JOURNAL OF INTERNATIONAL SCIENTIFIC RESEARCH
Volume 2, Issue 8, April, 2025 Online ISSN: 3030-3508
https://spaceknowladge.com

Kompyuter tizimlarida xavfsizlikni ta'minlashning zamonaviy yondashuvlari

Xolchayev Bekzod Nurali o'g'li
Axborot texnologiyalari va menejment universiteti magistranti

ARTICLE INFO

ARTICLE HISTORY:
Received:10.04.2025
Revised: 11.04.2025
Accepted:13.04.2025

KEYWORDS:
Qishloq xo'jaligi, mahsulotlarni saqlash, dastlabki ishlash, xalqaro tajriba, mahalliy tajriba, innovatsion texnologiyalar, oziq-ovqat xavfsizligi, mahsulot sifati, boshqariladigan gaz muhiti, saqlash infratuzilmasi.

ABSTRACT:

Ushbu maqola kompyuter tizimlarida xavfsizlikni ta'minlashning zamonaviy yondashuvlarini ko'rib chiqadi. Maqolada kiberxavfsizlikning asosiy tamoyillari, xavfsizlikni boshqarishning yangi usullari, va tizimlarda xatarlarni oldini olish uchun ishlatiladigan texnologiyalar tahlil qilinadi. Xavfsizlikni ta'minlashda foydalaniladigan kriptografiya, autentifikatsiya, tarmoq xavfsizligi va zararlangan dasturlardan himoya qilish usullari kabi masalalar muhokama qilinadi. Maqola ayniqsa, korporativ tizimlar va davlat organlari uchun foydalidir, chunki ular kompyuter tizimlarining xavfsizligini ta'minlashda o'zaro aloqalar va innovatsion yondashuvlarni qo'llash zaruriyatini his qilishadi.

Kirish. Bugungi kunda kompyuter tizimlari va internet texnologiyalarining rivojlanishi bilan birga, kiberxavfsizlik masalalari ham dolzarb ahamiyat kasb etmoqda. Kompyuter tizimlarining xavfsizligi faqatgina texnologik yutuqlar bilan emas, balki axborotning maxfiyligi, yaxlitligi va mavjudligini ta'minlash uchun muhim omil sifatida qaraladi. Xavfsizlikni ta'minlashning zamonaviy yondashuvlari turli xil texnologiyalar va metodlarni o'z ichiga oladi. Kriptografiya, autentifikatsiya tizimlari, tarmoq xavfsizligi, zararli dasturlardan himoya qilish va boshqa zamonaviy xavfsizlik choralarining birlashuvi bu sohadagi eng samarali yechimlarni yaratadi. Shuningdek, kiberxavfsizlikka oid tahdidlar va hujumlar har doim yangilanib turadi,

shuning uchun tizimlar xavfsizligini ta'minlash uchun yangilangan yondashuvlar va ilg'or texnologiyalarni joriy qilish zarurdir. Ushbu maqolada kompyuter tizimlarida xavfsizlikni ta'minlashning eng yangi va samarali usullari tahlil qilinadi va ularning joriy etilishining ahamiyati muhokama qilinadi [1].

Kompyuter tizimlarida xavfsizlikni ta'minlashda autentifikatsiya va avtorizatsiya jarayonlari muhim o'rin tutadi. Autentifikatsiya - bu foydalanuvchining kimligini tekshirish jarayoni bo'lib, odatda parol, biometrik ma'lumotlar (barmoq izlari, yuzni tanish), yoki ikki faktorli autentifikatsiya (2FA) orqali amalga oshiriladi. Avtorizatsiya esa foydalanuvchiga tizimda qanday huquqlar berilganini aniqlaydi. Zamonaviy autentifikatsiya usullari, masalan, biometrik tekshiruvlar va ikki faktorli autentifikatsiya, tizimlarni ruxsatsiz kirishlardan himoya qilishda samarali ishlaydi. Tarmoq xavfsizligi tizimlar va qurilmalar o'rtasida ma'lumotlar almashinuvi xavfsizligini ta'minlashga qaratilgan. Tarmoq xavfsizligini ta'minlashda eng ko'p qo'llaniladigan texnologiyalardan biri firewall (olov devori) hisoblanadi. Firewall, tarmoqni kirish va chiqish so'rovlaridan nazorat qiladi va ruxsatsiz kirishlarni bloklaydi. Bundan tashqari, VPN (Virtual Private Network) texnologiyasi, internetga ulanishda shifrlangan kanallarni yaratadi va foydalanuvchining internetda xavfsiz ishlashini ta'minlaydi. Zararlangan dasturlar (malware), viruslar, trojanlar, va boshqa zararli dasturlar tizimlarning xavfsizligini tahdid qiladi. Ular kompyuter tizimlariga kirish orqali ma'lumotlarni o'g'irlash, tizimni ishdan chiqarish yoki boshqa zararlar yetkazish imkonini beradi. Bugungi kunda bu tahdidlardan himoya qilish uchun antivirus dasturlari, antimalware vositalari va tizim monitoringi ishlatiladi. Ular tizimdagi xavfli dasturlarni aniqlaydi va ularga qarshi zarur choralarni ko'radi. Xavfsizlikni boshqarish tizimlari (SIEM) - bu korxonalarga tizimlarning xavfsizligini monitoring qilish va boshqarish imkonini beradigan ilg'or vositalardir. SIEM tizimlari real vaqt rejimida xavfsizlik hodisalarini tahlil qilish, potentsial xavflarni aniqlash va ularga tezkor javob berishga yordam beradi [2]. SIEM tizimlari o'z ichiga kiberhujumlarni aniqlash, xavfsizlik voqealarini qayd etish va tahlil qilish, hamda xodimlar va foydalanuvchilar faoliyatini monitoring qilishni oladi. Zamonaviy xavfsizlikni ta'minlashda sun'iy intellekt (AI) va mashinani o'rganish (ML) texnologiyalaridan foydalanish tobora kengayib bormoqda. AI va ML tizimlari

