ISSN 3060-4567

KIBERXAVFSIZLIK VA AXBOROT HIMOYASI SOHASIDAGI ZAMONAVIY YONDASHUVLAR

G‘iyosov Shavkatjon Ergashaliyevich
To‘raqo‘rg‘on tuman 1-son texnikumi
“Informatika va AT” fani o‘qituvchisi

Annotatsiya: *Ushbu maqolada kiberxavfsizlik va axborot himoyasi sohasida qo‘llanilayotgan zamonaviy texnologiyalar, xalqaro standartlar, ilg‘or metodologiyalar va ularning korporativ, davlat hamda global infratuzilmalardagi qo‘llanishi tahlil qilinadi. Shuningdek, sun’iy intellekt, kvant texnologiyalari, Zero Trust modeli, raqamli identifikatsiya tizimlari, axborot xavfsizligi risklarini boshqarish va kiberbarqarorlik konsepsiyalarining amaliy hamda nazariy jihatlari ko‘rib chiqiladi. Maqola ISO/IEC 27001, NIST Cybersecurity Framework, GDPR, MITRE ATT&CK kabi xalqaro standartlar kontekstida yondashuvlarni o‘rganadi.*

Kalit so‘zlar: *Kiberxavfsizlik, axborot himoyasi, Zero Trust, ISO/IEC 27001, sun’iy intellekt xavfsizligi, ma’lumotlarni himoyalash, kvant kriptografiyasi, risklarni boshqarish, MITRE ATT&CK, kiberbarqarorlik.*

Kirish

Raqamli iqtisodiyotning kengayishi, davlat xizmatlarining onlayn shaklga o‘tishi, korxonalar faoliyatining to‘liq raqamlashtirilishi axborot xavfsizligini zamonaviy boshqaruv tizimlarining ajralmas qismiga aylantirdi. Bugungi global muhitda kiberxavfsizlik nafaqat texnik, balki strategik, iqtisodiy, huquqiy va geopolitik ahamiyatga ega bo‘lgan sohadir. 2025–2030 yillar oralig‘ida kiberhujumlarning intensivligi 5–7 barobarga ko‘payishi, zarar esa trillionlab dollarga yetishi prognoz qilinmoqda.

Shu sababli, xalqaro standartlar asosida axborot tizimlarini himoyalash, kiberhujumlarni aniqlash, ularga javob berish va ularning oldini olish mexanizmlarini takomillashtirish dolzarb masala bo‘lib qolmoqda. Kiber tahdidlar

tabiati murakkablashib borar ekan, ularni bartaraf etish uchun yangi yondashuvlar, intellektual tizimlar va ilg‘or xavfsizlik arxitekturasi talab etiladi.

Mazkur maqolada kiberxavfsizlikning tadqiqotga loyiq zamonaviy paradigmalari, xalqaro standartlarga asoslangan boshqaruv tizimlari, texnik va tashkiliy choralar, shuningdek, sun’iy intellekt davrida axborot himoyasining transformatsiyasi yoritiladi.

Raqamli transformatsiya jarayonlari global miqyosda keng quloch yoyar ekan, kiberxavfsizlik masalalari har qachongidan ko‘ra dolzarbroq tus olmoqda. Bugungi kunda iqtisodiyotning deyarli barcha tarmoqlari — moliya, energetika, ta’lim, sog‘liqni saqlash, sanoat, transport va davlat boshqaruvi tizimlari — raqamli infratuzilmaga tayanadi. Mazkur jarayonning ijobiy jihatlaridan tashqari, axborot tizimlariga nisbatan tahdidlar ham geometrik progressiya asosida ortib bormoqda. Raqamli xizmatlarga to‘liq o‘tish jarayoni, IoT qurilmalarining keskin ko‘payishi va sun’iy intellektning hujumchilarga ham keng imkoniyat yaratib berishi global xavfsizlik ekotizimi oldiga yangi murakkab vazifalarni qo‘ymoqda.

