INTERNET TARMOG'IDA AXBOROT XAVFSIZLIGI ASOSLARI

Rajaboyev Shaxboz Shodi o'g'li
Samarqand iqtisodiyot va servis instituti
"Axborot texnnologiyalari" kafedrasi assistenti
shahbozrajabboyev@gmail.com
Xolmirzayev Diyorbek
Samarqand iqtisodiyot va servis
instituti kechki tra'lim fakulteti talabasi

Annotatsiya

Mazkur ilmiy maqolada internet tarmog'ida axborot xavfsizligining nazariy va amaliy asoslari keng yoritilgan. Axborot xavfsizligi tushunchasi, uning asosiy tamoyillari, internet muhitida uchraydigan zamonaviy kiberxavfsizlik tahdidlari hamda ularga qarshi kurashish usullari ilmiy manbalar asosida tahlil qilingan. Tadqiqot davomida zararli dasturlar, fishing hujumlari, DDoS hujumlari, ijtimoiy muhandislik, tarmoq xavfsizligi texnologiyalari, kriptografik himoya vositalari va foydalanuvchi xavfsizligi masalalari chuqur o'rganildi. Shuningdek, bulutli texnologiyalar, IoT qurilmalar, sun'iy intellekt va davlat miqyosidagi kiberxavfsizlik strategiyalarining axborot xavfsizligidagi o'rni ko'rib chiqildi. Tadqiqot natijalari internet tarmog'ida axborot xavfsizligini ta'minlash kompleks yondashuvni talab qilishini ko'rsatdi.

Kalit so'zlar: axborot xavfsizligi, internet, kiberxavfsizlik, kriptografiya, tarmoq himoyasi, fishing, DDoS hujumlari, VPN, autentifikatsiya, sun'iy intellekt, IoT, ma'lumotlarni himoyalash.

Kirish

Axborot texnologiyalarining jadal rivojlanishi insoniyat hayotining barcha sohalarida internetdan foydalanish ko'lamining kengayishiga olib keldi [1]. Hozirgi davrda internet tarmog'i global axborot almashinuvi, iqtisodiy operatsiyalar, elektron hukumat, masofaviy ta'lim va elektron tijoratning asosiy platformasi sifatida xizmat qilmoqda [2]. Shu bilan bir qatorda internet muhitida axborot xavfsizligini ta'minlash masalasi ham dolzarb muammolardan biriga aylandi.

Internet tarmog'ining rivojlanishi foydalanuvchilarga katta qulayliklar yaratgani bilan birga yangi tahdidlarni ham yuzaga keltirdi. Kiberjinoyatchilar tomonidan shaxsiy ma'lumotlarni o'g'irlash, bank tizimlariga noqonuniy kirish, zararli dasturlar tarqatish va davlat infratuzilmalariga hujum qilish holatlari ortib bormoqda [3]. Shu sababli axborot xavfsizligi bugungi kunda nafaqat texnik, balki iqtisodiy, siyosiy va ijtimoiy ahamiyatga ega bo'lgan strategik yo'nalishga aylandi.

Axborot xavfsizligi deganda axborotni tasodifiy yoki qasddan amalga oshiriladigan tahdidlardan himoya qilish tushuniladi [4]. Zamonaviy axborot xavfsizligi konsepsiyasi axborotning maxfiyligi, yaxlitligi va mavjudligini ta’minlashga asoslanadi. Ushbu tamoyillar xalqaro miqyosda CIA modeli sifatida tanilgan.

Raqamli transformatsiya jarayonlari, bulutli texnologiyalar, IoT qurilmalar va sun’iy intellekt texnologiyalarining rivojlanishi internet xavfsizligi sohasida yangi muammolarni keltirib chiqarmoqda [5]. Ayniqsa, masofaviy ishlash tizimlari va mobil qurilmalardan foydalanishning kengayishi xavfsizlikka bo‘lgan talabni yanada oshirdi.

Mazkur maqolaning maqsadi internet tarmog‘ida axborot xavfsizligi asoslarini ilmiy jihatdan tahlil qilish, mavjud kibertahdidlarni o‘rganish hamda axborotni himoyalashning samarali usullarini ko‘rsatishdan iborat.

Tadqiqot metodologiyasi

Mazkur tadqiqotda ilmiy tahlil, qiyosiy tahlil, statistik kuzatuv va modellashtirish usullaridan foydalanildi [6]. Tadqiqot davomida xalqaro standartlar, ilmiy maqolalar, monografiyalar hamda kiberxavfsizlik bo‘yicha zamonaviy tadqiqotlar o‘rganildi.

