ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-5

TARMOQDA AXBOROT XAVFSIZLIGI MUAMMOLARI VA ULARNING YECHIMLARI

Shukurov Orziqul Pardayevich
Muhammad al-Xorazmiy nomidagi TATU, Axborot xavfsizligi kafedrasi katta o'qituvchisi
myheartumi@gmail.com, +998996636990

Annotatsiya. Mazkur maqolada tarmoqlarda axborot xavfsizligi bilan bog'liq dolzarb muammolar, ularning kelib chiqish sabablari hamda zamonaviy yechimlari tahlil qilingan. Tadqiqotda zararli dasturlar, DDoS hujumlari, Fishing, ransomware, Man-in-the-Middle (MITM), insider threats va zero-day zaifliklar kabi asosiy tahdidlar ko'rib chiqilgan hamda ularning tarmoq tizimlariga ta'siri baholangan. Shuningdek, tarmoq xavfsizligini ta'minlashda foydalaniladigan firewall, IDS/IPS, SIEM, multifaktor autentifikatsiya (MFA), kriptografik himoya vositalari va sun'iy intellekt asosidagi anomaliyalarni aniqlash usullari tahlil etilgan.
Kalit so'zlar: tarmoq xavfsizligi, kiberxavfsizlik, DDoS, Fishing, IDS/IPS, firewall, zaifliklar, tarmoq hujumlari, SIEM.

KIRISH. Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida tarmoq tizimlari davlat boshqaruvi, bank sektori, sog'liqni saqlash, ta'lim, elektron tijorat va sanoat korxonalarining asosiy infratuzilmasiga aylandi[15]. Internetdan foydalanish ko'lamining kengayishi, masofaviy ishlash texnologiyalarining rivojlanishi va bulutli xizmatlardan foydalanishning ortishi bilan bir qatorda kiberxavfsizlik tahdidlari ham murakkablashib bormoqda[5,14].

Tarmoq xavfsizligi — bu kompyuter tarmoqlari, serverlar, uzatish kanallari va ulardagi ma'lumotlarni ruxsatsiz kirish, o'zgartirish, buzish yoki yo'qotishdan himoya qilish jarayonidir. Zamonaviy tarmoqlarda yuzaga kelayotgan tahdidlar nafaqat texnik zaifliklardan, balki inson omili, noto'g'ri konfiguratsiya va xavfsizlik siyosatining yetarli darajada joriy qilinmaganidan ham kelib chiqadi.

Bugungi kunda kiberjinoyatchilar tarmoqlarga hujum qilish uchun murakkab usullardan foydalanmoqda. Jumladan:

- *Distributed Denial of Service* (DDoS) hujumlari orqali xizmatlar ishlashi izdan chiqariladi;
- *"Fishing"* orqali foydalanuvchi ma'lumotlari qo'lga kiritiladi;
- *"ransomware"* hujumlari orqali ma'lumotlar shifrlanib, to'lov talab qilinadi;
- *"zero-day vulnerabilities"* ekspluatatsiyasi yordamida hali tuzatilmagan zaifliklardan foydalaniladi.

So'nggi yillarda dunyo miqyosida kiberhujumlar sonining ortishi natijasida tashkilotlar milliardlab dollar iqtisodiy zarar ko'rmoqda. Shu sababli tarmoq axborot xavfsizligi masalalari global muammoga aylangan.

O'zbekistonda ham davlat xizmatlarining raqamlashtirilishi, elektron hukumat tizimlarining rivojlanishi, onlayn bank xizmatlari va masofaviy ta'lim platformalarining keng qo'llanilishi kiberxavfsizlik talablarini kuchaytirishni taqozo etmoqda[9]. Mamlakatda davlat axborot tizimlarini himoyalash, milliy CERT faoliyatini rivojlantirish hamda axborot xavfsizligi standartlarini joriy etish bo'yicha qator ishlar olib borilmoqda. Shunga qaramay, Fishing, zararli dasturlar, noqonuniy kirish va ma'lumotlar sizib chiqishi bilan bog'liq muammolar dolzarbligicha qolmoqda.

Mazkur maqolaning maqsadi tarmoq axborot xavfsizligida uchraydigan asosiy muammolarni tizimli ravishda tahlil qilish, ularning tasnifini ishlab chiqish, tahdidlar va zaifliklarni baholash hamda zamonaviy himoya mexanizmlarini o'rganishdan iborat.

ADABIYOTLAR TAHLILI

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

Tarmoq axborot xavfsizligi sohasidagi tadqiqotlar so‘nggi o‘n yillikda sezilarli ravishda rivojlandi. Kiberxavfsizlikka oid ilmiy adabiyotlarda tarmoq tahdidlari, himoya vositalari va hujumlarni aniqlash algoritmlariga katta e’tibor qaratilgan.

Smith va Brooks (2021) tomonidan olib borilgan tadqiqotlarda tarmoq hujumlarining asosiy qismi inson omili bilan bog‘liqligi ko‘rsatib berilgan. Tadqiqot natijalariga ko‘ra, foydalanuvchilarning xavfsizlik savodxonligi pastligi Fishing va social engineering hujumlarining muvaffaqiyat darajasini oshiradi.

Kumar va Patel (2022) tadqiqotida esa DDoS hujumlarini aniqlashda mashinali o‘qitish algoritmlaridan foydalanish samaradorligi o‘rganilgan. Tadqiqotchilar sun’iy intellekt asosidagi intrusion detection tizimlari an’anaviy signatura asosidagi tizimlarga nisbatan yuqori aniqlik ko‘rsatishini qayd etgan.

Shuningdek, firewall va IDS/IPS tizimlarining birgalikda qo‘llanilishi ko‘p qatlamli himoya (Defense in Depth) tamoyilining samaradorligini oshirishga xizmat qilishi ilmiy jihatdan asoslangan. Zamonaviy SIEM platformalari esa real vaqt rejimida loglarni yig‘ish va tahdidlarni aniqlash imkonini bermoqda.

