ISSN 3060-4567

TARMOQLARDA KIBER XAVFSIZLIKNI TA'MINLASHDA RISKLARNI BOSHQARISH METODLARINI BAHOLASH

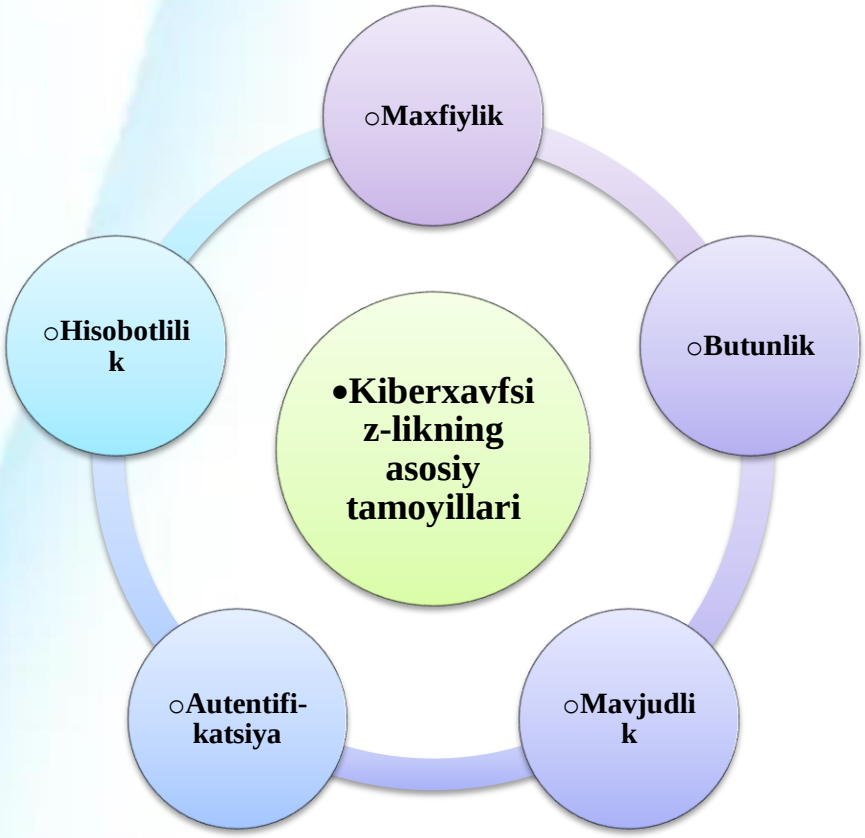
Sherqulov Abror Xujaqul o'g'li
O`zbekiston Respublikasi
Toshkent Bank-moliya akademiyasi

Bugungi kunda texnologiyalar rivojlanishi bilan tarmoqlarga asoslangan infratuzilmalar ko‘lamining kengayishi kuzatilmoqda. Shu bilan birga, kiberxavfsizlik sohasida yangi tahdidlar va zaifliklar paydo bo‘lmoqda. Davlat va xususiy tashkilotlar, korxonalar va shaxsiy foydalanuvchilar uchun kiberxavfsizlikni ta'minlash dolzarb muammo sifatida namoyon bo‘lyapti. Ayniqsa, tarmoqlarda ma'lumotlar xavfsizligini ta'minlash va kiberhujumlarga qarshi himoya choralarini ko‘rish zamonaviy dunyoda ustuvor ahamiyat kasb etadi. Ushbu sohadagi muammolarni hal qilish uchun samarali risklarni boshqarish metodlarini ishlab chiqish va baholash talab etiladi.

So‘nggi yillarda tarmoqlarda sodir bo‘layotgan kibertahdidlar soni va murakkabligi oshib bormoqda. Xakerlik hujumlari, ransomware, DDoS hujumlar, phishing va boshqa turdagi tahdidlar jiddiy xavf tug‘dirmoqda. Bu holat nafaqat iqtisodiy zarar yetkazmoqda, balki milliy xavfsizlikka tahdid soluvchi omil sifatida ham ko‘rilmoqda. Tarmoqlarning murakkab tuzilishi va turli xil xizmatlarning integratsiyalashuvi natijasida yangi turdagi zaifliklar paydo bo‘lmoqda. Ushbu xavflarni vaqtida aniqlash va samarali boshqarish uchun risklarni baholash usullariga ehtiyoj ortib bormoqda.

