TARMOQLARDA KIBER XAVFSIZLIKNI TA'MINLASHDA RISKLARNI BOSHQARISH METODLARINI BAHOLASH

O`zbekiston Respublikasi Bank-moliya akademiyasi 2-kurs tinglovchisi

Sherqulov Abror Xujaqul o'g'li

Annotatsiya. *Ushbu maqola tarmoqlarda kiberxavfsizlikni ta'minlashda xavf-xatarlarni boshqarish usullarini o'rganishga bag'ishlangan. Maqolada kiberxavfsizlikning dolzarbligi, tarmoq tahdidlari va zaifliklar tahlili, shuningdek, xavflarni aniqlash, baholash va ularni kamaytirish bo'yicha zamonaviy yondashuvlar ko'rib chiqilgan. Tadqiqotning asosiy maqsadi tarmoq xavfsizligini ta'minlashga qaratilgan samarali boshqaruv usullarini ishlab chiqish va ularni amaliyotga tatbiq etish imkoniyatlarini o'rganishdan iborat.*

Kalit so'zlar: *kiberxavfsizlik, tarmoq xavfsizligi, xavflarni boshqarish, tarmoq tahdidlari, xavfsizlik usullari, kiberhujumlar.*

Abstract. *This article is dedicated to studying risk management methods for ensuring cybersecurity in networks. It examines the relevance of cybersecurity, analysis of network threats and vulnerabilities, as well as modern approaches to identifying, assessing, and mitigating risks. The primary objective of the research is to develop effective management methods aimed at enhancing network security and explore the possibilities of their practical implementation.*

Keywords: *cybersecurity, network security, risk management, network threats, security methods, cyberattacks.*

Hozirgi raqamli asrda kiberxavfsizlik masalasi tobora dolzarblashib bormoqda. Raqamli texnologiyalar va internetning keng tarqalishi inson hayotining barcha jabhalarini qamrab oldi, shu jumladan biznes, davlat boshqaruvi, ta'lim, tibbiyot va kundalik turmush faoliyatini. Biroq, ushbu texnologiyalar bilan birga

turli kiberxavf-xatarlar ham yuzaga keldi. Shaxsiy va korporativ ma'lumotlarning o‘g‘irlanishi, infratuzilmalar tarmoqlariga hujumlar va iqtisodiy zararlar kiberxavfsizlikning nafaqat texnik, balki strategik muammo ekanligini ko‘rsatmoqda.

Bugungi kunda tarmoqlar zamonaviy texnologiyalar va axborot almashinuvi jarayonining markaziy qismi hisoblanadi. Ular davlat boshqaruvidan tortib, bank tizimlari, sog‘liqni saqlash, ta’lim va sanoat sohalarigacha bo‘lgan turli faoliyat yo‘nalishlarini birlashtiradi. Tarmoqlar orqali amalga oshiriladigan ma'lumotlar almashinuvi jarayonining xavfsizligi tashkilotlarning barqaror faoliyat yuritishi uchun muhim ahamiyatga ega. Shu sababli tarmoq xavfsizligini ta’minlash har qanday tashkilotning strategik maqsadlaridan biri hisoblanadi.

Tarmoq xavfsizligini ta'minlash birinchi navbatda ma'lumotlarning maxfiyligi, butunligi va mavjudligini kafolatlashga qaratilgan. Ma'lumotlar oqimi himoyasiz bo‘lsa, xakerlar yoki boshqa kiberjinoyatchilar ulardan noqonuniy ravishda foydalanishi mumkin. Bu esa shaxsiy yoki korporativ ma'lumotlarning o‘g‘irlanishi, infratuzilmaning buzilishi va katta moliyaviy yo‘qotishlarga olib kelishi mumkin. Ayniqsa, raqamli iqtisodiyotning kengayishi va onlayn faoliyatning ko‘payishi tarmoqlarda xavfsizlik choralarini kuchaytirishni talab qiladi.

