KIBERXAVFSIZLIK: RAQAMLI MUHITDA AXBOROTNI HIMOYA QILISHNING NAZARIY ASOSLARI, ZAMONAVIY TAHDIDLAR VA YECHIMLAR

UO‘K (UDK): 004.056

Muallif: Yunusov Jo`rabek Bahodirjon o`g`li
Lavozimi / ta’lim darajasi: `O`qituvchi/ Oliy ma`lumotli
Tashkilot: O`zbekiston tuman 4-sonli texnikum, Umumta`lim fanlar kafedrasi
Manzil: Farg`ona Viloyati O‘zbekiston tumani

Annotatsiya

Mazkur maqolada kiberxavfsizlikning nazariy asoslari, axborot xavfsizligining asosiy tamoyillari, zamonaviy kiberxavflar turlari va ularga qarshi qo‘llaniladigan texnik, tashkiliy hamda huquqiy himoya choralari tahlil qilinadi. Shuningdek, O‘zbekistonda kiberxavfsizlik sohasidagi qonunchilik asoslari, xalqaro standartlar va foydalanuvchilar uchun amaliy tavsiyalar yoritilgan. Tadqiqot natijalari axborot tizimlarini himoya qilishda kompleks yondashuv, doimiy monitoring va raqamli savodxonlikni oshirish muhimligini ko‘rsatadi.

Kalit so‘zlar: kiberxavfsizlik, axborot xavfsizligi, kiberhujum, fishing, zararli dastur, shifrlash, ikki bosqichli autentifikatsiya, nol ishonch modeli, raqamli savodxonlik.

Аннотация

В статье рассматриваются теоретические основы кибербезопасности, принципы информационной безопасности, современные киберугрозы, а также технические, организационные и правовые методы защиты. Отдельно рассмотрены законодательная база Узбекистана, международные стандарты и практические рекомендации для пользователей.

Ключевые слова: кибербезопасность, информационная безопасность,

кибератака, фишинг, вредоносное ПО, шифрование, двухфакторная аутентификация, модель «нулевого доверия», цифровая грамотность.

Abstract

This article examines the theoretical foundations of cybersecurity, core principles of information security, modern cyber threats, and the technical, organizational and legal measures used to counter them. It also reviews the legal framework of Uzbekistan, international standards and practical recommendations for users. The findings show that protecting information systems requires an integrated approach, continuous monitoring and improved digital literacy.

Keywords: cybersecurity, information security, cyberattack, phishing, malware, encryption, multi-factor authentication, zero trust, digital literacy.

Kirish

Raqamli texnologiyalarning jadal rivojlanishi jamiyat hayotining barcha sohalarini — davlat boshqaruvi, moliya, ta’lim, sog‘liqni saqlash, energetika va transportni — axborot tizimlariga bog‘liq qilib qo‘ydi. Bu bog‘liqlik katta imkoniyatlar bilan birga yangi xavflarni ham keltirib chiqardi. Kiberhujumlar natijasida shaxsiy ma’lumotlar oshkor bo‘lishi, moliyaviy yo‘qotishlar yuz berishi, muhim infratuzilma faoliyati to‘xtashi va tashkilotlarning obro‘siga zarar yetishi mumkin.

Shu bois kiberxavfsizlik bugungi kunda alohida texnik soha emas, balki milliy xavfsizlikning ajralmas qismi sifatida qaralmoqda. O‘zbekistonda ham raqamlashtirish jarayonlarining kengayishi, elektron davlat xizmatlari va onlayn to‘lov tizimlarining ommalashishi axborot xavfsizligini ta’minlash masalasini dolzarb qilib qo‘ymoqda.

Tadqiqotning maqsadi — kiberxavfsizlikning asosiy tushunchalari, zamonaviy tahdidlar va himoya usullarini tizimli tahlil qilish hamda amaliy tavsiyalar ishlab chiqish.

Tadqiqotning vazifalari:

kiberxavfsizlik va axborot xavfsizligi tushunchalarining mohiyatini aniqlash;

zamonaviy kiberhujum turlarini tasniflash;

himoya choralarini texnik, tashkiliy va huquqiy jihatdan ko‘rib chiqish;

O‘zbekiston va xalqaro tajribani tahlil qilish;

foydalanuvchi va tashkilotlar uchun amaliy tavsiyalar berish.

Tadqiqot usullari: ilmiy adabiyotlar va me’yoriy hujjatlarni tahlil qilish, qiyosiy tahlil, tizimli yondashuv, umumlashtirish.