So‘nggi tadqiqotlarda quyidagi yo‘nalishlarga alohida e’tibor qaratilmoqda:

1. Sun’iy intellektga asoslangan tahdidlarni aniqlash. Sun’iy intellekt yordamida anomaliyalarni aniqlash va real vaqt monitoringi.
2. *Zero Trust arxitekturasi.* “Never trust, always verify” tamoyiliga asoslangan xavfsizlik modeli.
3. *Blokcheynga asoslangan xavfsizlik*. Tarmoq tranzaksiyalarini himoyalash va ma’lumot yaxlitligini ta’minlash.
4. *Bulutli xavfsizlik*. Bulutli infratuzilmalarda xavfsizlikni boshqarish.
5. *IoT xavfsizligi*. IoT qurilmalarining DDoS va botnet hujumlariga bardoshliligini oshirish.

1-jadval. Tarmoq xavfsizligi bo‘yicha tadqiqotlar qiyosiy tahlili

Muallif	Yil	Tadqiqot yo‘nalishi	Asosiy natija
Smith & Brooks	2021	Fishing va inson omili	Savodxonlik oshishi xavfni kamaytiradi
Kumar & Patel	2022	AI-based IDS	Yuqori aniqlik ko‘rsatgan
Chen et al.	2023	Zero Trust	Ichki tahdidlarni kamaytirgan
Alshamrani	2024	Cloud security	Bulutli xavfsizlik samaradorligi oshgan

Tarmoq axborot xavfsizligi muammolarining taksonomiyasi. Tarmoq axborot xavfsizligi muammolarini tizimli ravishda tahlil qilish uchun ularni ma’lum kategoriyalarga ajratish muhim hisoblanadi. Taksonomiya tarmoq tahdidlarini ularning kelib chiqishi, amalga oshirish usuli va zarar yetkazish darajasiga ko‘ra klassifikatsiya qilish imkonini beradi.

Tadqiqotlar asosida tarmoq xavfsizligi tahdidlarini quyidagi asosiy guruhlarga ajratish mumkin:

1. Tashqi tahdidlar (External threats)

Bu tahdidlar tashqi hujumchilar tomonidan amalga oshiriladi va odatda internet orqali sodir bo‘ladi. Ular quyidagilarni o‘z ichiga oladi:

- DDoS hujumlari;
- fishing;
- ransomware;
- Zararli dastur;
- botnet hujumlari;

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

- “brute-force” hujumlari.

2. Ichki tahdidlar (Insider threats)

Ichki tahdidlar tashkilot xodimlari yoki tizimga ruxsatli kirish huquqiga ega shaxslar tomonidan yuzaga keladi.

Bunga quyidagilar kiradi:

- maxfiy ma’lumotlarni sizdirish;
- noto‘g‘ri konfiguratsiya;
- imtiyozlarni suiiste’mol qilish;
- qasddan zarar yetkazish.

3. Dasturiy zaifliklar (Software vulnerabilities)

Dasturiy ta’minotdagi xatolar yoki patch qilinmagan zaifliklar tarmoqqa kirish uchun asosiy vosita bo‘lib xizmat qiladi.

Misollar:

- Zero-day vulnerabilities;
- buferning toshib ketishi;
- SQL inyeksiya;
- Masofaviy kodni bajarish (Remote Code Execution RCE).

4. Infratuzilma tahdidlari (Infrastructure threats)

Tarmoq qurilmalari yoki serverlar konfiguratsiyasidagi xatoliklar bilan bog‘liq tahdidlar.

Misollar:

- noto‘g‘ri firewall qoidalari;
- ochiq portlar;
- standart parollardan foydalanish;
- segmentatsiya mavjud emasligi.

5. Ijtimoiy muhandislik hujumlari (Social engineering)

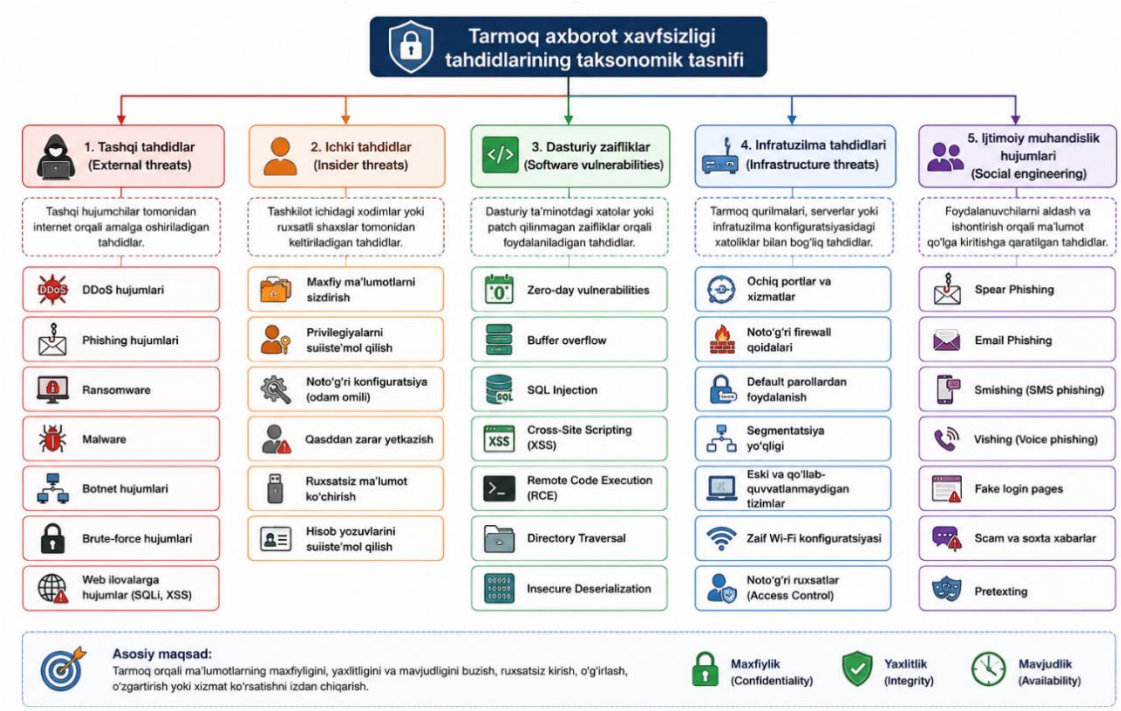
Foydalanuvchilarni aldash orqali ma’lumotlarni qo‘lga kiritishga qaratilgan hujumlar.