Tarmoq xavfsizligi davlat miqyosida ham strategik ahamiyatga ega. Energetika tarmoqlari, transport tizimlari, sog‘liqni saqlash infratuzilmasi va boshqa muhim tizimlarning ishlashi tarmoqlar orqali boshqariladi. Ushbu tizimlarning ishlashida uzilishlar yoki hujumlar jamiyatga jiddiy zarar yetkazishi va ijtimoiy barqarorlikni buzishi mumkin. Shu sababli tarmoq xavfsizligini ta'minlash davlatlar uchun milliy xavfsizlikning bir qismi sifatida qaralmoqda.

Bundan tashqari, biznes doirasida tarmoq xavfsizligi tashkilotning raqobatbardoshligini ta'minlashda ham muhim rol o‘ynaydi. Tarmoq xavfsizligi orqali korxonalar o‘z mijozlari va hamkorlarining ishonchini saqlab qoladi.

Xavfsizlik siyosati va zamonaviy texnologik yondashuvlar qo‘llanilishi nafaqat mavjud tahdidlarga qarshi kurashishni, balki ulardan oldini olishni ham ta’minlaydi.

Tadqiqotning maqsadi – tarmoqlarda kiberxavfsizlikni ta'minlash uchun xatarlarni boshqarish usullarini tahlil qilish va samaradorligini baholashdan iborat. Ushbu maqsadni amalga oshirish orqali tarmoq xavfsizligini oshirishga qaratilgan amaliy tavsiyalar ishlab chiqish va zamonaviy kiberxavf-xatarlarni kamaytirishning samarali usullarini taklif etish ko‘zda tutiladi.

Tadqiqotning vazifalari quyidagilardan iborat:

1. Kiberxavfsizlik va tarmoq xavfsizligi bo‘yicha nazariy asoslarni o‘rganish. Tarmoqlarda yuzaga keladigan xavflar, tahdidlar va zaifliklarning turkumlanishini o‘rganish va ular haqidagi ilmiy ma’lumotlarni umumlashtirish.
2. Xatarlarni boshqarish usullarini tahlil qilish. Tarmoqlardagi xavflarni aniqlash, baholash va ularni minimallashtirish usullarini tadqiq qilish.
3. Texnologik vositalarni tahlil qilish. Xavfsizlikni ta’minlashda foydalaniladigan zamonaviy texnologiyalar, dasturiy ta’minot va usullar samaradorligini baholash.
4. Tarmoqlar xavfsizligini ta’minlashda tavsiyalar ishlab chiqish. Xatarlarni boshqarish va xavfsizlikni oshirishga qaratilgan strategik va amaliy chora-tadbirlarni taklif etish.
5. Olingan natijalarni amaliyotga tatbiq qilish imkoniyatlarini o‘rganish. Tadqiqot natijalaridan tashkilotlar va davlat miqyosida foydalanish imkoniyatlarini ko‘rsatib berish.

Ushbu maqsad va vazifalarni amalga oshirish orqali zamonaviy kiberxavflarga qarshi samarali kurashish uchun zarur bo‘lgan ilmiy va amaliy asoslar yaratiladi. Bu esa tarmoqlarning xavfsizligini ta'minlash, tashkilotlarning raqobatbardoshligini oshirish va jamiyatdagi barqarorlikni mustahkamlashga xizmat qiladi.

Kiberhujumlar turlari va ularning murakkabligi yildan-yilga oshmoqda. Zamonaviy xakerlar texnologiyalarni suiiste'mol qilishning yangi usullarini ishlab chiqib, tashkilotlarning zaif tomonlarini aniqlashga intilishmoqda. Masalan, shaxsiy ma'lumotlar va moliyaviy axborotlarga yo‘naltirilgan ijtimoiy injiniring hujumlari yoki korporativ infratuzilmaga kirishga qaratilgan ransomware dasturlari hozirda eng keng tarqalgan xavflar hisoblanadi. Ayniqsa, "Narsalar interneti" (IoT) kabi yangi texnologiyalar bilan bog‘liq bo‘lgan xavflar soni oshib bormoqda, chunki bu qurilmalar ko‘pincha yetarli darajada himoya qilinmagan.