xavfsizlik tahdidlarini aniqlashda, ular tomonidan o'rganilgan namunalar asosida tizimlarni himoya qilishda yordam beradi. Masalan, mashinani o'rganish algoritmlari kiberhujumlarni oldindan prognoz qilish va real vaqtda tizimlarni himoya qilishda samarali bo'ladi. Har qanday tashkilot va kompaniya uchun xavfsizlikni ta'minlashning muvaffaqiyatli bo'lishi uchun aniq xavfsizlik siyosatlari va qoidalari zarur. Bu siyosatlar foydalanuvchilarni tizimlarga kirish huquqini boshqarish, ma'lumotlarni himoya qilish, xavfsizlikni monitoring qilish, va kiberhujumlarga qarshi kurashish bo'yicha aniq yo'riqnomalar taqdim etadi. Yaxshi ishlab chiqilgan xavfsizlik siyosatlari va qoidalari nafaqat tizim xavfsizligini ta'minlashga yordam beradi, balki tashkilotdagi barcha xodimlarni ham xavfsizlik masalalari bo'yicha ogoh qiladi. Kompyuter tizimlarida xavfsizlikni ta'minlashning zamonaviy yondashuvlari texnologik taraqqiyot bilan birgalikda o'zgarib bormoqda. Kriptografiya, autentifikatsiya, tarmoq xavfsizligi, zararlangan dasturlardan himoya qilish, va sun'iy intellekt kabi ilg'or texnologiyalar xavfsizlikni ta'minlashda samarali vositalar bo'lib xizmat qiladi. Kiberxavfsizlikni ta'minlash uchun barcha bu yondashuvlarni joriy qilish, yangi tahdidlarga qarshi kurashishda yordam beradi va tizimlarning xavfsizligini mustahkamlashga yordam beradi. Shu bilan birga, xavfsizlik siyosatlari va qoidalarining o'rnatilishi ham muhimdir, chunki ular xavfsizlikni boshqarishda ko'rsatmalar va nazoratni ta'minlaydi [3].

Adabiyotlar tahlili. Kompyuter tizimlarida xavfsizlikni ta'minlash bugungi kunda har bir tashkilot va shaxs uchun muhim ahamiyatga ega. Bu masala texnologiyalar rivojlanishi bilan birgalikda jadal o'zgarib bormoqda. Kompyuter tizimlaridagi xavfsizlik tahdidlarini kamaytirish va himoya qilish uchun bir qator zamonaviy yondashuvlar ishlab chiqilgan. Adabiyotlar tahlili orqali ushbu yondashuvlar, ularning samaradorligi va tadqiqotlarda qanday yondashilganligini ko'rib chiqamiz. Kriptografiya kompyuter tizimlarida xavfsizlikni ta'minlashning asosiy vositalaridan biridir. Wang et al. (2015) o'zlarining tadqiqotida ma'lumotlarni shifrlashning samaradorligini tahlil qilgan va ma'lumotlarning maxfiyligini ta'minlash uchun AES va RSA algoritmlarining keng qo'llanilishini ko'rsatgan. Ularning tahliliga ko'ra, bu algoritmlar nafaqat samarali, balki xavfsizlikni ta'minlashda yuqori darajadagi ishonchlilikni ta'minlaydi. Shuningdek, Menezes va Martins (2017) kriptografiya

usullarining dasturiy ta'minot va tarmoq xavfsizligidagi o'rnini ta'kidlagan va kriptografik texnologiyalarning shifrlash va autentifikatsiya jarayonlarida qanday ishlashini muhokama qilgan.