Misollar:

- spear Fishing;
- soxta kirish sahifalari;
- “scam” xabarlar;
- vishing.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

VOLUME-6, ISSUE-5



1-rasm. Tarmoq axborot xavfsizligi tahdidlarining taksonomik tasnifi

So‘nggi tadqiqotlar asosida tashkilotlarda uchraydigan tahdidlarning taqsimoti quyidagicha baholanishi mumkin:

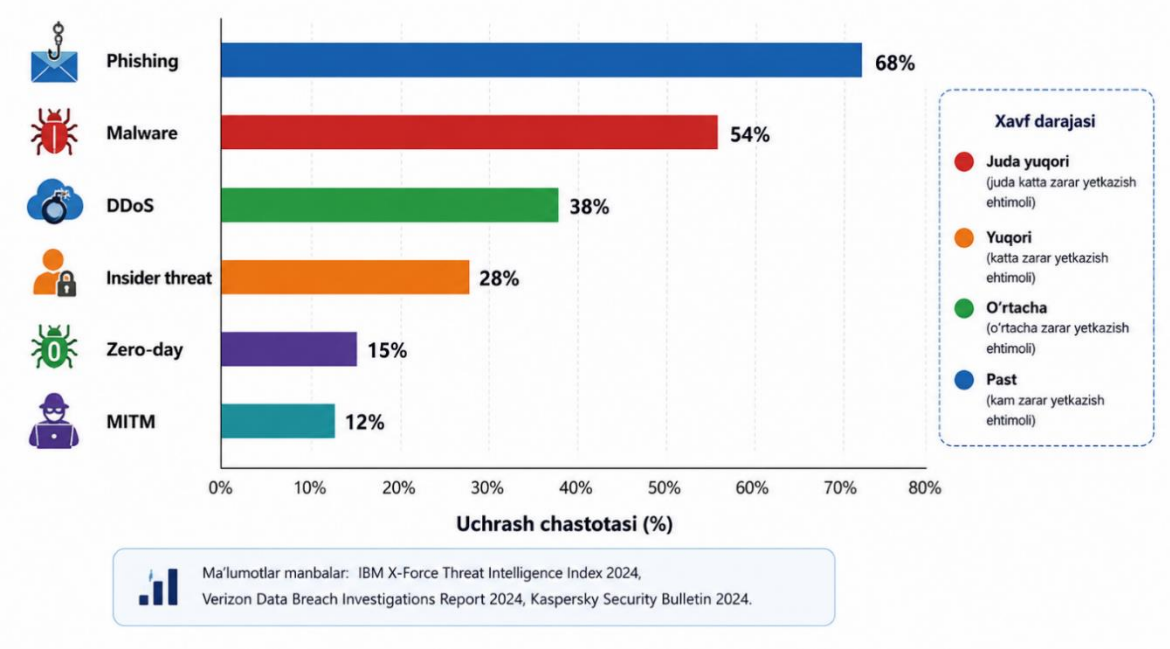
2-jadval. Tarmoq tahdidlarining uchrash chastotasi

Tahdid turi	Uchrash darajasi	Xavf darajasi
Fishing	Juda yuqori	Yuqori
Zararli dastur	Yuqori	Yuqori
DDoS	O‘rtacha	Juda yuqori
Insider threat	O‘rtacha	Yuqori
Zero-day	Past	Juda yuqori
MITM	Past	O‘rtacha

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-5



2-rasm. Tarmoq tahdidlarining tashkilotlardagi uchrash chastotasi

Xavfsizlik zaifliklari va tahdidlari. DDoS hujumlari zamonaviy tarmoq infratuzilmalariga eng katta xavf tug‘diruvchi tahdidlardan biri hisoblanadi[7]. Ushbu hujumda bir nechta qurilmalar (ko‘pincha botnet) maqsadli serverga juda katta hajmdagi trafik yuboradi, natijada xizmat ko‘rsatishda resurs yetishmasligi kuzatiladi.

DDoS hujumlarining asosiy turlari:

- Volumetrik hujumlar — bandwidthni to‘ldirishga qaratilgan;
- Protokol hujumlari — server resurslarini ekspluatatsiya qiladi;
- Ilova qatlami hujumlari — HTTP/HTTPS xizmatlariga hujum qiladi.

Ta’siri:

- xizmatning ishlamay qolishi;
- moliyaviy zarar;
- obro‘sizlanish;
- foydalanuvchi ishonchining kamayishi.

