KOMPYUTER TARMOQLARI VA XAVFSIZLIK

Kodirov Akbar Shuhratovich
Shahrisabz davlat pedagogika insituti
"Matematika va amaliy matematika" kafedrasi katta o'qituvchisi
E-mail: akbar 2005ak@ gmail.com
ORSID: 0000-0002-3556-5770
Nurboboyeva Sevinch
Shahrisabz davlat pedagogika insituti talabasi
Maktabgacha ta’lim yo’nalishi 3-bosqich talabasi
E-mail:nurboboboyevasevinch647@gmail.com
Sodiqova Ruxshona
Shahrisabz davlat pedagogika insituti
Maktabgacha ta’lim yo’nalishi 3-bosqich talabasi
E-mail:ruxshonay04@gmail.com
https://doi.org/10.5281/zenodo.20037898

ANNOTATSIYA

Mazkur maqolada kompyuter tarmoqlari va axborot xavfsizligi masalalari kompleks tarzda tahlil qilinadi. Zamonaviy axborot-kommunikatsiya texnologiyalarining rivojlanishi sharoitida tarmoqlarda ma’lumotlar almashinuvi, ularning himoyasi, xavfsizlik tahdidlari va ularni bartaraf etish usullari ilmiy jihatdan yoritilgan. Shuningdek, tarmoq xavfsizligini ta’minlashda kriptografik usullar, autentifikatsiya mexanizmlari, xavfsizlik siyosatlari va zamonaviy texnologiyalarning roli tahlil qilingan. Tadqiqot natijalari asosida samarali himoya choralarini ishlab chiqish bo‘yicha tavsiyalar berilgan.

Kalit so‘zlar: kompyuter tarmoqlari, axborot xavfsizligi, kiberxavfsizlik, kriptografiya, tarmoq protokollari, autentifikatsiya, xavfsizlik siyosati

АННОТАЦИЯ

В данной статье комплексно рассматриваются вопросы компьютерных сетей и информационной безопасности. В условиях стремительного развития информационно-коммуникационных технологий анализируются процессы передачи данных в сетях, угрозы безопасности и методы их предотвращения. Особое внимание уделено криптографическим методам, механизмам аутентификации, политике безопасности и современным технологиям защиты информации. На основе исследования предложены рекомендации по обеспечению эффективной защиты сетевых систем.

Ключевые слова: компьютерные сети, информационная безопасность, кибербезопасность, криптография, сетевые протоколы, аутентификация, защита данных

ABSTRACT

This article provides a comprehensive analysis of computer networks and information security. In the context of rapid development of information and communication technologies, the study explores data transmission processes, security threats, and mitigation techniques. Special attention is given to cryptographic methods, authentication mechanisms, security policies, and modern protection technologies. Based on the research findings, recommendations are proposed to enhance the effectiveness of network security systems.

Keywords: computer networks, information security, cybersecurity, cryptography, network protocols, authentication, data protection

KIRISH

Zamonaviy axborotlashgan jamiyatda kompyuter tarmoqlari va axborot xavfsizligi tushunchalari nafaqat texnik soha doirasida, balki global ijtimoiy-iqtisodiy tizimlarning ajralmas qismi sifatida qaralmoqda. Raqamli transformatsiya jarayonlari jadallashib borayotgan hozirgi davrda davlat boshqaruvi, bank-moliya sektori, sog‘liqni saqlash tizimi, ta’lim va sanoat kabi muhim sohalar to‘liq yoki qisman kompyuter tarmoqlariga bog‘langan. Bu esa axborot almashinuvi hajmining keskin oshishiga, ma’lumotlarning tezkorligi va aniqligiga bo‘lgan talabning ortishiga olib kelmoqda.

Kompyuter tarmoqlari — bu bir nechta hisoblash qurilmalarining o‘zaro bog‘langan tizimi bo‘lib, ular orqali ma’lumotlar uzatiladi va qayta ishlanadi. Ushbu tizimlar lokal (LAN), mintaqaviy (MAN) va global (WAN) ko‘rinishlarda mavjud bo‘lib, ular orasida Internet eng yirik global tarmoq hisoblanadi. Tarmoqlarning rivojlanishi bilan birga axborot resurslari hajmi ham ortib bormoqda, bu esa ularni himoya qilish zaruratini yanada kuchaytiradi.

Axborot xavfsizligi esa axborotning maxfiyligi (confidentiality), yaxlitligi (integrity) va mavjudligini (availability) ta’minlashga qaratilgan choralar majmuasidir. Ushbu uchlik “CIA triadasi” deb nomlanadi va zamonaviy xavfsizlik konsepsiyasining asosini tashkil etadi. Biroq bugungi kunda xavfsizlik masalalari faqat shu uch komponent bilan cheklanmay, autentifikatsiya, avtorizatsiya, inkor etib bo‘lmaslik (non-repudiation) kabi qo‘shimcha elementlarni ham qamrab oladi.