Autentifikatsiya va avtorizatsiya tizimlari kompyuter tizimlarida kirish huquqlarini boshqarish va xavfsizlikni ta'minlash uchun muhim omillardir. Zhang et al. (2016) ikki faktorli autentifikatsiya (2FA) tizimlarining samaradorligini o'rganib chiqqan va bu tizimlar foydalanuvchining kimligini tekshirishda an'anaviy parollarga qaraganda samaraliroq ekanligini ta'kidlagan. Shuningdek, Jain va Singh (2018) biometrik autentifikatsiya tizimlarining afzalliklarini ko'rsatgan, bu tizimlarning foydalanuvchi tajribasini yengillashtirishda va xavfsizlikni oshirishda muhim rol o'ynashini ta'kidlagan. Tarmoq xavfsizligi — bu kompyuter tizimlaridagi ma'lumotlarni himoya qilishda muhim jihatlardan biridir. Chou et al. (2019) tarmoq xavfsizligini ta'minlashda yangi texnologiyalarni qo'llashni o'rganib chiqqan va "firewall" tizimlarining tarmoqni himoya qilishda eng samarali vosita ekanligini ta'kidlagan. Shu bilan birga, Kaur va Singh (2017) o'zlarining tadqiqotlarida virtual maxfiy tarmoqlar (VPN) texnologiyasining tarmoq xavfsizligida o'rnini o'rgangan. Ularning tahliliga ko'ra, VPN texnologiyalari internet orqali ma'lumot uzatish jarayonida xavfsizlikni ta'minlash uchun samarali vosita hisoblanadi [4].

Zararlangan dasturlar (malware) va viruslar tizimlarning xavfsizligini tahdid qiladi. Gonzalez et al. (2018) antivirus va antimalware dasturlarining samaradorligini o'rganib chiqqan va ular zararli dasturlarni aniqlash va ularni bloklashda samarali ekanligini ko'rsatgan. Singh va Kumar (2020) esa, yangi zararli dasturlarni aniqlashda mashinani o'rganish (machine learning) texnologiyalaridan foydalanishning afzalliklarini tahlil qilgan. Ularning tadqiqotlari shuni ko'rsatadiki, mashinani o'rganish algoritmlari zararlangan dasturlarni aniqlashda an'anaviy usullarga qaraganda yuqori samaradorlikka ega. Sun'iy intellekt (AI) va mashinani o'rganish (ML) texnologiyalarining xavfsizlikni ta'minlashdagi roli tobora muhimlashib bormoqda. Xie et al. (2021) sun'iy intellektni kiberhujumlarni aniqlashda ishlatishning samaradorligini tahlil qilgan va AI texnologiyalari tizimlarning xavfsizligini real vaqt rejimida ta'minlashda yordam berishini ko'rsatgan. Patel va Desai (2019) mashinani o'rganish algoritmlarining tarmoq xavfsizligini

ta'minlashdagi o'rnini o'rganib chiqqan va bu texnologiyalarning yuqori samaradorligini ta'kidlagan. Kompyuter tizimlarida xavfsizlikni ta'minlash zamonaviy texnologiyalar bilan rivojlanayotgan soha bo'lib, kriptografiya, autentifikatsiya, tarmoq xavfsizligi, zararlangan dasturlardan himoya qilish va sun'iy intellekt kabi yondashuvlar uning asosiy vositalarini tashkil etadi. Adabiyotlar tahlili shuni ko'rsatadiki, zamonaviy xavfsizlik texnologiyalari yanada murakkablashib, tizimlarning xavfsizligini ta'minlashda samaradorlikni oshiradi. Tadqiqotlar xavfsizlikni ta'minlashning yangi yondashuvlari, shu jumladan mashinani o'rganish va sun'iy intellektni qo'llashni muvaffaqiyatli qo'llash imkoniyatlarini ko'rsatmoqda.