Kiberjinoyatchilar bugun an’anaviy zararli dasturlardan foydalanish bilan cheklanib qolmay, balki murakkab ssenariylar, sun’iy intellekt yordamida optimallashtirilgan hujumlar, davlat tomonidan qo‘llab-quvvatlangan kiberoperatsiyalar va ta’minot zanjiri orqali yashirin infiltratsiya kabi texnik jihatdan takomillashgan metodlardan foydalanmoqda. Bu esa korxonalar, davlat idoralari va xalqaro tashkilotlar uchun axborot xavfsizligini global boshqaruv darajasiga ko‘tarishni talab qiladi.

Shuningdek, zamonaviy jamiyatda shaxsiy ma’lumotlar, biometrik axborot, moliyaviy operatsiyalar, sanoat ishlab chiqarish jarayonlari hamda muhim infratuzilmalarning uzluksiz faoliyati nafaqat texnik, balki huquqiy, ijtimoiy va iqtisodiy xavfsizlik bilan chambarchas bog‘liq. Shu bois, kiberxavfsizlikni ta’minlash faqat texnik vositalar bilan cheklanmay, balki xalqaro standartlar, davlat siyosati, tashkilot ichki reglamentlari, risklarni boshqarish tizimlari va inson omilini qamrab oluvchi kompleks yondashuvni talab etadi.

Ushbu maqolaning maqsadi — kiberxavfsizlik va axborot himoyasi sohasidagi mazkur zamonaviy yondashuvlarni keng tahlil qilish, xalqaro standartlar bilan bog‘lash, zamonaviy tahdidlar tabiatini ilmiy asosda o‘rganish va istiqboldagi rivojlanish yo‘nalishlarini yoritishdan iborat.

1. Kiberxavfsizlikning zamonaviy tahdidlar manzarasi

1.1. Raqamli tizimlarga nisbatan yangi xavf turlari

Zamonaviy kiberxavfsizlikning asosiy muammosi – tahdidlar spektrining kengayishi va ularning murakkablashuvidir. Hozirgi tahdidlar quyidagi toifalarga bo‘linadi:

- **AI asosidagi hujumlar** – generativ AI orqali phishing xabarlarni avtomatik yaratish, deepfake audio/video bilan ijtimoiy muhandislik.
- **Supply-chain attacks** – kompaniyaga bevosita emas, balki texnik xizmat ko‘rsatuvchi sheriklar orqali hujum.
- **Ransomware 2.0** – nafaqat ma’lumotni bloklash, balki uni o‘g‘irlab, qo‘sh bosqichli shantaj.
- **IoT va IIoT hujumlari** – aqlli texnikalar, sanoat boshqaruv tizimlari, SCADA tizimlar zaifliklari.
- **Cloud-native hujumlar** – konteynerlar, orchestration tizimlari (Kubernetes), serverless arxitekturalardagi zaifliklar.
- **Kvant tahdidlari** – mavjud kriptografiyaning kelajakda kvant kompyuterlari tomonidan buzilishi ehtimoli.

1.2. Tahdidlar dinamikasining oshishi

Kiberhujumlarning o‘sishiga quyidagi faktorlar sabab:

- Raqamli xizmatlarga to‘liq o‘tish (bank, davlat, tibbiyot, ta’lim).
- Tarmoqlararo o‘zaro bog‘lanishning murakkablashuvi.
- Kiberjinoyatning iqtisodiy samara beruvchi biznesga aylanishi.
- Sun’iy intellektning himoya emas, hujum maqsadida ham qo‘llanishi.

Bu omillar davlatlar va tashkilotlardan yangi avlod kiberxavfsizlik strategiyasiga o‘tishni talab etadi.

ISSN 3060-4567

2. Xalqaro standartlar va boshqaruv tizimlari

2.1. ISO/IEC 27001:2022

ISO/IEC 27001 xalqaro axborot xavfsizligi boshqaruv standartidir. Uning asosiy mohiyati:

- Axborot xavfsizligini tizimli boshqarish (ISMS).
- Risklarni aniqlash, baholash va minimallashtirish.
- Siyosat, protsedura, texnik va tashkiliy choralarni integratsiya qilish.

2022-yilgi versiya 93 ta boshqaruv choralarini 4 asosiy kategoriya bo‘yicha belgilaydi:

1. Tashkiliy choralar
2. Kadrlar xavfsizligi
3. Texnik choralar
4. Fizik xavfsizlik

ISO 27001 kompaniyalarga xalqaro miqyosda ishonchli hamkorlik imkonini beradi.