1. Kiberxavfsizlikning nazariy asoslari

1.1. Asosiy tushunchalar

Axborot xavfsizligi — axborotning maxfiyligi, yaxlitligi va foydalanuvchanligini har qanday ruxsatsiz kirish, o‘zgartirish, yo‘q qilish yoki oshkor qilishdan himoya qilish holati. **Kiberxavfsizlik** esa shu himoyaning raqamli muhitga, ya’ni kompyuter tizimlari, tarmoqlar, dasturlar va ma’lumotlarga yo‘naltirilgan qismidir. Amalda bu ikki atama ko‘pincha bir-birini to‘ldiruvchi ma’noda ishlatiladi.

1.2. CIA triadasi

Axborot xavfsizligining klassik modeli uchta asosiy tamoyilga tayanadi (1-jadval).

1-jadval. Axborot xavfsizligining asosiy tamoyillari (CIA triadasi)

Tamoyil	Mohiyati	Buzilish misoli
Maxfiylik (Confidentiality)	Axborotga faqat vakolatli shaxslar kira oladi	Ma’lumotlar bazasining o‘g‘irlanishi
Yaxlitlik (Integrity)	Axborot ruxsatsiz o‘zgartirilmaydi, to‘liq va aniq saqlanadi	Hisob raqamidagi summaning yashirincha o‘zgartirilishi
Foydalanuvchanlik (Availability)	Axborot kerak vaqtda mavjud bo‘ladi	DDoS hujumi tufayli saytning ishlamay qolishi

Qo‘shimcha ravishda autentifikatsiya, avtorizatsiya va inkor etib bo‘lmaslik

(non-repudiation) tamoyillari ham muhim hisoblanadi.

1.3. Tahdid, zaiflik va xavf tushunchalari

Tahdid — tizimga zarar yetkazishi mumkin bo‘lgan potensial hodisa yoki shaxs.

Zaiflik — tizim, dastur yoki jarayondagi kamchilik bo‘lib, undan tahdid foydalanishi mumkin.

Xavf — tahdidning zaiflikdan foydalanib zarar yetkazish ehtimoli va uning oqibati.

Xavfni boshqarish jarayoni aktivlarni aniqlash, tahdid va zaifliklarni baholash, himoya choralarini tanlash va natijalarni doimiy nazorat qilishdan iborat.

2. Zamonaviy kiberxavflar tasnifi

2.1. Zararli dasturlar (malware)

Zararli dasturlarga viruslar, qurtlar (worms), troyan dasturlari, josuslik dasturlari (spyware), reklama dasturlari va **to‘lov talab qiluvchi dasturlar (ransomware)** kiradi. Ransomware ma’lumotlarni shifrlab qo‘yadi va ularni tiklash uchun to‘lov talab qiladi. Bu bugungi kunda tashkilotlar uchun eng og‘ir xavflardan biridir.

2.2. Ijtimoiy muhandislik va fishing

Ijtimoiy muhandislik texnik zaifliklarni emas, balki inson omilini nishonga oladi. **Fishing** (phishing) — ishonchli manba nomidan yuborilgan soxta xabar yoki sayt orqali foydalanuvchining login, parol yoki karta ma’lumotlarini qo‘lga kiritishdir. Uning turlari: ommaviy fishing, nishonli fishing (spear phishing), SMS orqali (smishing) va telefon orqali (vishing) amalga oshiriladigan hujumlar.

2.3. Xizmat ko‘rsatishdan mahrum qilish hujumlari (DoS/DDoS)

Bunday hujumlarda tizimga bir vaqtning o‘zida juda ko‘p so‘rov yuboriladi va u haqiqiy foydalanuvchilarga xizmat ko‘rsata olmay qoladi. Ko‘pincha hujumda zararlangan qurilmalar tarmog‘i (botnet) ishlatiladi.

2.4. Ilovalar va ma’lumotlar bazasiga hujumlar

Veb-ilovalardagi eng keng tarqalgan zaifliklar qatoriga SQL-injeksiya, saytlararo skriptlash (XSS), noto‘g‘ri autentifikatsiya va xavfsiz bo‘lmagan sozlamalar kiradi. Veb-ilovalar xavfsizligi bo‘yicha xalqaro OWASP loyihasi bu zaifliklarni muntazam tasniflab boradi.

2.5. Ichki tahdidlar va ta’minot zanjiri hujumlari

Xavf faqat tashqaridan emas, tashkilot ichidan ham kelishi mumkin: bilmasdan xato qilgan yoki g‘arazli niyatdagi xodim, haddan tashqari keng ruxsatlar. Shuningdek, ishonchli dasturiy ta’minot yetkazib beruvchisi orqali tizimga kirish (ta’minot zanjiri hujumi) ham tobora keng tarqalmoqda.