Davlat miqyosidagi kiberxavfsizlik tahdidlarining kuchayishi global xavfsizlikka ham ta'sir ko‘rsatmoqda. Xususan, davlat xizmatlari, transport tizimlari, energetika infratuzilmasi va boshqa muhim tizimlarga qaratilgan kiberhujumlar nafaqat iqtisodiy yo‘qotishlarga, balki ijtimoiy beqarorlikka ham olib kelishi mumkin. Ko‘plab davlatlar uchun kiberxavfsizlik masalasi milliy xavfsizlik strategiyasining ajralmas qismi sifatida qaralmoqda.

Bundan tashqari, kiberxavfsizlikning dolzarbligi moliyaviy jihatdan ham muhimdir. Statistika ma'lumotlariga ko‘ra, 2023-yilda kiberjinoyatlar oqibatida global iqtisodiyotga yetkazilgan zarar 8 trillion AQSh dollaridan oshgan. Tashkilotlar kiberhujumlar sababli nafaqat katta miqdorda mablag‘ yo‘qotmoqda, balki o‘z obro‘siga ham katta zarar yetkazmoqda. Bu esa foydalanuvchilar va mijozlar ishonchini yo‘qotish bilan birga, kelajakdagi moliyaviy barqarorlikka xavf tug‘diradi.

Kiberxavfsizlikning dolzarbligini ko‘rsatadigan yana bir omil – bu texnologiyalar tez sur'atlarda rivojlanayotgani. Sun'iy intellekt, bulutli texnologiyalar, 5G va boshqa zamonaviy innovatsiyalar bir tomondan biznes jarayonlarini soddalashtirsa, boshqa tomondan yangi tahdidlar va zaifliklarni keltirib chiqarmoqda. Shuning uchun har qanday tashkilot va davlat uchun kiberxavfsizlik sohasiga e'tibor qaratish strategik zaruratga aylanmoqda.

Xulosa qilib aytganda, kiberxavfsizlik nafaqat texnik masala, balki biznesning barqarorligi va davlatlarning xavfsizligini ta’minlash uchun strategik ustuvor yo‘nalishdir. Raqamli muhitda xavfsizlikni ta’minlash nafaqat texnologik vositalar, balki samarali boshqaruv va muntazam monitoring orqali amalga oshirilishi kerak. Bu esa tashkilotlar va davlatlarning raqamli xavfsizlik bo‘yicha maqsadli strategiyalar ishlab chiqishini talab qiladi.

Kiberxavfsizlik – bu axborot texnologiyalari infratuzilmasi, ma'lumotlar va tizimlarni kiberhujumlar, noqonuniy foydalanish va zarar yetkazishdan himoya qilishni ta'minlashga qaratilgan chora-tadbirlar majmuasidir. Uning asosiy maqsadi – ma'lumotlarning maxfiyligini, butunligini va mavjudligini kafolatlash. Kiberxavfsizlik nafaqat texnik choralardan iborat, balki tashkilotlar va foydalanuvchilar tomonidan qabul qilinadigan siyosatlar, jarayonlar va madaniyatni ham o‘z ichiga oladi.

Kiberxavfsizlikning ahamiyati texnologiyalarning kundalik hayotimizga chuqur kirib kelishi bilan ortib bormoqda. Tashkilotlar va davlatlarning ishlashi uchun asosiy infratuzilmalar bo‘lgan tarmoq tizimlari, ma'lumotlar bazalari va serverlar kiberxavf-xatarlarning asosiy nishoniga aylanmoqda. Shu sababli, zamonaviy dunyoda kiberxavfsizlik faqat texnologik muammo emas, balki ijtimoiy va iqtisodiy barqarorlikni ta'minlash vositasidir.