2.2. NIST Cybersecurity Framework (NIST CSF)

NIST CSF AQSh Milliy Standartlar Instituti tomonidan ishlab chiqilgan bo‘lib, 5 asosiy funksiyani o‘z ichiga oladi:

- **Identify** (identifikatsiya) – aktivlar, zaifliklar, risklar ro‘yxatini yuritish.
- **Protect** (himoya qilish) – kirishlarni boshqarish, kriptografiya, xavfsizlik siyosatlari.
- **Detect** (aniqlash) – monitoинг, anomaliya aniqlash, loglar tahlili.
- **Respond** (javob berish) – insidentlarni boshqarish.
- **Recover** (tiklash) – xizmatlarni qayta ishga tushirish, barqarorlikni oshirish.

Ko‘pgina davlatlar, jumladan Yevropa Ittifoqi, Yaponiya va Janubiy Koreya o‘z kiberxavfsizlik siyosatlarini NIST modeli asosida ishlab chiqmoqda.

2.3. GDPR va ma’lumotlarni himoyalash standartlari

ISSN 3060-4567

Yevropa ma’lumotlarni himoya qilish reglamenti – GDPR – shaxsiy ma’lumotlarga ishlov berish bo‘yicha eng qat’iy standartlardan biridir. Uning asosiy talablari:

- Ma’lumotlarni minimal yig‘ish
- Ma’lumot subyekti huquqlarini ta’minlash
- Shaffoflik
- Maxfiylik bo‘yicha o‘rnatilgan mexanizmlar ("Privacy by Design")

Bugun ko‘plab davlatlar GDPRga mos milliy qonunchiliklarni yaratmoqda.

3. Zamonaviy xavfsizlik arxitekturalari

3.1. Zero Trust Architecture (Nol Ishonch modeli)

Zero Trust prinsipi:

“Hech kimga ishonma, doim tekshir.”

Uning asosiy tamoyillari:

- Foydalanuvchi va qurilmalar identifikatsiyasini doimiy tasdiqlash
- Minimal ruxsat huquqlari (Least Privilege)
- Tarmoqni segmentatsiya qilish
- Trafikni doimiy monitor qilish
- Zaifliklar bo‘yicha real vaqt baholash

Zero Trust yirik korporatsiyalar (Google BeyondCorp) tomonidan keng qo‘llanilmoqda.

3.2. SASE (Secure Access Service Edge)

SASE – tarmoq va xavfsizlik xizmatlarini yagona bulut platformasiga birlashtiruvchi yondashuv. Unda:

- SD-WAN
- Firewall-as-a-Service
- Zero Trust Network Access
- Secure Web Gateway
- Cloud Access Security Broker

SASE raqamli korxonalar uchun eng mos zamonaviy model hisoblanadi.

3.3. XDR (Extended Detection and Response)

An’anaviy antivirus o‘rnini bosuvchi tizim:

- Endpoint, tarmoq, bulut, e-mail bo‘yicha integratsiyalashgan himoya
- Sun’iy intellekt asosidagi anomaliya aniqlash
- Insident tahlili va avtomatik javob berish

4. Sun’iy intellekt va kiberxavfsizlik

4.1. AI yordamida himoya

AI quyidagi yo‘nalishlarda qo‘llanadi:

- Trafik anomaliyalarini aniqlash
- Deep learning asosida phishing va zararli fayllarni tahlil qilish
- Avtomatik insidentga javob berish
- Xulq-atvor tahlili (UEBA)

4.2. AI asosidagi hujumlar

Sun’iy intellekt hujumlarni kuchaytirmoqda:

- Deepfake orqali insonlarni aldash
- AI yordamida kod yozish va eksploit yaratish
- Avtomatlashtirilgan kiberhujum dronlari
- Social engineeringning yuqori samaradorlik bilan olib borilishi

Shu sabab, AI xavfsizligini boshqarish strategiyalari yaratish zarur.

5. Ma’lumotlarni himoyalashning ilg‘or usullari

5.1. Post-quantum cryptography (PQC)

Kvant kompyuterlari RSA va ECC algoritmlarini buzishi mumkin. Shu sabab yangi algoritmlar ishlab chiqilmoqda:

- CRYSTALS-Kyber
- CRYSTALS-Dilithium
- Falcon
- Sphincs+

PQC kelajakdagi axborot xavfsizligi tayanchi bo‘ladi.

