KOMPYUTER TARMOQLARIDA AXBOROT XAVFSIZLIGINI TA'MINLASH USULLARI

Xudayberdiyev Shuxrat Komilovich

Qarshi davlat texnika universiteti dotsent v.b.
E-mail. shxudayberdiyev@kstu.uz

KEYWORDS

axborot xavfsizligi, kompyuter tarmoqlari, kiberxavfsizlik, firewall, VPN, autentifikatsiya, kriptografiya, tarmoq himoyasi

ABSTRACT

Mazkur maqolada kompyuter tarmoqlarida axborot xavfsizligini ta'minlashning zamonaviy usullari va texnologiyalari tahlil qilingan. Tadqiqot davomida tarmoq xavfsizligiga tahdid soluvchi asosiy omillar, kiberhujumlar, zararli dasturlar hamda axborotni himoyalash vositalari o'rganildi. Shuningdek, kriptografik himoya, autentifikatsiya, firewall texnologiyalari, VPN tarmoqlari va intrusion detection tizimlarining samaradorligi yoritildi. Tadqiqot natijalari kompyuter tarmoqlarida axborot xavfsizligini ta'minlashda zamonaviy himoya mexanizmlaridan kompleks foydalanish muhim ahamiyatga ega ekanligini ko'rsatadi.

Kirish. Bugungi kunda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida kompyuter tarmoqlari jamiyatning barcha sohalarida keng qo'llanilmoqda. Xususan, davlat boshqaruvi, bank-moliya tizimi, ta'lim, sog'liqni saqlash va sanoat tarmoqlarida axborot almashinuvi asosan kompyuter tarmoqlari orqali amalga oshirilmoqda. Bu esa axborot xavfsizligini ta'minlash masalasini dolzarb ilmiy-amaliy muammolardan biriga aylantirmoqda.

Kompyuter tarmoqlarida uzatilayotgan ma'lumotlarning maxfiyligi, yaxlitligi va ishonchliligini saqlash zamonaviy kiberxavfsizlik tizimining asosiy vazifalaridan biri hisoblanadi. Hozirgi kunda turli xil kiberhujumlar, zararli dasturlar, fishing, DDoS hujumlari va ruxsatsiz kirish holatlarining ortib borishi axborot xavfsizligini ta'minlashning zamonaviy usullarini ishlab chiqishni talab etmoqda. Ayniqsa, global tarmoq texnologiyalarining rivojlanishi bilan axborot resurslarini himoyalash masalasi yanada murakkablashmoqda. Axborot xavfsizligini ta'minlashda kriptografik himoya usullari, autentifikatsiya tizimlari, firewall texnologiyalari, VPN tarmoqlari, intrusion detection va intrusion prevention tizimlari muhim ahamiyatga ega. Ushbu texnologiyalar tarmoq orqali uzatilayotgan ma'lumotlarni himoyalash, ruxsatsiz kirishni oldini olish hamda tarmoq xavfsizligini nazorat qilish imkonini beradi. Shu bilan birga, sun'iy intellekt va Machine Learning texnologiyalarining rivojlanishi kiberxavfsizlik tizimlarining samaradorligini oshirishga xizmat qilmoqda. Bugungi kunda ko'plab davlatlarda axborot xavfsizligini ta'minlash bo'yicha milliy strategiyalar ishlab chiqilib, zamonaviy himoya mexanizmlarini joriy etishga alohida e'tibor qaratilmoqda. O'zbekistonda ham raqamli iqtisodiyotni rivojlantirish jarayonida axborot xavfsizligini ta'minlash davlat siyosatining ustuvor yo'nalishlaridan biri sifatida belgilangan.

Mazkur maqolaning maqsadi kompyuter tarmoqlarida axborot xavfsizligini ta'minlashning zamonaviy usullari va texnologiyalarini tahlil qilish hamda ularning samaradorligini ilmiy jihatdan asoslashdan iborat.