Tarmoqlar ko‘plab texnologiyalar va protokollardan tashkil topgan murakkab tizim bo‘lib, ularda yuzaga keladigan asosiy tahdidlar quyidagilardan iborat:

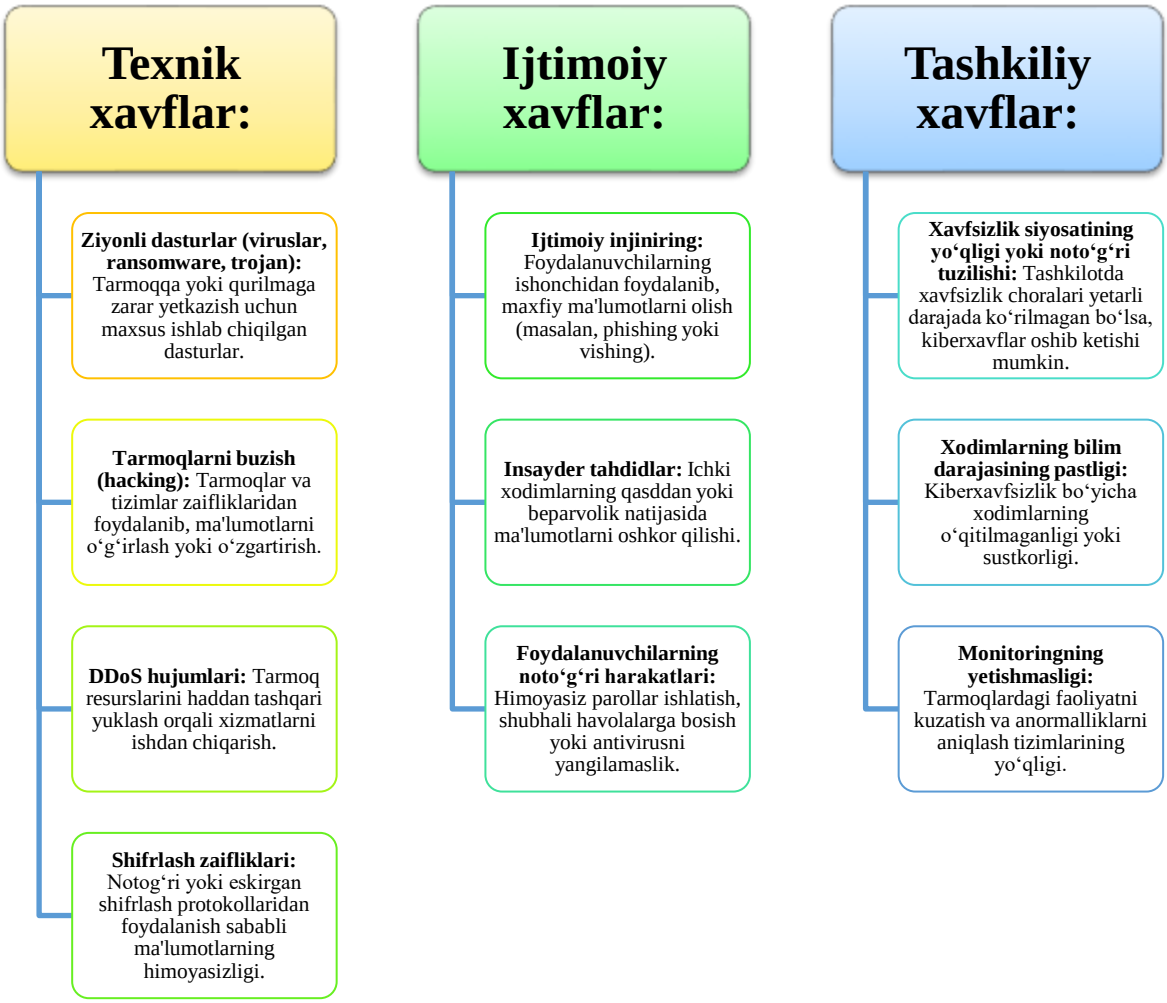
1. Kiberhujumlar: Tarmoqlarga ruxsatsiz kirish orqali ma'lumotlarni o‘g‘irlash yoki o‘zgartirishga qaratilgan xakerlik faoliyati. Masalan, DDoS hujumlari tarmoqlarni ishdan chiqarishga qaratilgan bo‘ladi.