Ushbu ishning asosiy maqsadi tarmoqlarda kiberxavfsizlikni ta'minlashda mavjud tahdidlarni aniqlash, ulardan kelib chiqadigan xavflarni baholash va samarali boshqarish usullarini ishlab chiqishdan iborat. Maqsadli yondashuvlar orqali risklarni boshqarishning dolzarb metodlarini o‘rganish va ularning samaradorligini amaliy jihatdan baholash nazarda tutiladi. Shu bilan birga, tarmoq xavfsizligini oshirishga qaratilgan taklif va tavsiyalarni ishlab chiqish ham ishning maqsadlaridan biridir.

ISSN 3060-4567



1-rasm. Kiberxavfsizlik asosiy tamoyillari

Kiberxavfsizlik sohasida samarali faoliyat yuritish uchun bir nechta asosiy tamoyillarga amal qilish zarur. Birinchi navbatda, bu maxfiylik tamoyili bo‘lib, u ma'lumotlarga ruxsatsiz kirishni cheklashni ta'minlaydi. Maxfiylik orqali faqat ruxsat etilgan foydalanuvchilar axborotdan foydalanishi mumkin bo‘ladi. Ikkinchi tamoyil – bu butunlik tamoyili, ya'ni ma'lumotlarning to‘g‘riligini va o‘zgarmasligini saqlash. Bu tamoyil orqali ma'lumotlar tasodifiy yoki qasddan o‘zgartirilishidan himoya qilinadi. Shuningdek, mavjudlik tamoyili ham muhim bo‘lib, bu tizim va ma'lumotlarning doimiy ravishda ruxsat etilgan foydalanuvchilar uchun foydalanishga ochiq bo‘lishini ta'minlaydi. Bundan tashqari, autentifikatsiya (shaxsni aniqlash) va hisobotlilik (foydalanuvchi harakatlarini nazorat qilish) tamoyillari ham kiberxavfsizlikning ajralmas qismlari hisoblanadi. Ushbu tamoyillar orqali tizim xavfsizligi va ishonchliligi ta'minlanadi.

Axborot xavfsizligi bugungi kunda tashkilotlarning texnologik infratuzilmasini muhofaza qilishda asosiy omil hisoblanadi. Tarmoqda uzatiladigan yoki saqlanadigan ma'lumotlarni xavfsiz saqlash, ulardan ruxsatsiz foydalanishni oldini olish axborot xavfsizligining asosiy maqsadi hisoblanadi. Axborot xavfsizligi tarmoqlar uchun bir

nechta jihatdan muhimdir. Birinchidan, bu ma'lumotlarning muhofazasini ta'minlaydi, ya'ni ma'lumotlarning begona shaxslar tomonidan o‘g‘irlanishi yoki zarar ko‘rishining oldini oladi. Ikkinchidan, u tarmoq xizmatlarining barqarorligini saqlab turishga xizmat qiladi, masalan, DDoS hujumlariga qarshi himoya orqali xizmatlarning uzluksiz ishlashini ta'minlaydi. Uchinchidan, axborot xavfsizligi tarmoqda paydo bo‘lishi mumkin bo‘lgan tahdidlarni oldindan aniqlash va ularga qarshi chora ko‘rish imkonini beradi. Nihoyat, axborot xavfsizligi tizimlardan foydalanuvchilarning ishonchini oshirishda ham muhim rol o‘ynaydi. Bu esa tashkilotlar va foydalanuvchilar o‘rtasidagi munosabatlarni mustahkamlaydi.

Har qanday tarmoq infratuzilmasi ma'lum bir zaifliklarga ega bo‘lib, ular kiberxavfsizlikka jiddiy tahdid solishi mumkin. Zaif tomonlarning biri – zaif autentifikatsiya va parollar, chunki foydalanuvchilar oddiy yoki oson topiladigan parollardan foydalanishi kiberhujumlar uchun imkoniyat yaratadi. Ikkinchi zaiflik – bu yangilanishlarning yo‘qligi, ya'ni dasturiy ta'minot va operatsion tizimlar o‘z vaqtida yangilanmasa, ularni ekspluatatsiya qilish osonlashadi. Uchinchidan, noto‘g‘ri tarmoq konfiguratsiyasi zaifliklar uchun asosiy sababdir. Masalan, firewall yoki boshqa xavfsizlik tizimlarining noto‘g‘ri sozlanishi hujumchilarga kirish imkonini beradi. Shuningdek, tarmoq xavfsizligiga zarar yetkazuvchi asosiy omillardan biri – foydalanuvchi xatolaridir. Foydalanuvchilar phishing xabarlariga ishonishi yoki zararli dasturlarni yuklab olishi orqali kiberhujumlarni osonlashtirishi mumkin. Bundan tashqari, chuqur monitoringning yo‘qligi sababli kiberhujumlar vaqtida aniqlanmaydi va ularga qarshi choralar kechikadi. Oxirgi, ammo muhim zaiflik – bu fizik xavfsizlikning yetishmasligi bo‘lib, serverlar va boshqa qurilmalar himoyasiz qolishi mumkin. Ushbu zaif tomonlarni bartaraf etish uchun maxsus xavfsizlik strategiyalarini ishlab chiqish talab etiladi.