Axborot xavfsizligiga tahdidlar turli shakllarda namoyon bo‘ladi. Ular ichida zararli dasturlar (malware), fishing hujumlari (phishing), xizmatdan voz kechishga majbur qiluvchi hujumlar (DDoS), ijtimoiy muhandislik (social engineering) kabi usullar keng tarqalgan. Ayniqsa, ransomware turidagi hujumlar oxirgi yillarda jiddiy muammo sifatida ko‘rilmoqda, chunki ular foydalanuvchi ma’lumotlarini shifrlab, to‘lov talab qiladi.

Shuningdek, zamonaviy texnologiyalar rivoji bilan yangi xavf manbalari ham yuzaga kelmoqda. Masalan, Internet of Things (IoT) qurilmalarining keng tarqalishi xavfsizlik darajasini pasaytirishi mumkin, chunki bu qurilmalar ko‘pincha yetarli darajada himoyalanmagan bo‘ladi. Bulutli hisoblash (cloud computing) texnologiyalarida esa ma’lumotlarning markazlashgan holda saqlanishi yangi xavfsizlik muammolarini keltirib chiqaradi.

Bugungi kunda kiberxavfsizlik davlat darajasidagi strategik muhim yo‘nalishlardan biriga aylangan. Ko‘plab davlatlar milliy kiberxavfsizlik strategiyalarini ishlab chiqib, axborot infratuzilmasini himoya qilish choralarini kuchaytirmoqda. O‘zbekiston Respublikasida ham raqamli iqtisodiyot va elektron hukumat tizimining rivojlanishi bilan bog‘liq holda axborot xavfsizligiga alohida e’tibor qaratilmoqda.

Mazkur maqolaning asosiy maqsadi kompyuter tarmoqlari va axborot xavfsizligining nazariy va amaliy jihatlarini kompleks tahlil qilish, mavjud tahdidlarni o‘rganish va ularni bartaraf etishning samarali usullarini aniqlashdan iborat. Tadqiqot doirasida zamonaviy xavfsizlik texnologiyalari, kriptografik algoritmlar, tarmoq himoya vositalari va xavfsizlik siyosatlari chuqur o‘rganiladi.

ADABIYOTLAR TAHLILI

Kompyuter tarmoqlari va axborot xavfsizligi sohasida ko‘plab ilmiy tadqiqotlar olib borilgan. Klassik yondashuvlarda tarmoq xavfsizligi asosan texnik vositalar orqali ta’minlangan bo‘lsa, zamonaviy tadqiqotlarda kompleks yondashuv ustuvorlik kasb etmoqda.

Ilk tadqiqotlarda tarmoqlarni himoyalash uchun asosan apparat va dasturiy vositalar qo‘llanilgan. Masalan, xavfsizlik devorlari (firewall), antivirus dasturlar va IDS/IPS tizimlari keng qo‘llanilgan. Keyinchalik esa kriptografik algoritmlar, autentifikatsiya va avtorizatsiya tizimlari rivojlandi.

Zamonaviy ilmiy ishlar quyidagi yo‘nalishlarga qaratilgan:

- Bulutli texnologiyalarda xavfsizlik
- IoT (Internet of Things) qurilmalarini himoyalash
- Sun’iy intellekt asosida kiberxavfsizlikni ta’minlash
- Blokcheyn texnologiyalaridan foydalanish

Shuningdek, ilmiy adabiyotlarda inson omili ham muhim xavf manbai sifatida ko‘rib chiqilmoqda. Foydalanuvchilarning bilim darajasi va xavfsizlik madaniyati pastligi ko‘plab muammolarni keltirib chiqarmoqda.

MUHOKAMA

Kompyuter tarmoqlarida xavfsizlikni ta’minlash ko‘p qatlamli yondashuvni talab etadi. Tarmoq xavfsizligi quyidagi asosiy komponentlardan iborat:

Birinchidan, identifikatsiya va autentifikatsiya tizimlari foydalanuvchini aniqlash va uning haqiqiyligini tasdiqlash uchun xizmat qiladi. Zamonaviy tizimlarda biometrik autentifikatsiya, ikki faktorli tasdiqlash keng qo‘llanilmoqda.

Ikkinchidan, kriptografiya ma’lumotlarni shifrlash orqali ularning maxfiyligini ta’minlaydi. Simmetrik va asimmetrik shifrlash algoritmlari keng qo‘llaniladi.

Uchinchidan, tarmoq monitoringi va tahdidlarni aniqlash tizimlari (IDS/IPS) xavf-xatarlarni oldindan aniqlash imkonini beradi.

To‘rtinchidan, xavfsizlik siyosati va boshqaruv tizimi tashkilot miqyosida yagona himoya strategiyasini ishlab chiqishga xizmat qiladi.

Bugungi kunda eng katta muammolardan biri — kiberhujumlarning murakkablashib borayotganidir. DDoS hujumlari, phishing, ransomware kabi tahdidlar tobora ko‘paymoqda.