2. Ziyonli dasturlar (malware): Viruslar, ransomware, trojan va boshqa zararli dasturlar tarmoqlarga kirib, tizimlarni buzishi yoki ma'lumotlarni shifrlab qo‘yishi mumkin.

3. Ijtimoiy injiniring: Xodimlarning beparvoligidan yoki bilim yetishmasligidan foydalanib, maxfiy ma'lumotlarni qo‘lga kiritish usuli. Masalan, phishing orqali foydalanuvchilarning login va parollari o‘g‘irlanadi.

4. Tarmoqlar zaifliklari: Himoyasiz tizimlar, noto‘g‘ri sozlangan serverlar yoki eskirgan dasturiy ta'minot kiberjinoyatchilar uchun imkoniyat yaratadi. Zaif parollar va xavfsizlik devorlarining yetarlicha samarali bo‘lmasligi ham katta xavf tug‘diradi.

5. Ichki tahdidlar: Tashkilot ichidagi xodimlarning beparvoligi yoki g‘arazli harakatlari tufayli tarmoq xavfsizligi buzilishi mumkin. Bu maxfiy ma'lumotlarning tarqalishi yoki tarmoqqa zarar yetkazilishi bilan bog‘liq bo‘lishi mumkin.



1-rasm. Kiberxavflarning turkumlanishi

Tarmoqlardagi asosiy zaifliklar texnologik, ijtimoiy va tashkiliy jihatlarga bo‘linadi. Himoya darajasining yetarli emasligi, foydalanuvchilarning bilim va ko‘nikmalarining pastligi hamda xavfsizlik siyosatining noto‘g‘ri tashkil etilishi – bularning barchasi xavflar yuzaga kelishiga sharoit yaratadi.

Kiberxavfsizlik – bu axborot tizimlari, tarmoqlar va ma'lumotlarni kiberhujumlardan himoya qilishga qaratilgan chora-tadbirlar majmui. Uning asosiy maqsadi – axborotning maxfiyligini, butunligini va mavjudligini ta'minlashdir. Kiberxavfsizlik nafaqat texnologik masala, balki iqtisodiy va ijtimoiy barqarorlikni ta'minlashning asosiy omillaridan biridir. Zamonaviy texnologiyalar va internet xizmatlarining keng qo‘llanilishi kiberxavfsizlikni tashkilotlarning rivojlanishi va faoliyat yuritishining ajralmas qismi sifatida qarashni talab qiladi.

Tizimlarning zaif tomonlarini o‘z vaqtida aniqlash va himoya choralarini ko‘rish kiberxavfsizlikni ta'minlashda muhim rol o‘ynaydi. Xavfsizlik siyosati va zamonaviy texnologiyalardan foydalanish nafaqat hujumlarning oqibatlarini bartaraf etishga, balki ulardan oldini olishga yordam beradi. Shu sababli, kiberxavfsizlik tashkilot va davlatlar uchun strategik ahamiyatga ega.

Tarmoqlar kiberxavf-xatarlar oldida eng zaif infratuzilmalardan biri hisoblanadi. Eng keng tarqalgan tahdidlar qatoriga kiberhujumlar, ziyonli dasturlar, ijtimoiy injiniring va ichki tahdidlar kiradi. Kiberhujumlar ma'lumotlarga noqonuniy kirish, ularni buzish yoki o‘g‘irlashga qaratilgan bo‘lib, tashkilotlarning moliyaviy va obro‘li zarar ko‘rishiga olib keladi. DDoS hujumlari esa tarmoq tizimlarini haddan tashqari yuklab, xizmatlarning ishlashini to‘xtatadi.