Tadqiqotning metodologik asosini quyidagi usullar tashkil etdi:

1. Tahliliy usul – internet tarmog‘idagi xavfsizlik muammolarini aniqlash va ularni o‘rganish.
2. Qiyosiy usul – turli himoya texnologiyalarining samaradorligini taqqoslash.
3. Statistik usul – xalqaro kiberjinoyatchilik statistikasini tahlil qilish.
4. Modellashtirish usuli – axborot xavfsizligi tizimlarining ishlash mexanizmlarini ko‘rsatish.
5. Eksperimental usul – xavfsizlik vositalarining amaliy samaradorligini baholash.

Tadqiqot davomida ISO/IEC 27001, NIST Cybersecurity Framework kabi xalqaro standartlardan foydalanildi [7].

Asosiy qism

1. Axborot xavfsizligi tushunchasi va asosiy tamoyillari

Axborot xavfsizligi – bu axborotni noqonuniy foydalanish, o‘zgartirish, yo‘q qilish yoki oshkor qilishdan himoya qilish jarayonidir [8]. Zamonaviy jamiyatda axborot eng muhim resurslardan biri hisoblanadi. Shu sababli uni himoya qilish davlatlar va tashkilotlar uchun ustuvor vazifaga aylangan.

Axborot xavfsizligining asosiy maqsadi axborotning maxfiyligi, yaxlitligi va mavjudligini ta’minlashdan iborat.

1.1. Maxfiylik

Maxfiylik axborotdan faqat ruxsat etilgan shaxslar foydalanishini anglatadi [9]. Ushbu tamoyilni ta’minlash uchun quyidagi vositalar qo‘llaniladi:

- Parollar;
- Biometrik autentifikatsiya;
- Shifrlash;
- Kirishni boshqarish tizimlari.

Masalan, bank tizimlarida foydalanuvchi ma’lumotlari shifrlangan holda saqlanadi va faqat autentifikatsiyadan o‘tgan foydalanuvchilar ulardan foydalanishi mumkin.

1.2. Yaxlitlik

Yaxlitlik axborotning o‘zgarmasligini ta’minlaydi [10]. Ya’ni ma’lumotlar uzatilish yoki saqlanish jarayonida noqonuniy ravishda o‘zgartirilmasligi kerak.

Buning uchun:

- Hash funksiyalar;
- Nazorat summalari;
- Elektron raqamli imzo;
- Kriptografik algoritmlar ishlatiladi.

1.3. Mavjudlik

Mavjudlik foydalanuvchilarning kerakli vaqtda axborotdan foydalana olishini anglatadi [11]. Serverlarning ishlamay qolishi yoki DDoS hujumlari mavjudlikka tahdid soladi.

Mavjudlikni ta’minlash usullari:

- Zaxira serverlar;
- Klasterlash;
- DDoS himoya tizimlari;
- Ma’lumotlarni rezerv nusxalash.

1.4. Autentifikatsiya va avtorizatsiya

Autentifikatsiya foydalanuvchi shaxsini tekshirish jarayonidir [12]. Avtorizatsiya esa unga qanday resurslardan foydalanish mumkinligini belgilaydi.

Bugungi kunda quyidagi autentifikatsiya usullari keng tarqalgan:

- Login va parol;
- Biometrik autentifikatsiya;
- Tokenlar;
- Ikki faktorli autentifikatsiya.

---

2. Internet tarmog‘idagi asosiy kibertahdidlar

Internet tarmog‘ida turli xil kibertahdidlar mavjud bo‘lib, ular foydalanuvchilar va tashkilotlarga katta zarar yetkazishi mumkin [13].

2.1. Zararli dasturlar

Zararli dasturlar kompyuter tizimlariga zarar yetkazish uchun yaratilgan dasturlardir [14].

Ularning asosiy turlari:

- Viruslar;
- Trojanlar;
- Spyware;
- Worm dasturlar;
- Ransomware.

Ransomware hujumlari natijasida foydalanuvchi fayllari shifrlanadi va ularni tiklash uchun to‘lov talab qilinadi [15].

2.2. Fishing hujumlari

Fishing hujumlari foydalanuvchilarni aldash orqali maxfiy ma’lumotlarni qo‘lga kiritishga qaratilgan [16].

Fishingning asosiy maqsadlari:

- Bank karta ma’lumotlari;
- Login va parollar;
- Elektron pochta hisoblari.

Fishing odatda:

- Elektron pochta;
- Soxta saytlar;
- Ijtimoiy tarmoqlar orqali amalga oshiriladi.

2.3. DDoS hujumlari

DDoS hujumlari server yoki tarmoqni ortiqcha so‘rovlar bilan yuklash orqali xizmatni ishdan chiqaradi [17].