Mavzuga oid adabiyotlarning tahlili. Kompyuter tarmoqlarida axborot xavfsizligini ta'minlash masalalari ko'plab xorijiy va mahalliy olimlar tomonidan tadqiq etilgan. Xususan, xorijiy olimlardan William Stallings kompyuter tarmoqlari va axborot xavfsizligi sohasidagi ilmiy ishlari bilan mashhur bo'lib, u "Data and Computer Communications" asarida tarmoq xavfsizligini ta'minlashda firewall (Tarmoqlararo ekran), autentifikatsiya va kriptografik himoya usullarining muhimligini ta'kidlaydi.[1]

Stuart Russell va Peter Norvig "Artificial Intelligence: A Modern Approach" (Sun'iy intellekt: zamonaviy yondashuv) asarida sun'iy

(cc) BY

intellekt texnologiyalaridan kiberxavfsizlik tizimlarida foydalanish tarmoqdagi tahdidlarni avtomatik aniqlash imkonini berishini qayd etadilar. Ularning fikricha, Machine Learning (Mashinali o‘qitish) algoritmlari asosida anomal holatlarni aniqlash zamonaviy axborot xavfsizligi tizimlarining asosiy yo‘nalishlaridan biridir.[2]

Shuningdek, Bruce Schneier axborot xavfsizligi va kriptografiya bo‘yicha olib borgan ilmiy tadqiqotlarida “ko‘p bosqichli himoya mexanizmlaridan foydalanish axborot xavfsizligini ta’minlashning eng samarali usuli” ekanligini ta’kidlaydi.[3]

Mahalliy olimlardan Muhammadjon Aripov axborot-kommunikatsiya texnologiyalari va kompyuter tarmoqlarining nazariy asoslarini tadqiq etgan. Olimning ilmiy ishlarida axborot tizimlari xavfsizligi va raqamli texnologiyalarni rivojlantirish masalalari yoritilgan.[4]

Azamat Abduqodirov ta’lim tizimida axborot texnologiyalaridan foydalanish hamda elektron ta’lim resurslarini yaratish bo‘yicha ilmiy izlanishlar olib borgan. Tadqiqotlarda raqamli texnologiyalar va axborot xavfsizligini ta’lim tizimiga integratsiyalash masalalariga alohida e’tibor qaratilgan.[5]

Tahlil qilingan ilmiy manbalar shuni ko‘rsatadiki, kompyuter tarmoqlarida axborot xavfsizligini ta’minlashda kriptografik himoya, autentifikatsiya, VPN, firewall hamda sun’iy intellekt asosidagi adaptiv himoya tizimlaridan kompleks foydalanish muhim ahamiyat kasb etadi. Shu bilan birga, zamonaviy kiberxavfsizlik tahdidlariga qarshi intellektual himoya tizimlarini takomillashtirish zarurati mavjud.

Tadqiqot metodologiyasi. Mazkur maqolada kompyuter tarmoqlarida axborot xavfsizligini ta’minlash usullarini o‘rganish va ularning samaradorligini aniqlashga qaratilgan metodologik yondashuvlardan foydalanildi. Tadqiqot jarayoni tizimli, kompleks va texnologik yondashuvlar asosida tashkil etildi. Kompyuter tarmoqlarida kriptografik himoya, autentifikatsiya, firewall, VPN va sun’iy intellekt asosidagi xavfsizlik texnologiyalaridan kompleks foydalanish axborot xavfsizligini samarali ta’minlash imkonini beradi degan gipoteza ilgari surildi:

1. **Kriptografik himoya usullari** Ma’lumotlarni shifrlash orqali axborotning maxfiyligini ta’minlaydi. AES, RSA, DES kabi algoritmlar tarmoq orqali uzatilayotgan ma’lumotlarni himoyalashda qo‘llaniladi.

2. **Autentifikatsiya va identifikatsiya tizimlari** Foydalanuvchilarni tekshirish va ruxsat berish jarayonini amalga oshiradi. Login-parol, biometrik autentifikatsiya va ikki bosqichli tekshiruv (2FA) keng qo‘llaniladi.

3. **Firewall texnologiyalari** Tarmoqqa kiruvchi va chiquvchi trafiklarni nazorat qiladi hamda ruxsatsiz kirishlarni cheklaydi. Firewall ichki tarmoqni tashqi tahdidlardan himoya qiladi.

4. **VPN (Virtual Private Network)** Internet orqali xavfsiz aloqa kanalini yaratadi. VPN texnologiyasi ma’lumotlarni shifrlangan holda uzatish imkonini beradi.