2.6. Sun’iy intellekt bilan bog‘liq yangi xavflar

Sun’iy intellekt himoya vositalarini kuchaytirish bilan birga, hujumchilarga ham imkoniyat yaratmoqda: ishonarli fishing matnlarini ommaviy tayyorlash, ovoz va tasvirni soxtalashtirish (deepfake) kabi. Shu sababli kutilmagan so‘rovlarni, hatto tanish ovoz yoki video orqali kelganda ham, mustaqil kanal orqali tasdiqlash odatga aylanishi kerak.

3. Himoya usullari va vositalari

3.1. Texnik choralar

Shifrlash. Ma’lumotlarni uzatishda (masalan, TLS/HTTPS) va saqlashda shifrlash maxfiylikni ta’minlaydi. Zamonaviy tizimlarda simmetrik (AES) va asimmetrik (RSA, elliptik egri chiziqlar) algoritmlardan foydalaniladi.

Autentifikatsiya. Kuchli va noyob parollar, parol menejerlari hamda ikki yoki ko‘p bosqichli autentifikatsiya (2FA/MFA) hisoblarni egallashdan himoya qiladi.

Tarmoq himoyasi. Xavfsizlik devorlari (firewall), kirishni aniqlash va oldini olish tizimlari (IDS/IPS), tarmoqni segmentlash va VPN.

Yangilanishlar. Operatsion tizim va dasturlarni o‘z vaqtida yangilash ma’lum zaifliklardan foydalanishning oldini oladi.

Zaxira nusxalash. Muhim ma’lumotlarning muntazam va alohida joyda saqlanadigan zaxira nusxasi ransomware oqibatlarini keskin kamaytiradi (“3-2-1” qoidasi: 3 nusxa, 2 xil muhit, 1 nusxa tashqarida).

Antivirus va EDR tizimlari. Oxirgi nuqtalarni (kompyuter, telefon) doimiy kuzatish va shubhali faoliyatni aniqlash.

3.2. Nol ishonch (Zero Trust) modeli

An’anaviy yondashuvda tarmoq ichidagi foydalanuvchiga ishoniladi. **Nol ishonch** modeli esa “hech kimga ishonma, har safar tekshir” tamoyiliga asoslanadi: har bir kirish so‘rovi shaxs, qurilma va kontekst bo‘yicha tekshiriladi, foydalanuvchiga faqat zarur minimal ruxsat beriladi (eng kam imtiyoz tamoyili).

3.3. Tashkiliy choralar

Texnika bilan birga tashkiliy tadbirlar ham muhim: axborot xavfsizligi siyosatini ishlab chiqish, xodimlarni muntazam o‘qitish, ruxsatlarni boshqarish, hodisalarga javob berish rejasini tayyorlash, zaiflik skanerlash va penetratsion testlar o‘tkazish. Amaliyot ko‘rsatadiki, ko‘plab muvaffaqiyatli hujumlarda inson omili hal qiluvchi rol o‘ynaydi, shuning uchun xodimlarni o‘qitish eng samarali va arzon himoya choralaridan biridir.

3.4. Hodisalarga javob berish bosqichlari

tayyorgarlik (siyosat, jamoa, vositalar);

aniqlash va tahlil;

cheklash (hujum tarqalishini to‘xtatish);

bartaraf etish (zararli komponentni olib tashlash);

tiklash (tizim faoliyatini qayta yo‘lga qo‘yish);

xulosalar chiqarish (kelgusi uchun saboqlar).

4. Me’yoriy-huquqiy va standartlar asosi

4.1. O‘zbekiston Respublikasida

O‘zbekistonda kiberxavfsizlik sohasi 2022-yil 15-aprelda qabul qilingan **“Kiberxavfsizlik to‘g‘risida”gi qonun** bilan tartibga solinadi [1]. Qonun kiberxavfsizlikni ta’minlash sohasidagi asosiy tamoyillarni, davlat organlarining vakolatlarini, muhim axborot infratuzilmasi obyektlarini himoya qilish tartibini belgilaydi. Shuningdek, shaxsiy ma’lumotlarni himoya qilish masalalari “Shaxsga doir ma’lumotlar to‘g‘risida”gi qonun orqali tartibga solinadi [2]. Tegishli me’yoriy hujjatlarning amaldagi tahririni rasmiy huquqiy portal (lex.uz) orqali tekshirish tavsiya etiladi.

4.2. Xalqaro standartlar va tajriba

ISO/IEC 27001 — axborot xavfsizligini boshqarish tizimiga qo‘yiladigan talablar standarti [3].