Tarmoq tizimlarining zaifliklari ko‘pincha eskirgan dasturiy ta'minot, xavfsiz parollar yo‘qligi yoki noto‘g‘ri konfiguratsiya natijasida yuzaga keladi. Bundan tashqari, xodimlarning beparvoligi yoki bilimsizligi ham kiberxavfsizlikka jiddiy zarar yetkazishi mumkin. Ijtimoiy injiniring orqali xakerlar xodimlardan maxfiy ma'lumotlarni olish uchun ularning ishonchidan foydalanadi. Tizimlarning zaif

tomonlarini vaqtida aniqlash va himoya choralarini kuchaytirish ushbu tahdidlarni kamaytirishda asosiy ahamiyatga ega.

Kiberxavflar kelib chiqish manbai va usullariga qarab texnik, ijtimoiy va tashkiliy xavflarga bo‘linadi. Texnik xavflarga ziyonli dasturlar, tarmoq buzilishlari, DDoS hujumlari va shifrlash zaifliklari kiradi. Masalan, ransomware dasturlari tizimlarni shifrlab, ma'lumotlarni qayta tiklash uchun to‘lov talab qiladi. Texnik xavflar ko‘pincha texnologiyalarning eskirganligi yoki noto‘g‘ri sozlanishi bilan bog‘liq.

Ijtimoiy xavflar esa inson omiliga asoslangan bo‘lib, ijtimoiy injiniring, phishing, va xodimlarning beparvoligini o‘z ichiga oladi. Masalan, xodimlarning shubhali havolalarga bosishi yoki zaif parollardan foydalanishi kiberjinoyatchilar uchun imkoniyat yaratadi. Bunday xavflarni kamaytirish uchun xodimlarni muntazam o‘qitish va ularning xabardorligini oshirish zarur.

Tashkiliy xavflar xavfsizlik siyosatining yo‘qligi yoki noto‘g‘ri tashkil etilishi bilan bog‘liq. Xavfsizlik choralarini e'tiborsiz qoldirish, monitoring tizimlarining yetishmasligi va xavfsizlikka mas’ul xodimlarning yetarlicha malakaga ega emasligi tashkilotlarning zaiflashishiga olib keladi. Tashkiliy xavflarni kamaytirish uchun xavfsizlik siyosatini qat’iy belgilash va uni muntazam nazorat qilib borish muhimdir.

Kiberxavflarni to‘g‘ri turkumlash va ularning har bir turiga nisbatan tegishli choralarni ko‘rish tarmoq xavfsizligini oshirishda muhim ahamiyatga ega. Texnik, ijtimoiy va tashkiliy xavflarga qarshi samarali strategiyalar ishlab chiqish va ulardan foydalangan holda xavfsizlikni ta’minlash imkoniyati yanada kengayadi.

Xulosa

Tarmoqlarda kiberxavfsizlikni ta’minlash hozirgi zamonning eng dolzarb muammolaridan biri bo‘lib, texnologik rivojlanish sur’atlari bilan birga uning ahamiyati ortib bormoqda. Kiberxavfsizlik – bu ma'lumotlarning maxfiyligi, butunligi va mavjudligini ta’minlash orqali shaxslar, tashkilotlar va davlatlarning

iqtisodiy va ijtimoiy barqarorligini qo‘llab-quvvatlashga qaratilgan jarayon. Texnik, ijtimoiy va tashkiliy xavflarni to‘g‘ri aniqlash va ularni boshqarish usullarini qo‘llash xavfsizlik darajasini oshirishda muhim rol o‘ynaydi.