5.2. Homomorfik shifrlash

ISSN 3060-4567

Ma’lumotni shifrlangan holatda qayta ishlash imkonini beradi. U:

- tibbiyot ma’lumotlari
- moliya operatsiyalari
- davlat xizmatlarida

maxfiylikni oshiradi.

5.3. Blockchain orqali xavfsizlik

Blockchain:

- tarqatilgan arxitektura
- o‘zgarmas yozuvlar
- markazlashmagan boshqaruv

orqali xavfsizlikni yangi bosqichga ko‘taradi.

6. Kiberxavfsizlikda risklarni boshqarish

6.1. Risk tahlili modellari

Zamonaviy risk modellari:

- OCTAVE
- FAIR (Factor Analysis of Information Risk)
- ISO 31000

Risklarni baholashda:

1. aktivlar qiymati
2. tahdidlar ehtimoli
3. zaifliklar
4. potentsial zarar

bosqichma-bosqich aniqlanadi.

6.2. Kiberbarqarorlik (Cyber Resilience)

Kiberbarqarorlik – hujumdan keyin ham xizmatlarni uzluksiz davom ettirish qobiliyatidir. Unda:

- redundans
- avariya rejasi (BCP, DRP)
- tizimlarning diversifikatsiyasi

ISSN 3060-4567

- avtomatik tiklash mexanizmlari

muhim rol o‘ynaydi.

7. MITRE ATT&CK va kiberhujumlarni tahlil qilish

MITRE ATT&CK – kiberhujum taktik va texnikalarining global ma’lumotlar bazasi. U:

- hujum bosqichlarini aniqlash
- zaifliklarni baholash
- himoya choralarini tanlash
- insidentga javob berish

uchun asosiy vosita bo‘lib xizmat qiladi.

8. Kiberxavfsizlikda inson omili

Tadqiqotlar shuni ko‘rsatadiki, kiberhujumlarning **70% dan ortig‘i inson xatosi** bilan bog‘liq. Shuning uchun:

- xodimlar uchun muntazam treninglar
- phishing simulyatsiyalari
- xavfsizlik siyosatlariga amal qilishni nazorat qilish
- ichki tahdidlarni boshqarish

asosiy ahamiyatga ega.

Xulosa

Kiberxavfsizlik sohasidagi zamonaviy yondashuvlar kompleks tizimli qarashni talab qiladi. Tahdidlarning murakkablashuvi, sun’iy intellektning tezkor rivojlanishi, bulut infratuzilmasining kengayishi va kvant texnologiyalarining paydo bo‘lishi axborot xavfsizligini boshqarishda yangi paradigmalarga o‘tishni taqozo etmoqda.

Ushbu maqolada Zero Trust, SASE, XDR, post-kvant kriptografiya, AI asosidagi himoya tizimlari, xalqaro standartlar (ISO/IEC 27001, NIST CSF, GDPR), MITRE ATT&CK kabi zamonaviy yondashuvlar yoritildi. Kelgusi yillarda tashkilotlar kiberbarqarorlikni oshirish, xavfsizlikni avtomatlashtirish, identifikatsiya va kirishlarni boshqarishni kuchaytirish, ma’lumotlar maxfiyligini

ISSN 3060-4567

himoyalash bo‘yicha izchil strategiyalarni amalga oshirishi muhim ahamiyat kasb etadi.

FOYDALANILGAN ADABIYOTLAR

1. ISO/IEC 27001:2022 International Standard for Information Security Management Systems.
2. NIST Cybersecurity Framework, National Institute of Standards and Technology, 2023.
3. GDPR – General Data Protection Regulation, European Parliament, 2018.
4. MITRE ATT&CK Framework, MITRE Corporation.
5. Schneier B. "Applied Cryptography".
6. P.W. Singer, Allan Friedman. "Cybersecurity and Cyberwar".
7. ENISA Threat Landscape Report 2024.
8. Microsoft Digital Defense Report 2023.
9. IBM Data Breach Report 2024.
10. ENISA – Zero Trust Architecture Guidelines, 2022.