NIST Cybersecurity Framework — kiberxavflarni boshqarish uchun asosiy funksiyalar (aniqlash, himoya qilish, kashf etish, javob berish, tiklash) bo‘yicha tavsiyalar to‘plami [4].

GDPR — Yevropa Ittifoqida shaxsiy ma’lumotlarni himoya qilish reglamenti [7].

OWASP — veb-ilovalar xavfsizligi bo‘yicha ochiq tavsiyalar [8].

Xalqaro hamkorlik, ma’lumot almashish va kiberhujumlarga birgalikda javob berish tizimlari kiberxavfsizlikning global xarakterini ko‘rsatadi.

5. Amaliy tavsiyalar

5.1. Oddiy foydalanuvchilar uchun

Har bir hisob uchun uzun (kamida 12–14 belgi) va noyob parol ishlating; parol menejeridan foydalaning.

Barcha muhim hisoblarda ikki bosqichli autentifikatsiyani yoqing.

Noma’lum havolalarni bosmang, ilovalarni faqat rasmiy do‘konlardan yuklab oling.

Bank kartasi ma’lumotlari, SMS-kodlar va parollarni hech kimga, hatto “bank xodimi” deb tanishtirgan shaxsga ham aytmang.

Qurilma va ilovalarni muntazam yangilab turing.

Ommaviy Wi-Fi tarmoqlarida muhim operatsiyalarni bajarishdan saqlaning.

Muhim fayllarning zaxira nusxasini oling.

5.2. Tashkilotlar uchun

Xavflarni muntazam baholang va xavfsizlik siyosatini yangilab boring.

Xodimlar uchun fishingga qarshi mashqlar va treninglar o‘tkazing.

Eng kam imtiyoz tamoyilini joriy qiling, ruxsatlarni davriy qayta ko‘rib chiqing.

Jurnallarni yuriting va monitoringni ta’minlang.

Hodisalarga javob berish rejasini yozma shaklda tayyorlab, mashq qiling.

Zaxira nusxalarni sinab turing va ularni asosiy tarmoqdan ajratib saqlang.

6. Kasblar va rivojlanish istiqbollari

Kiberxavfsizlik mutaxassislariga talab butun dunyoda ortib bormoqda. Xavfsizlik tahlilchisi (SOC analyst), penetratsion tester, xavfsizlik muhandisi, kriminalist-ekspert (digital forensics) va axborot xavfsizligi bo‘yicha rahbar (CISO) kabi kasblar shu jumlaga kiradi. Istiqbolda quyidagi yo‘nalishlar muhim bo‘ladi: sun’iy intellektga asoslangan tahdidlarni aniqlash, kvantga chidamli kriptografiya, bulutli va IoT muhitlarining xavfsizligi hamda avtomatlashtirilgan hodisalarga javob berish tizimlari.

Xulosa

Tadqiqot natijalariga ko‘ra, kiberxavfsizlik yagona vosita bilan ta’minlanmaydi, u texnik, tashkiliy va huquqiy choralarning uyg‘unligini talab qiladi. Kiberxavflar doimiy o‘zgarib borayotgani sababli himoya tizimlari ham muntazam yangilanishi, xodimlar va foydalanuvchilarning raqamli savodxonligi doimiy oshirilishi lozim. O‘zbekistonda qonunchilik bazasining shakllanishi, xalqaro standartlarning joriy etilishi va mutaxassislar tayyorlash tizimining rivojlanishi sohada barqaror taraqqiyot

uchun zamin yaratmoqda. Axborotni himoya qilish har bir davlat idorasi, tashkilot va har bir foydalanuvchining umumiy mas’uliyatidir.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni, 2022-yil 15-aprel. — Qonunchilik ma’lumotlari milliy bazasi (lex.uz).
2. O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni. — Qonunchilik ma’lumotlari milliy bazasi (lex.uz).
3. ISO/IEC 27001. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. — Geneva: ISO, amaldagi tahrir.
4. NIST. Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework). — Gaithersburg: National Institute of Standards and Technology, amaldagi tahrir.
5. Stallings W. Cryptography and Network Security: Principles and Practice. — Pearson, so‘nggi nashr.
6. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. — Wiley, so‘nggi nashr.
7. Regulation (EU) 2016/679 (General Data Protection Regulation). — Official Journal of the European Union, 2016.
8. OWASP Foundation. OWASP Top 10: Web Application Security Risks. — owasp.org.
9. Verizon. Data Breach Investigations Report (yillik hisobot). — verizon.com.

Eslatma: adabiyotlar ro‘yxatini o‘quv muassasangiz yoki jurnal talabiga (GOST, APA va h.k.) moslab, amaldagi nashr yili va sahifalarini aniqlashtiring.