Bugungi texnologik rivojlanish sharoitida zamonaviy kiberxavfsizlik tahdidlari ko‘lami va murakkabligi tobora oshib bormoqda. Eng keng tarqalgan tahdid turlari orasida xakerlik hujumlari yetakchi o‘rinda turadi. Xakerlik hujumlari foydalanuvchilarning tizimlariga ruxsatsiz kirish, ma'lumotlarni o‘g‘irlash, tizimlarni

buzish yoki ishlashini cheklashni o‘z ichiga oladi. Ushbu hujumlarning maqsadi ko‘pincha iqtisodiy manfaat olish yoki davlat tizimlariga zarar yetkazishdir.

Boshqa bir jiddiy tahdid turi bu zararli dasturlardir (malware). Bu dasturlar viruslar, troyanlar, ransomware (ma'lumotlarni bloklash orqali tovlamachilik) va spyware (josuslik dasturlari) kabi turlarga bo‘linadi. Zararli dasturlar orqali foydalanuvchining tizimiga kirib, shaxsiy ma'lumotlarni o‘g‘irlash, ma'lumotlarni shifrlash yoki buzish mumkin. Ayniqsa, ransomware keng tarqalgan bo‘lib, tashkilotlardan katta miqdordagi to‘lov talab qilish orqali zarar yetkazadi.

Phishing, ya'ni aldov orqali foydalanuvchilarning maxfiy ma'lumotlarini qo‘lga kiritish, kiberhujumlarning yana bir keng tarqalgan usulidir. Phishing hujumlari odatda elektron pochta xabarlari, soxta veb-saytlar yoki xabarlar orqali amalga oshiriladi. Foydalanuvchilarni aldash orqali ulardan login, parol yoki moliyaviy ma'lumotlarni olish phishingning asosiy maqsadidir.

Shuningdek, DDoS (Distributed Denial of Service) hujumlari ham zamonaviy tahdidlar orasida ko‘p uchraydi. Bu hujumlar tizimga juda ko‘p so‘rov yuborish orqali uning ishlash qobiliyatini cheklashga qaratilgan. Bunday hujumlar tashkilotlar uchun jiddiy moliyaviy zarar yetkazishi va xizmatlarni to‘xtatib qo‘yishi mumkin.

Ushbu tahdidlarning barchasi global darajada xavfsizlikka jiddiy ta'sir ko‘rsatmoqda va ularga qarshi samarali choralarni ishlab chiqish dolzarb masalaga aylanmoqda.

Tarmoqlardagi tahdidlarni aniqlash va ularni samarali boshqarish kiberxavfsizlikni ta'minlashda muhim ahamiyatga ega. Tahdidlarni aniqlash jarayonida birinchi yo‘nalish – bu real vaqt rejimida kuzatish tizimlarini qo‘llashdir. IDS (Intrusion Detection System) va IPS (Intrusion Prevention System) kabi tizimlar tarmoqdagi harakatlarni kuzatib boradi va shubhali faoliyatlarni aniqlaydi. Bunday tizimlar hujumlarni erta bosqichda aniqlash va ularga qarshi choralar ko‘rishga yordam beradi.

Ikkinchi yo‘nalish – SIEM (Security Information and Event Management) tizimlaridan foydalanishdir. Bu tizimlar turli xavfsizlik qurilmalari va dasturlardan ma'lumotlarni yig‘ib, ularni tahlil qiladi. SIEM tizimlari orqali tarmoqda sodir

ISSN 3060-4567

bo‘layotgan voqealarning umumiy manzarasini ko‘rish va tahdidlarni o‘z vaqtida aniqlash imkoniyati yaratiladi.

Uchinchi muhim yo‘nalish – sun'iy intellekt va mashinani o‘rganish algoritmlaridan foydalanishdir. Bu texnologiyalar tarmoq faoliyatidagi odatiy holatlarni tahlil qilish orqali anomaliyalarni aniqlaydi va yangi turdagi tahdidlarni oldindan bashorat qilish imkonini beradi. Mashinani o‘rganish asosidagi xavfsizlik vositalari kibertahdidlarning murakkabligi oshib borayotgan bir davrda juda samarali hisoblanadi.

Shuningdek, penetratsion testlash (penetration testing) usuli ham tahdidlarni aniqlashda keng qo‘llaniladi. Ushbu usul orqali tarmoqning zaif tomonlari sun'iy hujumlar orqali aniqlanadi va bartaraf etiladi.