3-jadval. DDoS hujumlari va ta’siri

Hujum turi	Nishon	Ta’siri
UDP Flood	Tarmoq bandwidth	Xizmat uzilishi
SYN Flood	TCP stack	Server overload
HTTP Flood	Web xizmatlar	Sayt ishlamasligi

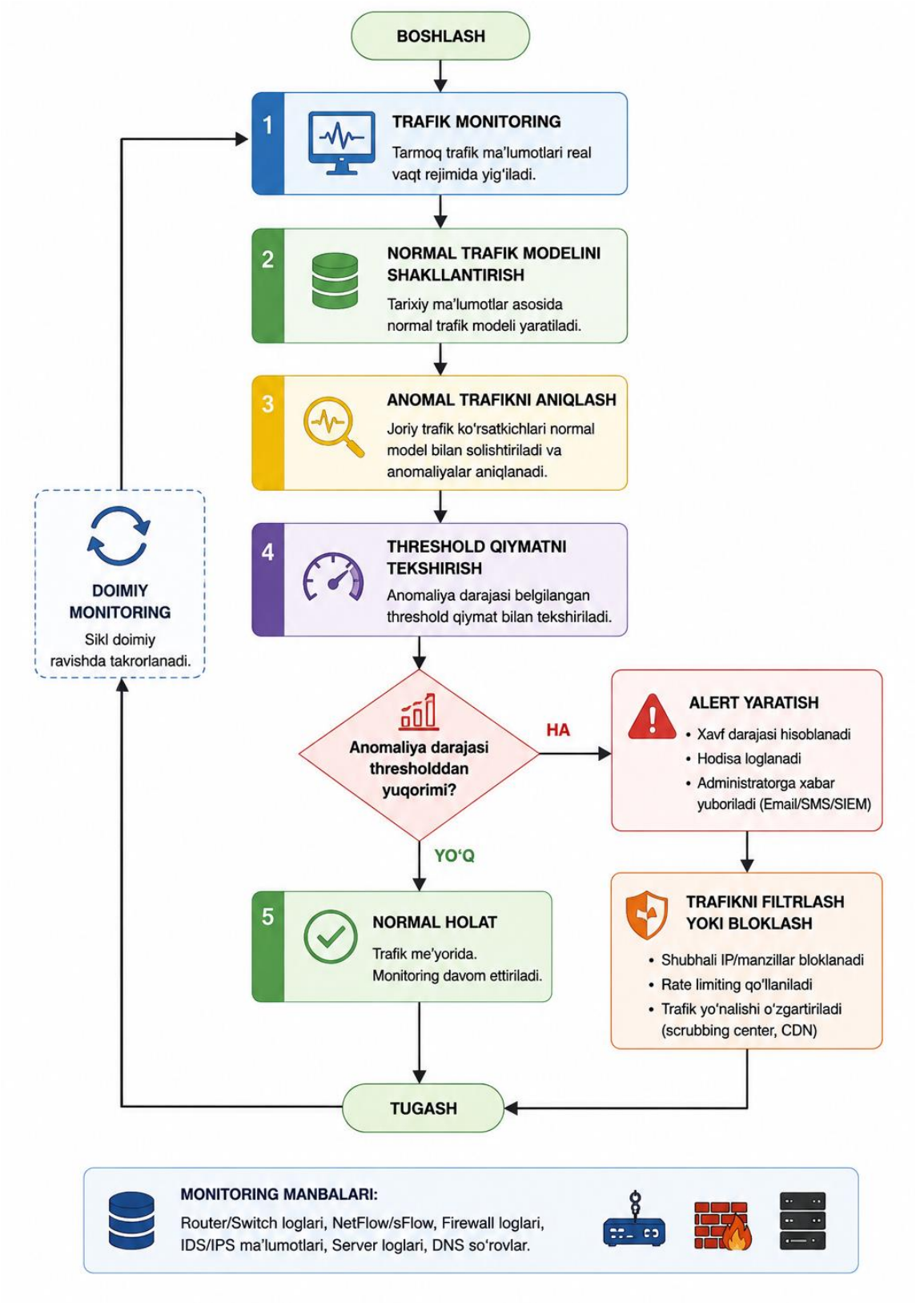
DDoS hujumini aniqlash algoritmi (tavsif)

1. Trafik monitoring qilinadi;
2. Normal trafik modeli shakllantiriladi;
3. Anomal trafik aniqlanadi;
4. Threshold qiymat oshsa alert yaratiladi;
5. Trafik filtrlanadi yoki bloklanadi. 3-rasmda algoritm ko‘rinishi keltirilgan.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-5



3-rasm. DDoS hujumini aniqlash algoritmi blok sxemasi

Zararli dastur — tizimga zarar yetkazuvchi dasturiy vositalar majmui hisoblanadi.

Zararli dastur turlari:

- Virus
- Qurt

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-5

- Trojan
- Josuslik dasturi (Spyware)
- Rootkit

“Ransomware” esa ma’lumotlarni shifrlab, tiklash uchun to‘lov talab qiluvchi zararli dasturdir.

Zararli dastur tahdidining oqibatlari quyidagilar bo‘lishi mumkin:

- ma’lumot yo‘qolishi;
- maxfiylik buzilishi;
- tizim ishlashining izdan chiqishi;
- iqtisodiy zarar.

4-jadval. Zararli dastur turlari qiyosiy tahlili

Zararli dastur turi	Tarqalish usuli	Zarari
Virus	Fayl orqali	Tizim buzilishi
Qurt	Tarmoq orqali	Tez tarqalish
Troyan	Soxta dastur	Ma’lumot o‘g‘irlash
Shpion dastur (Spyware)	Yashirin	Kuzatuv
Ransomware	Email/link	Fayl shifrlash