5. **Intrusion Detection System (IDS) va Intrusion Prevention System (IPS)** Tarmoqdagi shubhali faoliyatlarni aniqlaydi va kiberhujumlarning oldini oladi.

6. **Antivirus va antimalware tizimlari** Viruslar, trojanlar, spyware va boshqa zararli dasturlarni aniqlash hamda bartaraf etishga xizmat qiladi.

7. **Sun’iy intellekt va Machine Learning texnologiyalari** Tarmoqdagi anomal holatlarni avtomatik aniqlash va kiberxavfsizlik tahdidlarini prognoz qilish imkonini beradi.

8. **Ma’lumotlarni zaxiralash (Backup) tizimlari** Muhim axborotlarni saqlash va favqulodda holatlarda tiklash imkonini yaratadi.

9. **Raqamli sertifikat va elektron raqamli imzo (ERI)** Ma’lumotlarning haqiqiyligini va foydalanuvchi identifikatsiyasini tasdiqlash uchun qo‘llaniladi.

10. **Bulutli xavfsizlik texnologiyalari** Cloud computing tizimlarida ma’lumotlarni himoyalash va xavfsiz boshqarishni ta’minlaydi.

Mazkur usullardan kompleks foydalanish kompyuter tarmoqlarida axborot xavfsizligini yuqori darajada ta’minlash imkonini beradi. Zamonaviy axborot xavfsizligi tizimlarida sun’iy intellekt va Machine Learning texnologiyalaridan foydalanish ham kengayib bormoqda. Ushbu texnologiyalar yordamida tarmoqdagi anomal holatlar avtomatik aniqlanadi va ehtimoliy tahdidlar oldindan prognoz qilinadi.

(cc) BY

Bundan tashqari, antivirus dasturlari, ma'lumotlarni zaxiralash tizimlari hamda elektron raqamli imzo texnologiyalari axborot xavfsizligini ta'minlashning muhim vositalari hisoblanadi. Mazkur himoya mexanizmlaridan kompleks foydalanish kompyuter tarmoqlarida axborot xavfsizligini yuqori darajada ta'minlash imkonini beradi. Amaliy tadqiqot jarayonida Wireshark, Cisco Packet Tracer, Kali Linux, firewall va VPN texnologiyalari yordamida tarmoqdagi tahdidlar monitoring qilindi hamda himoya mexanizmlarining samaradorligi baholandi. Shuningdek, zararli trafiklarni aniqlash, ruxsatsiz kirishni cheklash va ma'lumotlarni shifrlash usullarining tarmoq xavfsizligiga ta'siri o'rganildi.

Tahlil va natijalar. Tadqiqot davomida kompyuter tarmoqlarida axborot xavfsizligini ta'minlashning zamonaviy usullari va texnologiyalarining samaradorligi tahlil qilindi. Tarmoq xavfsizligiga tahdid soluvchi asosiy omillar sifatida zararli dasturlar, fishing hujumlari, DDoS hujumlari, ruxsatsiz kirish va ma'lumotlarni o'g'irlash holatlari o'rganildi. Tahlillar natijasida zamonaviy kiberhujumlarning murakkablashib borayotgani va an'anaviy himoya usullari ayrim holatlarda yetarli darajada samarali bo'lmasligi mumkin.

Tadqiqot jarayonida firewall, VPN, antivirus tizimlari, intrusion detection system (IDS) va intrusion prevention system (IPS) texnologiyalarining funksional imkoniyatlari tahlil qilindi. Olingan natijalar firewall texnologiyalari tarmoqdagi ruxsatsiz trafiklarni filtrlashda samarali ekanligini ko'rsatdi. VPN texnologiyalaridan foydalanish esa ma'lumotlarni internet orqali xavfsiz uzatish imkonini yaratdi. Kriptografik himoya usullarining samaradorligi ham tahlil qilindi. Tadqiqot natijalariga ko'ra, AES va RSA algoritmlaridan foydalanish ma'lumotlarning maxfiyligini yuqori darajada ta'minlashi aniqlandi. Elektron raqamli imzo va autentifikatsiya tizimlari foydalanuvchilarni identifikatsiyalash va ruxsatsiz kirishni oldini olishda muhim ahamiyatga ega ekanligi qayd etildi.

