TEXNIK TIZIMLAR XAVFSIZLIGIDA SUN'IY INTELLEKT VA NEYRON TARMOQLARNI QO'LLASH

Kasimova Gulnora Ismoilovna
Ilmiy rahbar: (Toshkent davlat texnika universiteti asistenti)
Rahimova Barno Abdumutal qizi
(Toshkent davlat texnika universiteti 100-25 gr talabasi)
Qaimjonava Muattar Qobiljon qizi
(Toshkent davlat texnika universiteti 100-25 gr talabasi)

Annotasiya: *Ushbu maqolada zamonaviy texnik tizimlarda kiberxavfsizlikni ta'minlashning dolzarb masalalari tahlil qilinadi. Tadqiqot davomida apparat va dasturiy ta'minot majmualarini tashqi kiberhujumlardan himoya qilish usullari, ma'lumotlarni shifrlash texnologiyalari hamda avtomatlashtirilgan boshqaruv tizimlarining barqarorligini oshirish strategiyalari ko'rib chiqilgan. Shuningdek, maqolada milliy kiberxavfsizlik infratuzilmasini rivojlantirish va texnik tizimlardagi zaifliklarni aniqlash metodikasi bo'yicha tavsiyalar berilgan.*

Tayanch so'zlar: *kiberxavfsizlik, texnik tizimlar, axborot himoyasi, kriptografiya, kiberhujum, avtomatlashtirilgan tizimlar, xavfsizlik protokollari.*

Аннотация: *В данной статье анализируются актуальные вопросы обеспечения кибербезопасности в современных технических системах. В ходе исследования рассматриваются методы защиты аппаратных и программных комплексов от внешних кибератак, технологии шифрования данных и стратегии повышения устойчивости автоматизированных систем управления.Также в статье представлены рекомендации по развитию национальной инфраструктуры кибербезопасности и методики выявления уязвимостей в технических системах.*

Ключевые слова: *кибербезопасность, технические системы, защита информации, криптография, кибератака, автоматизированные системы, протоколы безопасности.*

Annotation: *This article analyzes current issues of ensuring cybersecurity in modern technical systems. The research examines methods for protecting hardware and software complexes from external cyberattacks, data encryption technologies, and strategies to increase the stability of automated control systems. Additionally, the article provides recommendations on the development of national cybersecurity infrastructure and methodology for identifying vulnerabilities in technical systems.*

Keywords: *cybersecurity, technical systems, information protection, cryptography, cyberattack, automated systems, security protocols.*

KIRISH

Hozirgi globallashuv va raqamli texnologiyalar taraqqiyoti davrida axborot resurslari jamiyatning eng muhim boyliklaridan biriga aylanib bormoqda. Davlat boshqaruvi, bank-moliya tizimi, sanoat korxonalari, transport, sog‘liqni saqlash, ta’lim va boshqa ko‘plab sohalarda texnik tizimlardan keng foydalanilmoqda. Ushbu tizimlar orqali katta hajmdagi ma’lumotlar saqlanadi, qayta ishlanadi va uzatiladi. Natijada texnik tizimlarning xavfsizligi nafaqat alohida tashkilotlar, balki butun jamiyat barqarorligi uchun ham muhim ahamiyat kasb etmoqda.

Texnik tizimlar deganda kompyuterlar, serverlar, lokal va global tarmoqlar, avtomatlashtirilgan boshqaruv tizimlari, sanoat uskunalari, videokuzatuv vositalari, mobil qurilmalar hamda turli dasturiy-apparat majmualari tushuniladi. Ushbu tizimlarning samarali ishlashi axborot xavfsizligiga bevosita bog‘liqdir. Agar tizimlarga zararli dasturlar kirib qolsa, ma’lumotlar o‘g‘irlanishi, yo‘qolishi yoki o‘zgartirilishi mumkin. Bu esa iqtisodiy zarar, ishlab chiqarish jarayonlarining to‘xtashi va foydalanuvchilar ishonchining pasayishiga olib keladi.