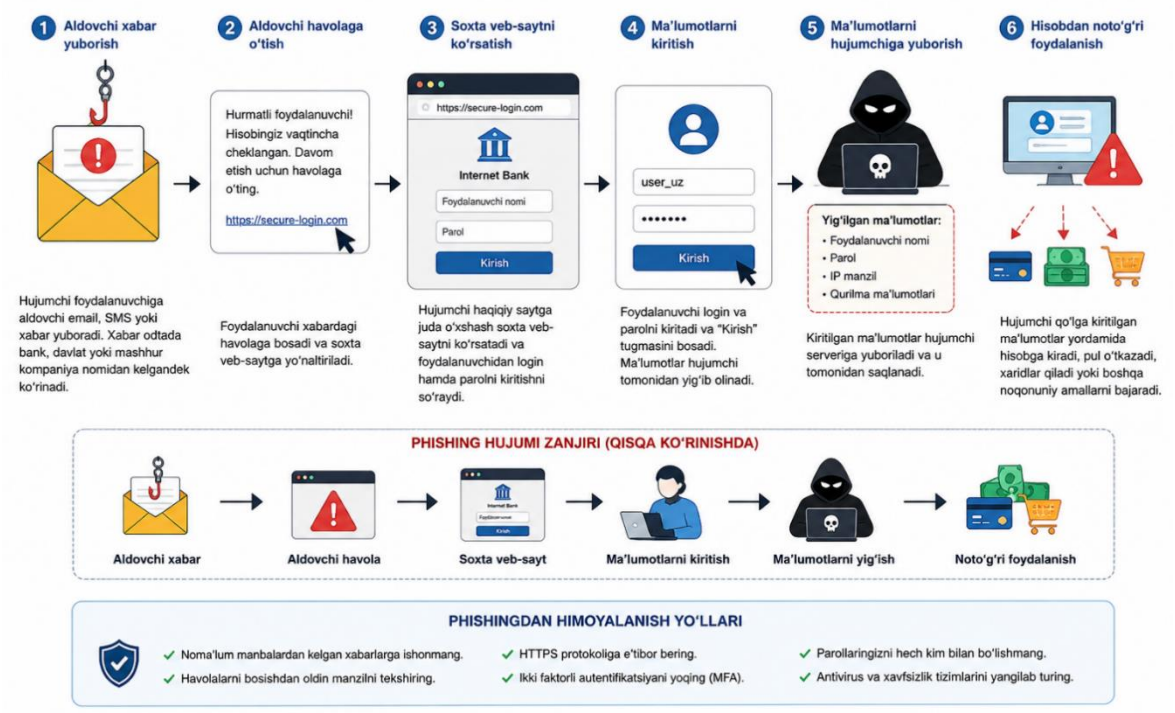
Fishing hujumlari. Fishing — foydalanuvchini aldash orqali maxfiy ma’lumotlarni qo‘lga kiritish usuli hisoblanadi[6].

Fishing hujumlarining ko‘rinishlari:

- Email fishing;
- Spear fishing;
- SMS fishing (smishing);
- Ovozli fishing (vishing).

Eng ko‘p nishonga olinayotgan ma’lumotlar:

- login va parollar;
- bank karta ma’lumotlari;
- OTP kodlari;
- korporativ akkauntlar.



ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

VOLUME-6, ISSUE-5

4-rasm. Fishing hujumlarining ishlash mexanizmi

Fishing hujumining xavflilik omillari quyidagilar:

- inson omili;
- xavfsizlik savodxonligi pastligi;
- MFA ishlatilmasligi.

Man-in-the-Middle (MITM) Attacks. MITM hujumi davomida hujumchi foydalanuvchi va server o‘rtasidagi trafikni yashirin kuzatadi yoki o‘zgartiradi[13].

MITM hujum usullari:

- ARP spoofing;
- Sessiyani o‘g‘irlash;
- DNS spoofing;
- Noqonuniy Wi-Fi.

MITM hujumi oqibatlari:

- sessiyani egallash;
- maxfiy ma’lumotlar o‘g‘irlanishi;
- tranzaksiyalarni manipulyatsiya qilish.

Ichki tahdidlar. Ichki tahdidlar ko‘plab tashkilotlarda eng xavfli tahdid sifatida qaraladi.

Sabablari:

- xodim noroziligi;
- noto‘g‘ri kirishni boshqarish;
- umumiy foydalanuvchi hisoblardan foydalanish;
- monitoring mavjud emasligi.

Insider threat darajalari

Tahdid turi	Sababi	Xavf
Intentional	Qasddan	Juda yuqori
Negligent	E’tiborsizlik	O‘rtacha
Compromised	Account buzilishi	Yuqori

Zero-day zaifligi — ishlab chiqaruvchi hali patch chiqarmagan dasturiy zaiflikdir.

Asosiy xavflar

- antivirus aniqlamasligi mumkin;
- exploit tez tarqaladi;
- katta masshtabdagi buzilishlar yuz beradi.

Zero-day hujumlarini kamaytirish usullari:

- davriy “patch”larni qo‘llash;
- zaifliklarni skanerlash;
- EDR/XDR tizimlari;
- Tahdid razvedkasi platformalarini qo‘llash.

5-jadval. Tahdidlar va xavf darajasi qiyosiy tahlili

Tahdid	Ehtimollik	Zarar darajasi	Ustuvorlik
DDoS	Yuqori	Yuqori	1
Fishing	Juda yuqori	O‘rtacha	1
Zararli dastur	Yuqori	Yuqori	1
Insider threat	O‘rtacha	Juda yuqori	2
MITM	Past	Yuqori	3
Zero-day	Past	Juda yuqori	2

Xavfsizlik choralari. Tarmoq xavfsizligini samarali ta’minlash uchun ko‘p qatlamli himoya mexanizmlaridan foydalanish zarur. Zamonaviy tashkilotlarda tahdidlarni kamaytirish uchun

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

texnik, tashkiliy va inson omiliga asoslangan choralar birgalikda qo‘llaniladi. “Defense in Depth” tamoyiliga ko‘ra, yagona himoya vositasiga tayanish emas, balki bir nechta xavfsizlik qatlamlarini tashkil etish maqsadga muvofiq hisoblanadi.

Xavfsizlik devori texnologiyalari

Firewall — kiruvchi va chiquvchi trafikni nazorat qiluvchi tarmoq xavfsizlik vositasidir. U oldindan belgilangan xavfsizlik siyosatlari asosida trafikni filtrlash imkonini beradi.

Firewall turlari:

- Paketlarni filtrlash xavfsizlik devori.
- “Stateful Inspection” xavfsizlik devori
- Proksi xavfsizlik devori.
- Keyingi avlod xavfsizlik devori (NGFW).