Muhokama. Kompyuter tizimlarida xavfsizlikni ta'minlash bugungi kunda har bir tashkilot, kompaniya va shaxs uchun dolzarb masalalardan biriga aylangan. Raqamli texnologiyalar, internet va tarmoq xizmatlarining kengayishi bilan birga, xavfsizlikka tahdidlar ham kuchaygan. Shu sababli, zamonaviy xavfsizlik yondashuvlari tizimlarni himoya qilishda muhim rol o'ynaydi. Adabiyotlar tahlilidan kelib chiqib, bir necha asosiy jihatlar va yondashuvlarni muhokama qilamiz. Kriptografiya kompyuter tizimlarida xavfsizlikni ta'minlashda eng muhim vositalardan biri sifatida qaraladi [5]. Kriptografik algoritmlar, xususan, AES, RSA kabi texnologiyalar ma'lumotlarning maxfiyligini va yaxlitligini saqlashda samarali ishlaydi. Biroq, har qanday texnologiya singari, kriptografiya ham zaif tomonlarga ega. Masalan, uzluksiz yangi kriptografik xujumlar va kuchli hisoblash quvvatlarining rivojlanishi tufayli ba'zi eski algoritmlar o'z ahamiyatini yo'qotmoqda. Bu esa yangi, yanada kuchli va ishonchli kriptografik yechimlarni izlash zaruratini tug'diradi. Shu bilan birga, kriptografiya tizimlarni himoya qilishda samarali bo'lsa-da, u faqatgina bir qismini tashkil etadi. Ma'lumotlarni himoya qilish uchun, shu jumladan autentifikatsiya va avtorizatsiya, tarmoq xavfsizligi kabi boshqa yondashuvlar ham muhimdir. Autentifikatsiya va avtorizatsiya jarayonlari kompyuter tizimlarida xavfsizlikni ta'minlash uchun juda muhim hisoblanadi. Ular foydalanuvchilarning tizimga kirishini va resurslarga bo'lgan huquqlarini boshqarish imkonini beradi. Yangi autentifikatsiya usullari, masalan, biometrik tizimlar va ikki faktorli autentifikatsiya (2FA), xavfsizlikni oshirishda samarali vositalar sifatida qaralmoqda. Biroq, autentifikatsiya tizimlarining samaradorligi har doim tashqi tahdidlarga qarshi

tura olmaydi. Biometrik ma'lumotlar, masalan, barmoq izlari yoki yuzni tanish tizimlari, foydalanuvchining kimligini tasdiqlashda samarali bo'lsa-da, ularni aldagan yoki noto'g'ri ishlatgan kiberjinoyatchilar tomonidan manipulyatsiya qilinishi mumkin. Shuning uchun, bu tizimlarning xavfsizligini oshirish uchun qo'shimcha chora-tadbirlar, masalan, foydalanuvchi xatti-harakatlarini kuzatish va tarmoq faoliyatini monitoring qilish zarur [6].

Tarmoq xavfsizligi — bu tizimlarni himoya qilishda muhim omil bo'lib, firewall, VPN, tarmoq monitoringi kabi vositalar orqali amalga oshiriladi. Hozirgi kunda tarmoq xavfsizligini ta'minlashda yangilangan texnologiyalar, masalan, "next-generation firewall" (NGFW) va tarmoqni kuzatishning ilg'or tizimlari, yanada samarali va murakkab xavf-xatarlarni aniqlash imkonini beradi. Shu bilan birga, tarmoq xavfsizligini ta'minlashda sun'iy intellekt va mashinani o'rganish (ML) texnologiyalaridan foydalanishning afzalliklari ko'rinmoqda. Masalan, mashinani o'rganish algoritmlari tarmoq faoliyatini real vaqtda tahlil qilish va yangi xavflarni aniqlashda yuqori samaradorlikka ega. Lekin, bu texnologiyalarni keng qo'llashda ba'zi muammolar ham mavjud. Avvalo, mashinani o'rganish tizimlari uchun katta hajmdagi ma'lumotlar va mukammal modelni yaratish talab etiladi, bu esa texnik jihatdan qiyin va vaqt talab qiladi. Bundan tashqari, sun'iy intellekt tizimlari ham o'z navbatida tahdidlarga, masalan, adversarial hujumlarga qarshi himoyasiz bo'lishi mumkin. Zararlangan dasturlar (malware) va viruslar kompyuter tizimlari uchun jiddiy tahdidlardan biridir. Antivirus va antimalware dasturlari, shuningdek, tarmoq xavfsizligi vositalari zararlangan dasturlarni aniqlashda samarali yordam beradi [7]. Biroq, yangi zararli dasturlarni aniqlashda mashinani o'rganish texnologiyalarining qo'llanishi samarali bo'lsa-da, bu tizimlar har doim yangilangan tahdidlarga qarshi turishda kamchiliklarga ega. Zararlangan dasturlarni aniqlashda samaradorlikni oshirish uchun, ko'p qatlamli xavfsizlik yondashuvlarini amalga oshirish zarur. Bu yondashuvlar antivirus dasturlaridan tashqari, tizim monitoringi, foydalanuvchi xatti-harakatlarini tahlil qilish va tarmoqdan keladigan xavf-xatarlarni aniqlashni o'z ichiga oladi. Sun'iy intellekt va mashinani o'rganish texnologiyalarining xavfsizlikni ta'minlashdagi roli tobora oshib bormoqda. Bu texnologiyalar xavfsizlik tahdidlarini oldindan prognoz qilish va tizimlarni real vaqtda himoya qilishda samarali vositalar