Sun'iy intellekt va Machine Learning texnologiyalaridan foydalanish natijasida tarmoqdagi anomal holatlarni avtomatik aniqlash imkoniyati kengaygani kuzatildi. AI asosidagi tizimlar zararli trafiklarni tezkor aniqlash va ehtimoliy tahdidlarni prognoz qilishda yuqori samaradorlik ko'rsatdi.

Tahlillar natijasida kompyuter tarmoqlarida axborot xavfsizligini ta'minlashda:

- ko'p bosqichli himoya tizimlarini joriy etish;
- kriptografik himoya usullaridan foydalanish;
- zamonaviy firewall va VPN texnologiyalarini qo'llash;
- sun'iy intellekt asosidagi monitoring tizimlarini integratsiyalash yuqori samaradorlikka ega ekanligi aniqlandi.

Olingan natijalar zamonaviy himoya texnologiyalaridan kompleks foydalanish kompyuter tarmoqlarida axborot xavfsizligini ta'minlashning eng muhim omillaridan biri ekanligini ko'rsatdi.

Xulosa va takliflar. Mazkur tadqiqot natijalari kompyuter tarmoqlarida axborot xavfsizligini ta'minlash zamonaviy axborot-kommunikatsiya tizimlarining muhim tarkibiy qismi ekanligini ko'rsatdi. Tahlillar asosida kiberhujumlar, zararli dasturlar, ruxsatsiz kirish va ma'lumotlarni o'g'irlash holatlarining ortib borishi tarmoq xavfsizligini ta'minlashda zamonaviy himoya texnologiyalaridan foydalanishni talab etishi aniqlandi. firewall, VPN, kriptografik himoya, autentifikatsiya tizimlari, IDS/IPS hamda antivirus texnologiyalarining samaradorligi o'rganildi. Natijalar ushbu himoya mexanizmlaridan kompleks foydalanish tarmoq xavfsizligini sezilarli darajada oshirishini ko'rsatdi. Ayniqsa, sun'iy intellekt va Machine Learning texnologiyalarining tarmoq xavfsizligi tizimlariga integratsiyalashuvi tahdidlarni tezkor aniqlash va oldini olish imkoniyatlarini kengaytirishi aniqlandi.

Shuningdek, ma'lumotlarni shifrlash, foydalanuvchilarni autentifikatsiyalash va tarmoq trafiklarini monitoring qilish axborot xavfsizligini ta'minlashning asosiy omillaridan biri ekanligi ilmiy jihatdan asoslandi.

Tadqiqot natijalari asosida quyidagi takliflar ishlab chiqildi:

- kompyuter tarmoqlarida ko'p bosqichli himoya tizimlarini joriy etish;
- kriptografik himoya texnologiyalaridan keng foydalanish;

(cc) BY

- firewall va VPN texnologiyalarini doimiy yangilab borish;
- sun'iy intellekt asosidagi monitoring tizimlarini qo'llash;
- foydalanuvchilarning kiberxavfsizlik bo'yicha bilim va ko'nikmalarini oshirish;
- tarmoq xavfsizligi tizimlarini muntazam monitoring va auditdan o'tkazish.

Kelgusida kompyuter tarmoqlarida axborot xavfsizligini ta'minlashda sun'iy intellekt va adaptiv himoya tizimlarini yanada rivojlantirish, avtomatlashtirilgan xavfsizlik monitoringi hamda bulutli xavfsizlik texnologiyalarini takomillashtirish istiqbolli ilmiy yo'nalishlardan biri hisoblanadi.

Foydalanilgan adabiyotlar ro'uyxati

1. Stallings W. Data and Computer Communications. – New York: Pearson Education, 2017.
2. Russell S., Norvig P, Norvig P. Artificial Intelligence: A Modern Approach. – London: Pearson, 2021.
3. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C. – New York: Wiley, 2015.
4. Aripov M.M. Axborot-kommunikatsiya texnologiyalari. – Toshkent: O'zbekiston faylasuflari milliy jamiyati nashriyoti, 2021.
5. Abduqodirov A.A. Ta'limda axborot texnologiyalaridan foydalanish. – Toshkent: Fan va texnologiya, 2019.

(cc) BY