NATIJALAR

Tadqiqot natijalari shuni ko‘rsatadiki:

- Kompyuter tarmoqlarida xavfsizlikni ta’minlash kompleks yondashuvni talab qiladi
- Kriptografik usullar ma’lumotlarni himoyalashda samarali vosita hisoblanadi
- Inson omili xavfsizlikdagi eng zaif bo‘g‘inlardan biri bo‘lib qolmoqda
- Zamonaviy texnologiyalar (AI, blockchain) xavfsizlik darajasini oshirishda muhim rol o‘ynaydi

Shuningdek, tashkilotlarda muntazam audit va xavfsizlik treninglarini o‘tkazish zarur.

XULOSA

Yuqoridagi tahlillar asosida shuni ta’kidlash mumkinki, kompyuter tarmoqlari va axborot xavfsizligi zamonaviy axborot jamiyatining eng muhim infratuzilma elementlaridan biri hisoblanadi. Tarmoqlarning kengayishi va raqamli texnologiyalarning chuqur integratsiyalashuvi natijasida axborot resurslari qiymati keskin oshdi va ular strategik resurs darajasiga ko‘tarildi. Shu sababli ularni himoya qilish masalasi global miqyosdagi dolzarb muammoga aylandi.

Tadqiqot natijalari shuni ko‘rsatadiki, axborot xavfsizligini ta’minlashda yagona texnik vositalarga tayanish yetarli emas. Bu jarayon kompleks yondashuvni talab qiladi, ya’ni texnologik, tashkiliy va inson omillari uyg‘un holda ko‘rib chiqilishi lozim. Xususan, xavfsizlik siyosatini ishlab chiqish, foydalanuvchilarni o‘qitish, xavfsizlik auditlarini o‘tkazish va zamonaviy himoya vositalarini joriy etish birgalikda amalga oshirilgandagina samarali natija beradi.

Kriptografiya va autentifikatsiya mexanizmlari axborotni himoya qilishning asosiy vositalari sifatida o‘z ahamiyatini saqlab qolmoqda. Shu bilan birga, sun’iy intellekt va mashinaviy o‘rganish texnologiyalarining rivojlanishi kiberxavfsizlik sohasida yangi imkoniyatlarni yaratmoqda. Masalan, avtomatlashtirilgan tahdidlarni aniqlash tizimlari real vaqt rejimida hujumlarni aniqlash va ularga qarshi choralar ko‘rish imkonini beradi.

Biroq, xavfsizlik tizimlarining rivojlanishiga qaramay, kiberjinoyatchilik ham takomillashib bormoqda. Bu esa doimiy ravishda yangi himoya usullarini ishlab chiqishni talab etadi. Ayniqsa, nol kunlik (zero-day) zaifliklar va murakkab kiberhujumlar mavjud xavfsizlik tizimlari uchun jiddiy sinov bo‘lib qolmoqda.

Shuningdek, inson omili hanuzgacha eng zaif bo‘g‘in sifatida qolmoqda. Foydalanuvchilarning ehtiyotsizligi, xavfsizlik qoidalariga amal qilmasligi yoki yetarli bilimga ega emasligi ko‘plab xavfsizlik buzilishlariga sabab bo‘lmoqda. Shu sababli axborot xavfsizligi madaniyatini oshirish va doimiy ravishda malaka oshirish ishlari muhim ahamiyatga ega.

Kelgusida kompyuter tarmoqlari va axborot xavfsizligi sohasida quyidagi yo‘nalishlar ustuvor bo‘lishi kutilmoqda:

- Sun’iy intellekt asosida avtomatlashtirilgan xavfsizlik tizimlari
- Kvant kriptografiyasi va yangi shifrlash algoritmlari
- IoT va smart tizimlar xavfsizligini ta’minlash
- Bulutli infratuzilmalarda xavfsizlikni kuchaytirish

Axborot xavfsizligi uzluksiz jarayon bo‘lib, u doimiy monitoring, tahlil va takomillashtirishni talab etadi. Faqatgina kompleks va tizimli yondashuv orqali kompyuter tarmoqlarida yuqori darajadagi xavfsizlikni ta’minlash mumkin.

Adabiyotlar, References, Литературы:

1. Stallings W. Network Security Essentials. – Pearson, 2020
2. Kurose J., Ross K. Computer Networking: A Top-Down Approach. – Pearson, 2021
3. Schneier B. Applied Cryptography. – Wiley, 2019
4. Tanenbaum A. Computer Networks. – Prentice Hall, 2020
5. ISO/IEC 27001 Information Security Standard
6. O‘zbekiston Respublikasi “Axborot xavfsizligi to‘g‘risida”gi qonuni
7. NIST Cybersecurity Framework, 2022
8. Cisco Networking Academy Materials
9. ENISA Cybersecurity Reports
10. IEEE Security and Privacy Journal maqolalari