So‘nggi yillarda kiberhujumlar soni va murakkabligi ortib bormoqda. Xakerlik hujumlari, phishing, viruslar, troyan dasturlar, DDoS hujumlari va ma’lumotlar sizib chiqishi kabi xavflar texnik tizimlar uchun jiddiy tahdid hisoblanadi. Ayniqsa, internetga ulangan qurilmalar sonining oshishi bilan tahdidlar doirasi ham kengaymoqda. Shu sababli har qanday tashkilot o‘z texnik infratuzilmasini himoyalashga alohida e’tibor qaratishi zarur.

Kiberxavfsizlik – bu axborot tizimlari, kompyuter tarmoqlari va elektron qurilmalarni tashqi hamda ichki tahdidlardan himoya qilishga qaratilgan chora-tadbirlar majmuasidir. Uning asosiy vazifasi ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlashdan iborat. Buning uchun zamonaviy dasturiy vositalar, apparat himoya tizimlari, shifrlash usullari hamda foydalanuvchilarning bilim va ko‘nikmalaridan foydalaniladi.

Mazkur maqolada texnik tizimlarda axborot xavfsizligini ta’minlashning dolzarbligi, asosiy tahdidlar va ulardan himoyalanishning samarali usullari tahlil qilinadi. Shuningdek, texnik vositalarni ishonchli boshqarish, ma’lumotlarni saqlash va tarmoq xavfsizligini kuchaytirish bo‘yicha tavsiyalar yoritiladi.

Xulosa. Xulosa qilib aytganda, zamonaviy jamiyatda texnik tizimlar barcha sohalarning ajralmas qismiga aylangan bo‘lib, ularning xavfsiz ishlashi axborot xavfsizligi bilan chambarchas bog‘liqdir. Korxonalar, davlat muassasalari, ta’lim maskanlari, bank tizimlari va ishlab chiqarish korxonalarida qo‘llanilayotgan texnik vositalar doimiy

ravishda turli kiberxavflar ta’sirida bo‘ladi. Shu sababli ushbu tizimlarni himoyalash har bir tashkilotning ustuvor vazifalaridan biri hisoblanadi.

Texnik tizimlarda axborot xavfsizligini ta’minlash uchun kompleks yondashuv zarur. Bunda kuchli parollarni qo‘llash, zamonaviy antivirus dasturlaridan foydalanish, tarmoq xavfsizligini mustahkamlash, ma’lumotlarni shifrlash, zaxira nusxalar yaratish va tizimlarni muntazam yangilab borish muhim ahamiyat kasb etadi. Shu bilan birga, foydalanuvchilarning kiberxavfsizlik bo‘yicha bilimini oshirish ham katta samara beradi, chunki ko‘plab tahdidlar inson omili bilan bog‘liq holda yuzaga keladi.

Bugungi kunda kiberjinoyatchilik usullari tobora takomillashib borayotganligi sababli himoya choralarini ham doimiy ravishda rivojlantirib borish lozim. Sun’iy intellekt asosidagi himoya tizimlari, avtomatik monitoring vositalari va tahdidlarni erta aniqlash texnologiyalari kelajakda yanada muhim o‘rin egallaydi.

Shunday qilib, texnik tizimlarda axborot xavfsizligini ta’minlash nafaqat ma’lumotlarni himoya qilish, balki tashkilot faoliyatining uzluksizligi, iqtisodiy barqarorlik va foydalanuvchilar ishonchini saqlashning asosiy omillaridan biridir. Har bir tashkilot va foydalanuvchi kiberxavfsizlikka mas’uliyat bilan yondashgan taqdirdagina xavfsiz raqamli muhitni yaratish mumkin.

FOYDALANILGAN ADABIYOTLAR RO’YHATI:

1. Ganiyev S. K., Ganiyev A. A., Xudoyqulov Z. T. "Kiberxavfsizlik asoslari" (O‘quv qo‘llanma). Toshkent: "Aloqachi", 2020.
2. Karimov Sh. A. "Axborot xavfsizligi va kiberxavfsizlik asoslari". Toshkent: Innovatsiya nashriyoti, 2022.
3. Xolmatov B. R. "Axborot texnologiyalarida xavfsizlik asoslari". Toshkent: Fan, 2021.
4. Qodirov F. E., O‘ktamov M. O‘., Musirmanov Sh. U. "Kiberxavfsizlik asoslari". Toshkent, 2024.
5. Mamajonov R. Y., Rajabov T. J. va boshqalar. "Kiber xavfsizlik" (O‘quv qo‘llanma). 2024.