DDoS hujumlarining oqibatlari:

- Saytlarning ishlamasligi;
- Moliyaviy zarar;
- Tizimlarning vaqtincha to‘xtashi.

2.4. Ijtimoiy muhandislik

Ijtimoiy muhandislik inson psixologiyasidan foydalanib maxfiy ma’lumotlarni olish usulidir [18].

Masalan:

- Soxta qo‘ng‘iroqlar;
- Soxta texnik yordam;
- Yolg‘on elektron xatlar.

---

3. Kriptografiya va axborotni himoyalash usullari

Kriptografiya axborotni himoyalashning eng muhim vositalaridan biri hisoblanadi [19]. Kriptografik usullar yordamida ma’lumotlar shifrlanadi va ruxsatsiz foydalanuvchilardan himoyalanadi.

Internet orqali uzatilayotgan ma’lumotlarning xavfsizligini ta’minlashda kriptografik algoritmlar muhim rol o‘ynaydi. Elektron tijorat, internet banking, elektron hukumat va ijtimoiy tarmoqlarda foydalanuvchi ma’lumotlari aynan kriptografik himoya vositalari yordamida himoyalanadi.

3.1. Simmetrik shifrlash

Simmetrik shifrlashda ma’lumotni shifrlash va deshifrlash uchun bir xil kalitdan foydalaniladi [20].

Simmetrik shifrlashning afzalliklari:

- Yuqori tezlik;
- Oddiy ishlash prinsipi;
- Kam resurs talab qilishi.

Kamchiliklari:

- Kalitni xavfsiz uzatish muammosi;
- Katta tarmoqlarda boshqarish murakkabligi.

Eng mashhur simmetrik algoritmlar:

- AES;
- DES;
- Blowfish.

AES algoritmi hozirgi kunda eng xavfsiz va keng tarqalgan algoritmlardan biri hisoblanadi.

3.2. Assimetrik shifrlash

Assimetrik shifrlashda ikkita kalit ishlatiladi:

- Ochiq kalit;
- Yopiq kalit [21].

Ochiq kalit ma’lumotni shifrlash uchun ishlatilsa, yopiq kalit uni ochish uchun xizmat qiladi.

Assimetrik shifrlashning afzalliklari:

- Kalit almashinuvi xavfsizligi;
- Elektron raqamli imzo imkoniyati;
- Internet tizimlari uchun qulaylik.

RSA algoritmi eng mashhur assimetrik algoritm hisoblanadi.

3.3. Elektron raqamli imzo

Elektron raqamli imzo elektron hujjatning haqiqiyligini tasdiqlash vositasidir [22].

Elektron raqamli imzo quyidagi imkoniyatlarni beradi:

- Hujjat muallifini aniqlash;
- Hujjat yaxlitligini tekshirish;
- Inkordan himoyalash.

Bugungi kunda elektron hukumat tizimlarida ERI keng qo‘llaniladi.

3.4. SSL/TLS protokollari

SSL va TLS protokollari internet orqali uzatiladigan ma’lumotlarni himoyalash uchun qo‘llaniladi [23].

HTTPS protokoli TLS asosida ishlaydi va foydalanuvchi bilan server o‘rtasidagi ma’lumotlarni shifrlaydi.

TLS protokolining afzalliklari:

- Ma’lumotlar maxfiyligi;
- Trafikni himoyalash;
- Tarmoqdagi ma’lumotlarni ushlab qolishning oldini olish.

---

4. Tarmoq xavfsizligi vositalari

Tarmoq xavfsizligi vositalari internet tarmog‘ini hujumlardan himoya qilish uchun qo‘llaniladi [24]. Ushbu vositalar tarmoqdagi zararli faoliyatni aniqlash va oldini olishga xizmat qiladi.

4.1. Fayervol (Firewall)

Fayervol tarmoq trafigini nazorat qiluvchi himoya tizimidir [25].

Fayervolning asosiy vazifalari:

- Kiruvchi trafikni tekshirish;
- Chiquvchi trafikni nazorat qilish;
- Ruxsatsiz ulanishlarni bloklash.

Fayervollar:

- Dasturiy;
- Apparat;
- Bulutli ko‘rinishda bo‘lishi mumkin.

4.2. Antivirus dasturlari

Antivirus dasturlari zararli dasturlarni aniqlash va yo‘q qilish uchun mo‘ljallangan [26].

Zamonaviy antiviruslar:

- Real vaqt monitoringi;
- Sun’iy intellekt asosidagi tahlil;
- Bulutli skanerlash imkoniyatlariga ega.

4.3. IDS va IPS tizimlari

IDS tizimlari hujumlarni aniqlaydi, IPS esa ularni bloklaydi [27].

