ISSN 3060-4567

“KIBERXAVFSIZLIKNING ZAMONAVIY AXBOROT TIZIMLARIDAGI O‘RNI VA AHAMIYATI”

QAHHOROVA NILUFAR QODIR QIZI

Qarshi davlat texnika unversiteti raqamli texnologiyalar va sun’iy intellekt fakulteti kompyuter injiniringi 2-kurs talabasi

SHAHLO ULASHEVA

“Kompyuter tizimlarining dasturiy va texnika ta’minoti”

Raqamli texnologiyalar va sun’iy intellekt fakultet, Xotin-qizlar masalalari bo'yicha dekan maslahatchisi

ANNOTATSIYA: *Ushbu maqolada kiberxavfsizlikning axborot tizimlarida tutgan o‘rni, axborot himoyasi tamoyillari, kiberxavflarning turlari hamda ularni oldini olish usullari tahlil etiladi. Raqamli texnologiyalarning rivojlanishi bilan bog‘liq tahdidlar, korxonalar va davlat infratuzilmasi uchun xavfsizlik choralarining ahamiyati yoritiladi. Shuningdek, kiberxavfsizlik bo‘yicha zamonaviy yo‘nalishlar va mutaxassislar uchun talablar keltirilgan.*

Kalit so‘zlar: *Kiberxavfsizlik, axborot tizimi, kiberhujum, ma’lumotlar himoyasi, xavfsizlik protokollari, tarmoq xavfsizligi.*

KIRISH

Axborot texnologiyalarining keskin rivojlanishi inson faoliyatining deyarli barcha jabhalariga — iqtisodiyot, tibbiyot, sanoat, ta’lim va davlat boshqaruviga chuqur kirib bordi. Raqamli tizimlarning keng qo‘llanilishi bilan bir qatorda, axborot xavfsizligiga bo‘lgan ehtiyoj ham ortmoqda. Bugungi kunda dunyo miqyosida sodir bo‘layotgan kiberhujumlar soni keskin oshgani sababli kiberxavfsizlik masalasi strategik darajadagi muhim omilga aylangan.

ASOSIY QISM

1. Kiberxavfsizlik tushunchasi va uning zamonaviy ahamiyati

Kiberxavfsizlik — bu axborot tizimlari, kompyuter tarmoqlari, dasturiy ta’minot va ma’lumotlarni ruxsatsiz kirish, zarar yetkazish yoki o‘g‘irlashdan himoya qilishga qaratilgan kompleks choralar majmuasidir.

Zamonaviy jamiyatda kiberxavfsizlik quyidagilar uchun muhimdir:

- davlatning siyosiy va iqtisodiy barqarorligi;
- korxonalar uchun moliyaviy xavfsizlik;
- shaxsiy ma’lumotlar himoyasi;
- raqamli xizmatlarning uzluksiz ishlashi.

2. Kiberxavflarning asosiy turlari

Kiber tahdidlar shaklan va maqsad bo‘yicha farqlanadi. Eng ko‘p uchraydiganlari:

- **Fishing (phishing)** — firibgarlarning soxta saytlar yoki pochta orqali shaxsiy ma’lumotlarni qo‘lga kiritish usuli.
- **DDoS hujumlar** — serverlarni ishlamay qolish holatiga olib keladigan tarmoq yuklanishi.
- **Malware va ransomware dasturlari** — tizimga zarar yetkazuvchi zararli dasturlar.
- **Tarmoqdagi zaifliklar orqali kirish** — himoyasi kuchsiz bo‘lgan portlar va servislar orqali tajovuz.

Har bir hujum turi o‘ziga xos himoya choralarini talab qiladi.

3. Axborot tizimlarida xavfsizlikni ta’minlash usullari

Axborot tizimlari xavfsizligini ta’minlash quyidagi tamoyillarga asoslanadi:

- **Konfidensiallik** — ma’lumotlarga faqat vakolatli shaxslarning kirishini ta’minlash.
- **Butunlik** — ma’lumotlar o‘zgarmagan bo‘lishi yoki ruxsat etilgan tartibda o‘zgartirilgan bo‘lishi.
- **Mavjudlik** — tizimning uzluksiz ishlashi va kerakli paytda foydalanuvchiga xizmat ko‘rsatishi.

Amaliy choralar esa:

- xavfsizlik devorlari (firewall);

- antivirus va antimalware tizimlari;
- ikki bosqichli autentifikatsiya;
- ma’lumotlarni shifrlash (encryption);
- zaxira nusxalar yaratish (backup);
- tarmoq monitoringi va log tahlili.

4. Kiberxavfsizlik bo‘yicha zamonaviy yo‘nalishlar

So‘nggi yillarda kiberxavfsizlikda quyidagi yo‘nalishlar faol rivojlanmoqda:

- **Sun’iy intellekt yordamida tahdidlarni aniqlash**

AI algoritmlari real vaqt rejimida tarmoq xatti-harakatlarini tahlil qiladi.

- **Zero Trust Architecture**
- Har qanday tarmoq elementi ishonchsiz deb hisoblanadi va har safar tasdiqlash talab etiladi.
- **Cloud security**
- Bulutli tizimlar xavfsizligini oshirish kompaniyalar uchun ustuvor vazifa.
- **Cyber Threat Intelligence (CTI)**
- Tahdidlar haqidagi oldindan ma’lumot to‘plash va tahlil qilish.

5. Kiberxavfsizlik mutaxassislariga qo‘yiladigan talablar

Zamonaviy kiberxavfsizlik sohasi mutaxassislardan quyidagi ko‘nikmalarni talab qiladi:

- tarmoq protokollarini chuqur bilish;
- Linux/Windows server boshqaruvi;
- xavfsizlik devorlari va IDS/IPS tizimlari bilan ishlash;
- shifrlash algoritmlaridan xabardorlik;
- zaifliklarni aniqlash (penetration testing);
- CEH, CompTIA Security+, CISSP kabi sertifikatlarga ega bo‘lish.
- **XULOSA:**Kiberxavfsizlik zamonaviy axborot tizimlarining ajralmas qismi bo‘lib, raqamli infratuzilmaning barqarorligini ta’minlaydi. Cybertahdidlarning keskin ortib borayotgan sharoitida davlat va tashkilotlar kuchli himoya mexanizmlariga ega bo‘lishi zarur. Kiberxavfsizlik sohasiga

ISSN 3060-4567

investitsiyalarni oshirish, malakali kadrlani tayyorlash va ilg‘or texnologiyalarni joriy etish kelajak xavfsizligining kafolatidir.

FOYDALANILGAN ADABIYOTLAR

1. Stallings, W. *Network Security Essentials*. Pearson, 2021.
2. Schneier, B. *Applied Cryptography*. Wiley, 2016.
3. Andress, J. *Foundations of Cybersecurity*. Syngress, 2020.
4. CompTIA Security+ Official Guide, turli yillar.