NGFW tizimlari an’anaviy firewall imkoniyatlariga qo‘shimcha ravishda:

- chuqur paket tekshiruvi;
- bosqinni oldini olish;
- zararli dasturlarni aniqlash;
- ilovalarni filtrlash kabi funksiyalarni ham taqdim etadi.

Afzalliklari:

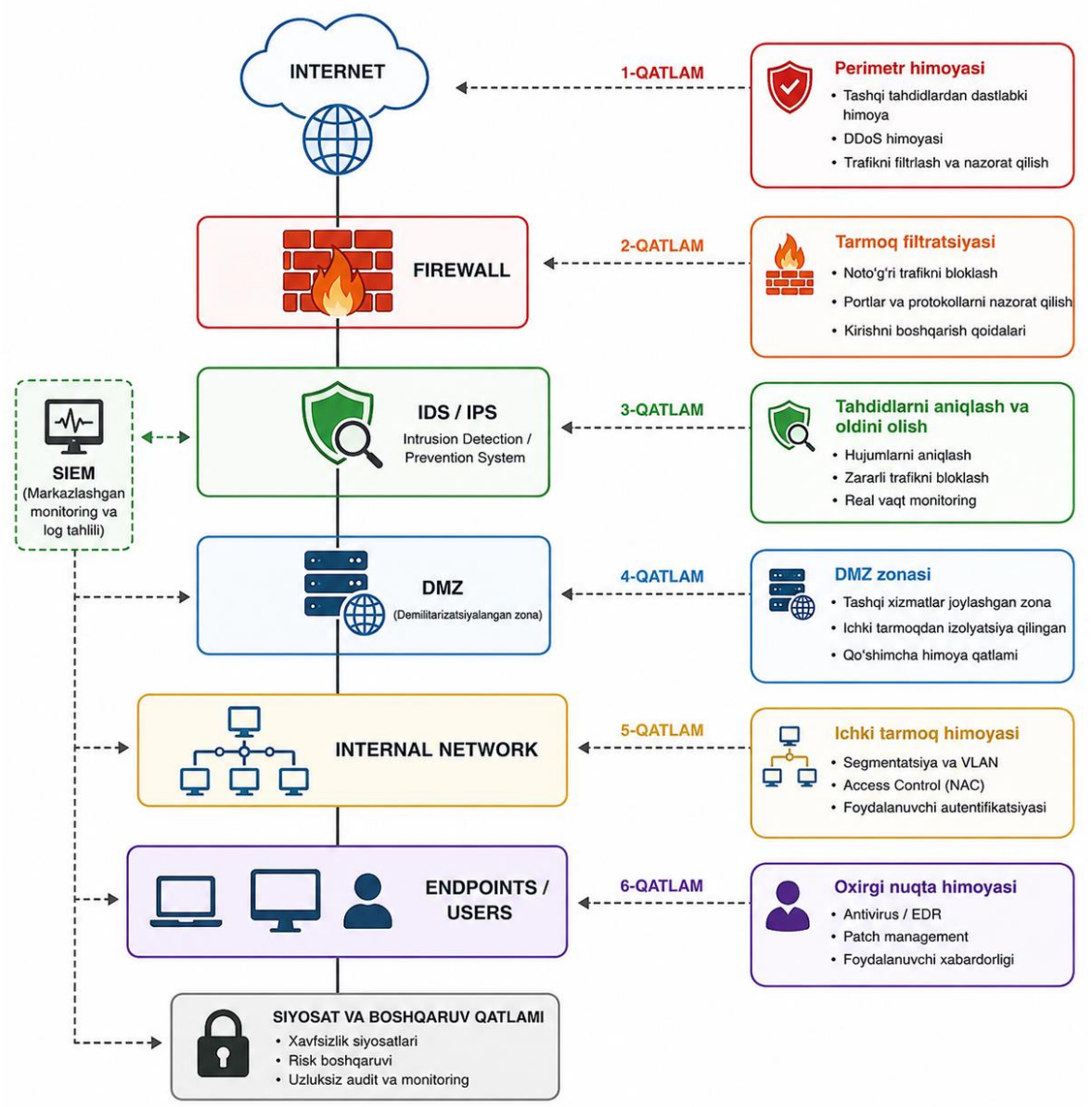
- noqonuniy trafikni bloklash;
- portlarni nazorat qilish;
- tarmoq segmentatsiyasi;
- kirishni cheklash.

Kamchiliklari:

- noto‘g‘ri konfiguratsiya xavfi;
- ichki tahdidlarga nisbatan samaradorligi past.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

VOLUME-6, ISSUE-5



5-rasm. Ko‘p qatlamli tarmoq himoyasi arxitekturasi

IDS/IPS tizimlari tarmoqdagi shubhali faoliyatlarni aniqlash va oldini olish uchun ishlatiladi[1].

IDS turlari:

1. Signatura asosidagi IDS

Oldindan ma’lum tahdid signaturalari asosida ishlaydi.

2. Anomaliya asosidagi IDS

Normal trafik modelidan chetga chiqishni aniqlaydi.

3. Gibrid IDS

Ikkala yondashuvni birlashtiradi.

IPS funksiyalari

- zararli trafikni bloklash;
- hujum sessiyasini to‘xtatish;
- avtomat tarzda ogohlantirish yaratish.

Sun’iy intellekt asosidagi IDS afzalliklari

- noaniq hujumlarni aniqlash;
- real vaqtda monitoring;

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

- noto‘g‘ri javob berishning kamayishi.

6-jadval. IDS va IPS tizimlarining qiyosiy tahlili

Xususiyat	IDS	IPS
Monitoring	Ha	Ha
Hujumni bloklash	Yo‘q	Ha
“Alert” yaratish	Ha	Ha
Trafikka ta’siri	Minimal	O‘rtacha

SIEM platformalari turli qurilmalar, serverlar va tarmoq uskunalaridan loglarni yig‘ib, markazlashgan monitoringni amalga oshiradi[11].