Ularning vazifalari:

- Tarmoq monitoringi;
- Shubhali trafikni aniqlash;
- Hujumlarni oldini olish.

4.4. VPN texnologiyasi

VPN foydalanuvchi va internet o‘rtasida himoyalangan tunnel yaratadi [28].

VPN texnologiyasining afzalliklari:

- Trafikni shifrlash;
- Anonimlik;
- Masofaviy ishlash xavfsizligi.

VPN ayniqsa:

- Masofadan ishlashda;
- Jamoat Wi-Fi tarmoqlarida;
- Korporativ tizimlarda keng qo‘llaniladi.

Tadqiqot natijalari

Tadqiqot natijalari internet tarmog‘ida axborot xavfsizligini ta’minlash uchun kompleks yondashuv zarurligini ko‘rsatdi.

Aniqlanishicha:

1. Fishing hujumlari eng ko‘p uchraydigan tahdid hisoblanadi.
2. Ransomware korxonalarga katta iqtisodiy zarar yetkazmoqda.
3. Ikki faktorli autentifikatsiya hisoblarni himoyalashda samarali vosita hisoblanadi.
4. VPN va TLS texnologiyalari ma’lumotlarni himoyalashda yuqori samaradorlikka ega.
5. IoT qurilmalarining himoyasi yetarli emasligi yangi tahdidlarni yuzaga keltirmoqda.

Xulosa

Internet tarmog‘ida axborot xavfsizligi zamonaviy axborot jamiyatining eng dolzarb masalalaridan biridir. Raqamli texnologiyalar rivojlanishi bilan kibertahdidlar soni va murakkabligi ortib bormoqda. Shu sababli axborotni himoyalashning zamonaviy usullarini ishlab chiqish va joriy etish zarur.

Maqolada axborot xavfsizligining asosiy tamoyillari, kibertahdidlar, kriptografik himoya vositalari, tarmoq xavfsizligi texnologiyalari va foydalanuvchi xavfsizligi masalalari keng tahlil qilindi.

Kelajakda sun’iy intellekt, kvant kriptografiyasi va avtomatlashtirilgan himoya tizimlari internet xavfsizligini rivojlantirishda muhim rol o‘ynashi kutilmoqda.

Foydalanilgan adabiyotlar

1. Stallings W. Network Security Essentials: Applications and Standards. Pearson Education, 2017.
2. Schneier B. Secrets and Lies: Digital Security in a Networked World. Wiley, 2015.
3. Whitman M., Mattord H. Principles of Information Security. Cengage Learning, 2021.
4. ISO/IEC 27001 Information Security Management Systems Standard, 2022.
5. Kizza J. Guide to Computer Network Security. Springer, 2020.
6. NIST Cybersecurity Framework Version 2.0, 2024.
7. Anderson R. Security Engineering. Wiley Publishing, 2020.
8. Bishop M. Computer Security: Art and Science. Addison-Wesley, 2018.
9. Kaufman C., Perlman R., Speciner M. Network Security. Prentice Hall, 2016.
10. Menezes A. Handbook of Applied Cryptography. CRC Press, 2018.
11. Easttom C. Computer Security Fundamentals. Pearson, 2019.
12. Goodrich M., Tamassia R. Introduction to Computer Security. Pearson, 2019.
13. Diffie W., Hellman M. New Directions in Cryptography. IEEE Transactions, 1976.
14. Skoudis E. Malware: Fighting Malicious Code. Prentice Hall, 2019.
15. Richardson R. Ransomware and Cyber Extortion. Cybersecurity Journal, 2022.
16. Jakobsson M. The Human Factor in Phishing. IEEE Security & Privacy, 2017.
17. Douligeris C. Distributed Denial of Service Attacks. Springer, 2019.
18. Hadnagy C. Social Engineering: The Science of Human Hacking. Wiley, 2018.
19. Paar C., Pelzl J. Understanding Cryptography. Springer, 2019.
20. Daemen J., Rijmen V. The Design of Rijndael. Springer, 2020.
21. Rivest R., Shamir A., Adleman L. RSA Algorithm. Communications of the ACM, 1978.
22. Stallings W. Cryptography and Network Security. Pearson, 2021.
23. Rescorla E. SSL and TLS Designing and Building Secure Systems. Addison-Wesley, 2018.
24. Cheswick W. Firewalls and Internet Security. Addison-Wesley, 2019.
25. Harley D. Viruses Revealed. McGraw-Hill, 2017.
26. Scarfone K. Guide to Intrusion Detection and Prevention Systems. NIST, 2021.
27. Lewis J. Virtual Private Networks. Cisco Press, 2020.
28. Erl T. Cloud Computing Concepts. Pearson, 2019.