Kiberxavflar turlari va tahdidlarning murakkablashishi kiberxavfsizlik strategiyalarini takomillashtirishni talab qiladi. Xavfsizlik siyosatlarini belgilash, xodimlarni muntazam o‘qitish, zamonaviy texnologik vositalarni joriy etish va tarmoqlarni doimiy monitoring qilish – bu xavflarni samarali boshqarish uchun muhim choralardir. Ayniqsa, zamonaviy kiberhujumlarga qarshi kurashda sun’iy intellekt, mashinani o‘rganish va avtomatlashtirilgan xavfsizlik tizimlaridan foydalanish ehtiyoj sezilmoqda.

Shuni unutmaslik kerakki, kiberxavfsizlik nafaqat texnologik muammo, balki tashkilotlar va davlatlarning strategik xavfsizligi bilan bog‘liq murakkab jarayondir. Tizimli yondashuv va innovatsion boshqaruv usullaridan foydalangan holda, tarmoqlarda xavfsizlikni ta'minlash bo‘yicha barqaror va samarali yechimlarni ishlab chiqish mumkin. Bu esa nafaqat tashkilotlarning faoliyat barqarorligini ta'minlaydi, balki foydalanuvchilarning ishonchini oshirib, raqamli infratuzilmalarni himoya qilishning poydevorini yaratadi.

Umuman olganda, kiberxavfsizlikni ta'minlash uchun texnik vositalar, inson omili va tashkilotlar siyosatini uyg‘unlashtirish zarur. Shu asosda amalga oshiriladigan xavfsizlik choralarining samaradorligi kelajakda raqamli dunyoning barqaror rivojlanishini ta’minlashga xizmat qiladi.

Foydalanilgan adabiyotlar va manbalar ro‘yxati

1. Ahmedov B.K., *Axborot xavfsizligi va zamonaviy tahdidlar*. – Samarqand: SamDU nashri, 2021.

2. Anderson R., *Security Engineering: A Guide to Building Dependable Distributed Systems*. – Wiley, 3rd edition, 2020.

3. Blum R., Liu D., *Cybersecurity For Dummies*. – Wiley, 2019.

4. Cisco Systems, *Cisco Annual Cybersecurity Report*. – Cisco Press, 2023.

5. Cybersecurity Ventures, *2023 Official Cybercrime Report*. – Cybersecurity Ventures, 2023.

6. Gartner Research, *Top Trends in Cybersecurity 2023*. – Gartner Reports, 2023.

7. ISO/IEC 27001:2013, *Informatsion xavfsizlik, boshqaruv tizimlari bo‘yicha xalqaro standart*. – Xalqaro standartlar tashkiloti.

8. Kaspersky Lab, *Global IT Security Risks Survey*. – Kaspersky Security Report, 2023.

9. Karimov S.R., *Axborot texnologiyalari xavfsizligi*. – Toshkent: TATU nashriyoti, 2020.

10. Kutlubekov Sh.X., *Kiberxavfsizlik asoslari*. – Toshkent: O‘zbekiston milliy ensiklopediyasi nashriyoti, 2020.

11. NIST (National Institute of Standards and Technology), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, 2018.

12. Pfleeger C.P., Pfleeger S.L., *Security in Computing*. – Prentice Hall, 5th edition, 2015.

13. Qodirov R.T., *Axborot xavfsizligida ilg‘or texnologiyalar*. – Namangan: NDU nashri, 2022.

14. Stallings W., *Network Security Essentials: Applications and Standards*. – Pearson Education, 6th edition, 2019.

15. Symantec Corporation, *Internet Security Threat Report*. – Symantec, 2022.

16. Whitman M., Mattord H., *Principles of Information Security*. – Cengage Learning, 6th edition, 2017.

17. Statista, *Kiberhujumlar natijasida yetkazilgan moliyaviy yo‘qotishlar bo‘yicha tadqiqotlar* (https://www.statista.com).