o‘zida amalga oshiriladi. Bunday hujumlar kompaniyalar uchun katta moliyaviy yo‘qotishlarga olib keladi, chunki xizmatlar vaqtincha to‘xtab qoladi.

3.Zararli dasturlar (Malware)

Zararli dasturlar — foydalanuvchining ruxsatisiz qurilmaga o‘rnatilib, unga zarar yetkazuvchi yoki maxfiy ma’lumotlarni o‘g‘irlaydigan dasturlar turidir. Ular orasida viruslar, trojanlar, shpion dasturlar (spyware), reklama dasturlari (adware) mavjud. Malware orqali foydalanuvchi nazoratisiz qurilmaning ishlashiga aralashish mumkin bo‘ladi.

4.Ransomware (talabnoma dasturlar)

Ransomware — foydalanuvchining fayllarini shifrlab, ularga kirishni cheklaydi va ularni tiklash evaziga pul talab qiladi. Bu eng xavfli kiber tahdidlardan biri bo‘lib, aksariyat hollarda shifrlangan ma’lumotni tiklashning iloji bo‘lmaydi. Bunday dasturlar odatda pochta orqali yoki soxta dastur ko‘rinishida tarqatiladi.

5.SQL Injection

Bu hujum turi veb-ilovalarda mavjud bo‘lgan zaiflikdan foydalangan holda, ma’lumotlar bazasiga zarar yetkazish yoki undan ma’lumotlarni noqonuniy tarzda olish imkonini beradi. Bu hujumlar asosan xavfsizlik choralarini noto‘g‘ri joriy qilgan veb-saytlarda sodir bo‘ladi.

6.Inside threat (Ichki tahdid)

Bu kompaniya yoki tashkilot ichidagi xodimlar hayotidagi xavflardir.

Himoya qilishda qo`llanilayotgan texnologiyalar

Kiberxavfsizlikka qarshi samarali kurash hozirgi kunda bir nechta zamonaviy texnologiyalar yordamida olib boriladi. Quyida eng muhim to‘rt yondashuv tavsiflangan:

1.Sun’iy intellekt va mashinaviy o‘qitish

Sun’iy intellekt (AI) va mashinaviy o‘qitish (ML) xavfli xatti-harakatlarni avtomatik aniqlash va ularga munosabat bildirishni sezilarli darajada tezlashtiradi. ML modellari tarmoq trafigidagi anomaliyalarni o‘rganib, normal holatdan chetga chiqadigan naqshlarni aniqlaydi. Masalan, foydalanuvchining odatdagi login vaqtlari, joylashuvi yoki ma’lumotlarga kirish usullari tahlil qilib, shubhali kirishlarga darhol signal beradi.

2.Kriptografik algoritmlar

Ma’lumotlarni himoya qilishning eng ishonchli usullaridan biri – kuchli kriptografiya. Simmetrik algoritmlar (AES, Snowflake) va assimmetrik algoritmlar (RSA, ECC) ma’lumotlarni kodlab, ruxsatsiz shaxslar uchun foydasiz holga keltiradi.

Shuningdek, ma’lumotlarga kirishni nazorat qilish uchun raqamli imzolar va sertifikatlash tizimlari amal qiladi, bu esa ma’lumot manbasini va yaxlitligini kafolatlaydi.

3.Bulutli xavfsizlik xizmatlari

Katta korxonalar va tashkilotlar uchun “Bulutda xavfsizlik” (Security as a Service) modeli mashhur bo‘lmoqda. Bu yondashuvda real vaqtda tarmoq trafigi skanerlash, hujumni oldindan aniqlash, DDoS himoyasi va avtomatik yangilanish kabi xizmatlar bulut provayder tomonidan ta’minlanadi. S.hu tarzda kompaniyaning ichki infratuzilmasiga kamroq sarmoya kiritib, doimiy yangilanadigan himoya darajasi saqlanadi.

4. Zero Trust arxitekturasi

“Zero Trust” tamoyili bo‘yicha har bir kirish so‘rovi avtomatik tarzda tekshiriladi — ichki tarmoqlar va foydalanuvchilar bundan mustasno emas. Har bir foydalanuvchi va qurilma kirish huquqi cheklangan “kam huquqli” formatda beriladi, hamda doimiy autentifikatsiya, kirish siyosati va konteksual baholash orqali ruxsat yoki rad qarori qabul qilinadi. Bu uslub eski “ichkarida — ishon — tashqarida — tekshir” tamoyilidan qat’iy ozod bo‘lib, zamonaviy tahdidlarga nisbatan ancha chidamli.

Xulosa

Ushbu maqolada kiberxavfsizlikning zamonaviy yondashuvlari orqali raqamli ma’lumotlarni himoya qilish masalalari keng qamrovda ko‘rib chiqildi. Avvalo, kiberxavfsizlik tushunchasi va u bilan bog‘liq muammolar tahlil qilindi, so‘ngra phishing, DDoS, malware, ransomware, SQL Injection va ichki tahdid kabi asosiy kiberxavf turlari yoritildi. Himoya vositalari sifatida sun’iy intellekt va mashinaviy o‘qitish, kuchli kriptografik algoritmlar, bulutli xavfsizlik xizmatlari hamda Zero Trust arxitekturasi taqdim etildi. O‘zbekiston misolida esa huquqiy bazaning mustahkamlanishi, “Raqamli O‘zbekiston – 2030” strategiyasi, yagona integratsiyalashgan axborot tizimi va kadrlar tayyorlash bo‘yicha amalga oshirilayotgan chora-tadbirlar muhokama qilindi.

Kelajakda kiberxavfsizlikni yanada takomillashtirish uchun: mahalliy kadrlar malakasini oshirish va xalqaro sertifikatlash dasturlarini kengaytirish, kichik va o`rta biznes sub’ektlariga subsidiyalangan xavfsizlik yechimlarini taklif etish, aholining axborot xavfsizligi madaniyatini rivojlantirish bo`yicha keng ko`lamli ma`rifiy kompaniyalarni tashkil etish zarur.

Foydalanilgan adabiyotlar:

1. Schneier, B. (2020). Applied Cryptography. Wiley.

2. Stallings, W. (2021). Network Security Essentials. Pearson.
3. O‘zbekiston Respublikasi “Kiberxavfsizlik to‘g‘risida”gi Qonuni (2020).
4. Cybintsolutions.com. (2024). Global Cybersecurity Statistics.
5. Lex.uz. (2020). O‘zbekiston Respublikasi Qonun hujjatlari ma’lumotlar bazasi.