



INNOVATIVE WORLD
Ilmiy tadqiqotlar markazi

YANGI RENESSANS

RESPUBLIKA ILMIY JURNALI

2025



+998335668868



www.innoworld.net

Google Scholar



zenodo

OpenAIRE



2025

YANGI RENESSANS

RESPUBLIKA ILMIY JURNALI

2-JILD 3-SON



YANGI RENESSANS

**RESPUBLIKA ILMIY JURNALI
TO'PLAMI**

**2 - JILD, 3 - SON
2025**



www.innoworld.net

O'ZBEKISTON-2025

**KIBERXAVFSIZLIK VA ZAMONAVIY AXBOROT TEXNOLOGIYALARI****Qurbonaliyev Sanjarbek**

Toshkent Hidrometeorologiya Texnikumi

Maxsus fanlar kafedrası o'qituvchisi

Annotatsiya. Kiberxavfsizlik zamonaviy axborot texnologiyalari tizimlarida muhim o'rin tutadi. Ushbu maqolada ma'lumotlarni himoya qilish usullari, kiberhujum turlari, xavfsizlik protokollari va innovatsion texnologiyalarning roli tahlil qilingan. Shuningdek, sun'iy intellekt va zamonaviy IT yechimlari yordamida tizimli xavfsizlikni ta'minlash hamda shaxsiy va korporativ ma'lumotlarni himoya qilishning samaradorligi yoritilgan. Tadqiqot natijalari shuni ko'rsatadiki, axborot tizimlaridagi xavfsizlikni strategik va oqilona boshqarish IT muhitining barqarorligini ta'minlashning muhim omili hisoblanadi.

Kalit so'zlar: kiberxavfsizlik, axborot texnologiyalari, ma'lumotlarni himoya qilish, shaxsiy ma'lumotlar, tarmoq xavfsizligi, kiberhujum, protokollar, IT xavfsizlik, zamonaviy texnologiyalar, kriptografiya.

Kirish. So'nggi yillarda axborot texnologiyalari hayotning deyarli barcha sohalariga kirib, ma'lumotlar almashinuvi va onlayn faoliyatni kengaytirdi. Shu bilan birga, kiberxavfsizlik masalalari ham dolzarb muammo sifatida namoyon bo'lmoqda. Internet, mobil ilovalar, korporativ tarmoqlar va bulutli xizmatlar kundalik faoliyatning ajralmas qismiga aylangani sayin, ma'lumotlarni himoya qilish va tarmoq xavfsizligini ta'minlash muhim ahamiyat kasb etmoqda. Kiberxavfsizlik nafaqat texnik masala, balki axborot siyosati, qonunchilik va innovatsion yechimlar bilan uyg'unlashgan tizimdir.

Axborot tizimlarida xavfsizlikni ta'minlash tizimli yondashuvni talab qiladi. Shaxsiy foydalanuvchilar, kompaniyalar va davlat muassasalari doimiy ravishda yangi xavf-xatarlar va kiberhujumlarni hisobga olgan holda strategiyalar ishlab chiqishi zarur. Shu bois, kiberxavfsizlik sohasi mutaxassislari nafaqat texnik bilimga, balki global xavfsizlik tahdidlarini tahlil qilish, xavf-xatarlarni prognoz qilish va innovatsion yechimlarni tatbiq etish qobiliyatiga ega bo'lishi kerak.

Asosiy qism. Kiberxavfsizlik bir qator asosiy yo'nalishlarda amalga oshiriladi. Eng avvalo, shifrlash, autentifikatsiya, tarmoq monitoringi, xavfsizlik protokollari va foydalanuvchilarni tarbiyalash kabi chora-tadbirlar ma'lumotlarni himoya qilishda muhimdir. Shifrlash ma'lumotlarni ruxsat etilgan foydalanuvchilar uchun o'qilishi mumkin bo'lgan formatga aylantiradi. Autentifikatsiya tizimlari foydalanuvchining shaxsini aniqlash imkonini beradi, ikki faktorli autentifikatsiya esa qo'shimcha xavfsizlik qatlamini yaratadi.





Kiberhujumlar tobora murakkablashib, phishing, malware, ransomware, DDoS va ijtimoiy muhandislik kabi shakllarda sodir bo'ladi. Shu sababli kiberxavfsizlik choralari tizimli ravishda joriy etish zarur. Masalan, kompaniya serverlarini himoya qilishda firewall, antivirus va intrusion detection tizimlari birgalikda ishlatiladi. Shaxsiy foydalanuvchilar esa kuchli parollar, ikki faktorli autentifikatsiya va shubhali havolalardan ehtiyot bo'lish orqali ma'lumotlarini himoya qiladi.

Zamonaviy IT muhitida innovatsion yechimlar, xususan sun'iy intellekt va big data texnologiyalari kiberxavfsizlikni kuchaytirishda muhim rol o'ynaydi. AI algoritmlari tarmoqlarni monitoring qilish, anomal faoliyatni aniqlash va hujumlarni oldini olish imkonini beradi. Bulutli xizmatlar esa markazlashtirilgan va himoyalangan ma'lumot saqlashni ta'minlab, foydalanuvchilarga masofadan xavfsiz kirish imkonini yaratadi.

Kiberxavfsizlik nafaqat texnik, balki madaniy va strategik masaladir. Foydalanuvchilar axborot madaniyati, plagiatga yo'l qo'ymaslik, tanqidiy fikrlash va ma'lumot manbalarini tahlil qilish qobiliyatiga ega bo'lishi lozim. Shu bilan birga, xodimlarni muntazam tayyorlash, seminar va treninglar tashkil etish ham xavfsizlikni ta'minlashning muhim jihatlaridan biridir.

O'zbekistonda kiberxavfsizlik bo'yicha qonunlar va me'yoriy hujjatlar qabul qilinib, axborot tizimlarining xavfsizligi va kiberhujumlarga qarshi chora-tadbirlar tartibga solinmoqda. Shu bilan birga, kompaniyalar va davlat muassasalari yangi texnologiyalarni joriy etish va mutaxassislarni tayyorlash orqali IT muhitini barqarorlashtirmoqda.

Xulosa. Kiberxavfsizlik zamonaviy axborot texnologiyalarining ajralmas qismiga aylangan. U ma'lumotlarni himoya qilish, tarmoqlarni barqaror ishlashini ta'minlash va kiberhujumlarning oldini olish orqali IT muhitida xavfsizlikni kafolatlaydi. Sun'iy intellekt va innovatsion IT yechimlari xavfsizlik choralari takomillashtirish imkonini beradi. Har bir foydalanuvchi va IT mutaxassisi kiberxavfsizlik madaniyatiga ega bo'lishi, shaxsiy va korporativ ma'lumotlarni himoya qilishda mas'uliyatli bo'lishi zarur. Kiberxavfsizlikni doimiy rivojlantirish va yangi texnologiyalarni tatbiq etish IT tizimlarining ishonchliligi va samaradorligini ta'minlovchi asosiy omildir.

Foydalanilgan adabiyotlar

1. O'zbekiston Respublikasi Prezidenti "Raqamli O'zbekiston – 2030" strategiyasi. – 2020.
2. Stallings, W. *Network Security Essentials: Applications and Standards*. – Pearson, 2021.
3. Andress, J. *The Basics of Information Security*. – Syngress, 2020.
4. Schneier, B. *Applied Cryptography*. – Wiley, 2019.
5. European Union Agency for Cybersecurity (ENISA). *Cybersecurity Guidelines and Best Practices*. – 2022.
6. Whitman, M., Mattord, H. *Principles of Information Security*. – Cengage Learning, 2021.