SIEM imkoniyatlari sifatida quyidagilarni keltirish mumkin:

- log korrelyatsiyasi;
- hodisani aniqlash;
- tahdid haqida ma’lumot;
- avtomatlashtirilgan javob.

Mashhur SIEM platformalari:

- Splunk;
- IBM QRadar;
- Elastic SIEM;
- Microsoft Sentinel.

Tashkilotlar uchun SIEM ahamiyati:

- real vaqt monitoring;
- forensik tahlil;
- compliance talablarini bajarish.

Ko‘p faktorli autentifikatsiya (MFA). Parolga asoslangan autentifikatsiya zamonaviy tahdidlarga qarshi yetarli emas[8]. Shu sababli ko‘p faktorli autentifikatsiya qo‘llaniladi.

MFA faktorlariga misollar:

1. Bilim omili — parol.
2. Egalik omili — OTP tokeni.
3. Biometrik omil — barmoq izi, Face ID

Afzalliklari:

- hisob ma’lumotlarini o‘g‘irlash xavfini kamaytiradi;
- Fishing natijasidagi zararlarni kamaytiradi;
- hisobni buzish darajasini pasaytiradi.

Shifrlash texnologiyalari. Kriptografik himoya tarmoqdagi ma’lumotlarning maxfiyligi va yaxlitligini ta’minlaydi.

Keng qo‘llaniladigan protokollar:

- TLS/SSL
- AES
- RSA
- VPN tunnellash

Qo‘llanilish sohalari

- internet banking;
- elektron hukumat;
- bulutli hisoblash;
- xavfsiz elektron pochta.

Sun’iy intellektga asoslangan xavfsizlik. Sun’iy intellekt tarmoq xavfsizligida tahdidlarni avtomatik aniqlashda keng qo‘llanilmoqda[1].

Sun’iy intellekt asosidagi xavfsizlik imkoniyatlari:

- anomaliyani aniqlash;

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

- xulq-atvor tahlili;
- bashoratli tahdid tahlili;
- avtomatlashgan javob.

Kamchiliklari:

- katta hajmdagi dataset talab qiladi;
- noto‘g‘ri javob xavfi mavjud;
- hisoblash resurslari ko‘p talab etiladi.

7-jadval. Himoya mexanizmlarining samaradorligi

Himoya vositasi	Tahdidlarni aniqlash	Narx	Samaradorlik
Firewall	O‘rtacha	Past	O‘rtacha
IDS/IPS	Yuqori	O‘rtacha	Yuqori
SIEM	Juda yuqori	Yuqori	Juda yuqori
MFA	Yuqori	Past	Yuqori
Sun’iy intellektga asoslangan xavfsizlik	Juda yuqori	Yuqori	Juda yuqori

O‘zbekistonda raqamli iqtisodiyot va elektron hukumat tizimlarining rivojlanishi natijasida axborot xavfsizligi masalalari ustuvor yo‘nalishga aylangan[9]. Davlat xizmatlari, bank tizimlari, elektron to‘lov platformalari va masofaviy ta’lim tizimlarining rivojlanishi bilan bir qatorda kiberxavfsizlik tahdidlari ham ortib bormoqda.

Asosiy muammolar sifatida quyidagilarni keltirish mumkin:

1. Fishing va moliyaviy firibgarlik. Aholi orasida internet savodxonligining yetarli emasligi Fishing hujumlarining samaradorligini oshirmoqda.
2. Zaif konfiguratsiya

Ko‘plab tashkilotlarda:

- standart parollar;
- eski dasturiy ta’minot;
- “patch management” yetishmasligi kuzatiladi.

3. Mutaxassislar yetishmovchiligi. Axborot xavfsizligi bo‘yicha malakali mutaxassislar soni hali ham yetarli emas.
4. Eskirgan tizimlar. Eski tizimlardan foydalanish zaifliklarni oshiradi.

Amaldagi yechimlar:

O‘zbekistonda quyidagi yo‘nalishlarda ishlar olib borilmoqda:

- davlat axborot tizimlarini sertifikatsiyalash;
- CERT faoliyatini rivojlantirish;
- kiberxavfsizlik bo‘yicha qonunchilikni takomillashtirish;
- mahalliy SOC markazlarini tashkil qilish.

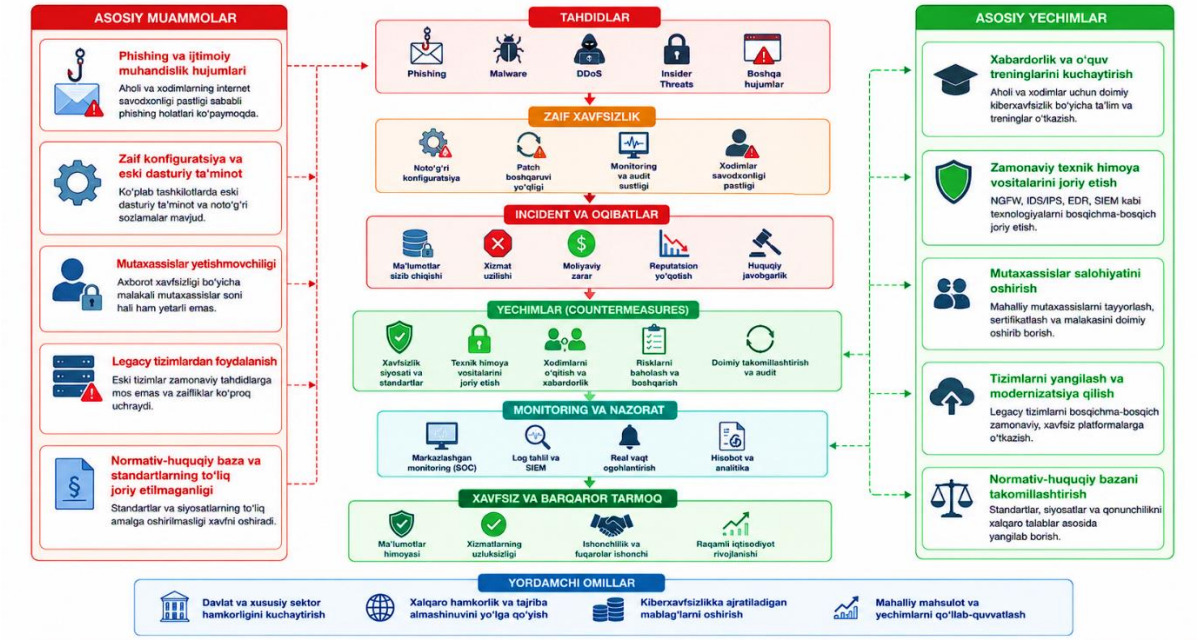
Taklif etilayotgan yechimlar:

1. Zero Trust arxitekturasini joriy qilish;
2. Milliy tahdid razvedkasi platformasi yaratish;
3. Sun’iy intellekt asosidagi monitoring tizimlarini joriy etish;
4. Kiber gigiyena bo‘yicha ommaviy treninglar.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-5



6-rasm. O‘zbekistonda tarmoq xavfsizligi muammolari va yechimlari diagrammasi

MUHOKAMA.

Tahlillar shuni ko‘rsatadiki, tarmoq axborot xavfsizligidagi tahdidlar murakkablashib bormoqda. Ayniqsa fishing va ransomware hujumlari tashkilotlarga katta iqtisodiy zarar yetkazmoqda. An’anaviy xavfsizlik vositalari ko‘plab holatlarda yetarli bo‘lmay qolmoqda.

Sun’iy intellekt asosidagi tizimlar va Zero Trust arxitekturasi istiqbolli yondashuv sifatida baholanmoqda[10]. Biroq ularni joriy etish katta xarajat va yuqori malakali mutaxassislarni talab qiladi.

O‘zbekiston sharoitida esa kiberxavfsizlikni kuchaytirish uchun texnik vositalar bilan bir qatorda foydalanuvchi savodxonligini oshirish ham muhim omil hisoblanadi.

Murakkabliklar. Tarmoq xavfsizligini ta’minlashda quyidagi muammolar mavjud:

- kiberhujumlarning murakkablashuvi;
- zero-day zaifliklar;
- IoT qurilmalar xavfsizligi;
- malakali mutaxassislar tanqisligi;
- katta hajmdagi loglarni qayta ishlash qiyinligi;
- xavfsizlik infratuzilmasining qimmatligi.

Xulosa. Mazkur maqolada tarmoq axborot xavfsizligi bilan bog‘liq muammolar, tahdidlar va ularning zamonaviy yechimlari kompleks ravishda tahlil qilindi. Tadqiqot natijalari shuni ko‘rsatdiki, Fishing, Zararli dastur, ransomware, ichki tahdidlar va DDoS hujumlari zamonaviy tashkilotlar uchun asosiy xavf omillari hisoblanadi.

Shuningdek, firewall, IDS/IPS, SIEM, MFA, kriptografik himoya va sun’iy intellekt asosidagi tizimlarning samaradorligi baholandi. O‘zbekiston sharoitida axborot xavfsizligini oshirish uchun texnologik vositalar bilan bir qatorda kiberxavfsizlik madaniyatini rivojlantirish ham muhimligi aniqlandi.

Kelgusida sun’iy intellekt asosidagi avtomatlashtirilgan tahdidlarni aniqlash tizimlari hamda Zero Trust arxitektura konsepsiyasi tarmoq xavfsizligini ta’minlashning asosiy yo‘nalishlaridan biri bo‘lishi kutilmoqda.

Foydalanilgan adabiyotlar

1. Buczak, A. L., & Guven, E. (2016). *A survey of data mining and machine learning methods for cyber security intrusion detection*. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

2. Cybersecurity Center of Uzbekistan. (2024). *Milliy kiberxavfsizlik monitoringi bo‘yicha yillik hisobot*. Toshkent, O‘zbekiston.
3. ENISA. (2024). *ENISA Threat Landscape 2024*. European Union Agency for Cybersecurity.
4. Goodrich, M. T., & Tamassia, R. (2019). *Introduction to computer security*. Pearson.
5. IBM. (2024). *IBM X-Force Threat Intelligence Index 2024*. IBM Security.
6. Jakobsson, M., & Myers, S. (2006). *Fishing and countermeasures: Understanding the increasing problem of electronic identity theft*. Wiley.
7. Kaspersky. (2024). *Kaspersky Security Bulletin 2024*. Kaspersky Lab.
8. NIST. (2020). *Zero Trust Architecture (SP 800-207)*. National Institute of Standards and Technology.
9. Raqamli texnologiyalar vazirligi. (2024). *O‘zbekistonda raqamli transformatsiya va kiberxavfsizlik holati bo‘yicha hisobot*. Toshkent.
10. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture*. NIST.
11. Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention systems (IDPS)*. NIST.
12. Shackleford, D. (2023). *Modern cybersecurity technologies and network defense*. SANS Institute.
13. Stallings, W. (2018). *Network security essentials: Applications and standards* (6th ed.). Pearson.
14. Verizon. (2024). *Data Breach Investigations Report 2024*. Verizon Enterprise.
15. Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.

Ishtirok etish uchun anketa shakli

№	**Anketa shakli**	
1.	Muallifning F.I.O. (to‘liq)	Shukurov Orziqul Pardayevich
2.	Tashkilot (ish joyi)	Muhammad al-Xorazmiy nomidagi TATU
3.	Material (maqola) nomi	
4.	Sho‘ba nomi (yo‘nalishi)	
5.	Aloqa uchun telefon raqam	myheartumi@gmail.com
6.	E-mail	+998 99 663 69 90