Oxirgi, ammo muhim yo‘nalish – xodimlarni muntazam o‘qitish va tahdidlar haqida xabardorlikni oshirishdir. Chunki xodimlarning phishing yoki zararli dasturlarga nisbatan ehtiyotsizligi ko‘pincha kiberhujumlarga sabab bo‘ladi. Tahdidlarni samarali aniqlash va ularga qarshi choralar ko‘rish uchun texnologik vositalar bilan bir qatorda inson omiliga ham e'tibor qaratish zarur.

Xulosa

Bugungi kunda kiberxavfsizlik masalalari jamiyatning barcha sohalarida, xususan, axborot texnologiyalari va tarmoq infratuzilmasida dolzarb muammolardan biriga aylangan. Tarmoqlarni samarali himoya qilish uchun zamonaviy tahdidlarni aniqlash, risklarni baholash va ularni boshqarish bo‘yicha kompleks yondashuv talab etiladi. Xakerlik, zararli dasturlar, phishing kabi zamonaviy tahdidlar nafaqat tashkilotlarga iqtisodiy zarar yetkazadi, balki ular faoliyatining uzluksizligini ham xavf ostiga qo‘yadi. Ushbu tahdidlarning ko‘lamini cheklash va ularning salbiy ta'sirini minimallashtirish uchun texnologik va boshqaruv usullarining kombinatsiyasi zarur.

Kiberxavfsizlikni ta'minlashning asosiy yo‘nalishlari orasida real vaqt rejimida monitoring tizimlari, sun'iy intellekt asosidagi tahdidlarni aniqlash usullari va xavfsizlik siyosatlarini takomillashtirish katta ahamiyatga ega. Shu bilan birga, tashkilot xodimlarini muntazam o‘qitish va ularning kiberxavfsizlik bo‘yicha

xabardorligini oshirish orqali inson omiliga bog‘liq zaifliklarni bartaraf etish mumkin.

Xulosa qilib aytganda, tarmoqlarda kiberxavfsizlikni ta'minlashda tahdidlarni o‘z vaqtida aniqlash va risklarni boshqarishning samarali usullarini joriy qilish muhim ahamiyatga ega. Ushbu yo‘nalishda olib borilgan tadqiqotlar va amaliy ishlar kiberxavfsizlikni kuchaytirish va tashkilotlarning global miqyosda raqobatbardoshligini oshirishga xizmat qiladi. Shuningdek, ilg‘or texnologiyalarni joriy qilish va xavfsizlik bo‘yicha innovatsion yondashuvlarni ishlab chiqish tahdidlar oldini olishda kelajakka yo‘naltirilgan muhim qadam hisoblanadi.

ADABIYOTLAR RO’YXATI

1. ANDERSON, R. SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS. – WILEY, 2020. – 1080 C.
2. ISO/IEC 27001:2013. INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — INFORMATION SECURITY MANAGEMENT SYSTEMS — REQUIREMENTS. – INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2013. – 30 C.
3. KIZZA, J. M. GUIDE TO COMPUTER NETWORK SECURITY. – SPRINGER, 2019. – 569 C.
4. NIST SPECIAL PUBLICATION 800-53. SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS. – NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2020. – 508 C.
5. SHON HARRIS, F. M. CISSP ALL-IN-ONE EXAM GUIDE. – MCGRAW-HILL EDUCATION, 2021. – 1456 C.
6. STALLINGS, W. NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS. – PEARSON, 2017. – 480 C.
7. SYMANTEC CORPORATION. INTERNET SECURITY THREAT REPORT. – SYMANTEC CORPORATION, 2021. – 64 C.
8. TANENBAUM, A. S., WETHERALL, D. J. COMPUTER NETWORKS. – PEARSON, 2021. – 960 C.

ISSN 3060-4567

9. WHITMAN, M., MATTORD, H. PRINCIPLES OF INFORMATION SECURITY. – CENGAGE LEARNING, 2018. – 752 C.

10. XOLMATOV O., ABDURAHMONOV A. TARMOQ XAVFSIZLIGI VA UNING BOSHQARUVI. – TOSHKENT: O‘ZBEKISTON MILLIY UNIVERSITETI NASHRIYOTI, 2022. – 312 C.

11. SANS INSTITUTE. INFORMATION SECURITY TRAINING [ЭЛЕКТРОННЫЙ РЕСУРС]. – URL: HTTPS://WWW.SANS.ORG.

12. NIST. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY [ЭЛЕКТРОННЫЙ РЕСУРС]. – URL: HTTPS://WWW.NIST.GOV.