sifatida qaralmoqda. Sun'iy intellekt yordamida tizimlar kiberhujumlarni avtomatik ravishda aniqlay olishadi, lekin bu tizimlar ham ba'zi hollarda hujumlarni noto'g'ri tasniflash yoki xatolarga yo'l qo'yishi mumkin [8].

Mashinaning o'rganish imkoniyatlarini to'liq ishlatish uchun tizimlar katta ma'lumotlar bazasiga va aniq ma'lumotlarga asoslangan bo'lishi kerak. Bu esa resurslar va vaqtni talab qiladigan jarayon. Shu bilan birga, sun'iy intellektning xavfsizlikdagi rolini kengaytirish uchun, tizimlarning doimiy yangilanishi va takomillashtirilishi zarur. Kompyuter tizimlarida xavfsizlikni ta'minlash zamonaviy texnologiyalar yordamida yanada samarali amalga oshirilmoqda. Kriptografiya, autentifikatsiya, tarmoq xavfsizligi, zararli dasturlarni aniqlash, va sun'iy intellekt kabi yondashuvlar xavfsizlikni ta'minlashda muhim rol o'ynaydi. Biroq, har bir texnologiyaning o'ziga xos kuchli va zaif tomonlari mavjud. Shuning uchun, xavfsizlikni ta'minlashda ko'p qatlamli va integratsiyalangan yondashuvlar talab etiladi. Bu yondashuvlar xavfsizlikni mustahkamlashda samarali bo'lishi uchun doimiy ravishda yangilanib, yangi tahdidlarga qarshi kurashish uchun moslashtirilishi kerak.

Xulosa. Kompyuter tizimlarida xavfsizlikni ta'minlash bugungi raqamli davrda eng muhim masalalardan biri hisoblanadi. Zamonaviy tahdidlarning murakkablashuvi ushbu sohada innovatsion va tizimli yondashuvlarni talab qilmoqda. Kriptografik usullar, sun’iy intellekt asosidagi xavfsizlik tizimlari, tarmoq monitoringi va foydalanuvchi faoliyatini tahlil qilish kabi texnologiyalar yordamida axborot xavfsizligini yuqori darajada ta’minlash mumkin. Shuningdek, xavfsizlik madaniyatini shakllantirish, xodimlarni muntazam o‘qitish va global standartlarga asoslangan yondashuvlar joriy etilishi muhim ahamiyatga ega. Faqatgina texnologik emas, balki tashkiliy va huquqiy choralarni uyg‘unlashtirish orqali kompyuter tizimlarining xavfsizligini kompleks tarzda ta’minlash mumkin bo‘ladi.

Foydalanilgan adabiyotlar ro`yxati

1. Wang, Y., Li, Z., & Zhang, L. (2015). "A Study on the Security of Cryptographic Algorithms for Data Protection." International Journal of Computer Science and Information Security.

2. Zhang, H., Wang, L., & Li, J. (2016). "Evaluation of Two-Factor Authentication Systems for Network Security." Journal of Cryptographic Engineering.

3. Jain, A. K., & Singh, A. (2018). "Biometric Authentication: A Survey on Techniques and Applications." International Journal of Computer Applications.

4. Chou, T. S., Zhang, J., & Wang, R. (2019). "Advanced Techniques for Network Security in Modern IT Systems." International Journal of Computer Networks and Security.

5. Kaur, M., & Singh, M. (2017). "VPN-Based Security Solutions for Safe Internet Access." Journal of Network Security and Applications.

6. Gonzalez, M., Lopez, R., & Garcia, E. (2018). "Antivirus and Anti-malware Technologies: A Comparative Study." Journal of Information Security.

7. Singh, P., & Kumar, P. (2020). "Using Machine Learning for Malware Detection and Classification." International Journal of Computer Science and Cyber Security.

8. Xie, X., Li, Y., & Wang, Z. (2021). "Artificial Intelligence in Cybersecurity: Techniques and Applications." International Journal of Artificial Intelligence.