KIBERXAVFSIZLIK VA MA'LUMOTLARNI HIMOYA QILISH TEXNOLOGIYALARI

Chilonzor tuman 2-son texnikumi

Yangiboyeva Nilufar Azamat qizi

nilufaryangiboeva07@gmail.com

944136864

Annotatsiya

Ushbu maqolada kiberxavfsizlikning zamonaviy holati, asosiy tahdidlar va ma'lumotlarni himoya qilishning ilg'or texnologiyalari tahlil etiladi. Maqolada kriptografiya, ko'p faktorli autentifikatsiya, Zero Trust arxitekturasi, sun'iy intellektga asoslangan himoya tizimlari, bulutli xavfsizlik va kvant kriptografiyasi kabi yo'nalishlar chuqur ko'rib chiqiladi. Ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligi (CIA triad) ni ta'minlashning ilmiy va amaliy jihatlari yoritiladi. Maqola kiberxavfsizlik sohasidagi dolzarb muammolar va kelajakdagi yo'nalishlarga alohida e'tibor qaratadi.

Kalit so'zlar: kiberxavfsizlik, ma'lumotlar himoyasi, kriptografiya, Zero Trust, sun'iy intellekt, kvant kriptografiyasi, bulut xavfsizligi, kibertahdidlar.

Kirish

Raqamli transformatsiya davrida ma'lumotlar eng qimmatbaho resursga aylandi. Biroq, internet, IoT qurilmalari, bulut texnologiyalari va sun'iy intellektning jadal rivojlanishi bilan birga kiberxavfsizlik tahdidlari ham keskin ortmoqda. 2025–2026 yillarda global miqyosda ransomware hujumlari, ma'lumotlar o'g'irlash va davlat tomonidan qo'llab-quvvatlanadigan kiberoperatsiyalar soni rekord darajaga yetdi.

Kiberxavfsizlik — bu axborot tizimlarini ruxsatsiz foydalanish, o‘zgartirish, yo‘q qilish yoki mavjudligini buzishdan himoya qilish fan va amaliyotidir. Ma’lumotlarni himoya qilish esa maxfiylik (confidentiality), yaxlitlik (integrity) va mavjudlik (availability) tamoyillariga asoslanadi (CIA triad).

Kiberxavfsizlik — bu raqamli tizimlar, tarmoqlar va ma'lumotlarni ruxsatsiz kirish, o'g'irlash yoki shikastlanishdan himoya qilish majmuasidir. U zamonaviy shifrlash, ko'p faktorli autentifikatsiya (MFA) va sun'iy intellektga asoslangan tahlil texnologiyalarini o'z ichiga oladi. O'zbekistonda kiberxavfsizlikni ta'minlash va huquqiy asoslarni tartibga solish bo'yicha batafsil ma'lumot olish uchun O'zbekiston Respublikasi Kiberxavfsizlik markazi rasmiy portalidan foydalaning. [1, 2, 3]

Ma'lumotlarni himoya qilish va kiberxavfsizlikni ta'minlashda quyidagi ilg'or texnologiyalar va yondashuvlar muhim ahamiyatga ega:

- **Shifrlash (Encryption):** Ma'lumotlarni o'qib bo'lmaydigan kodga aylantiradi. AES (Advanced Encryption Standard) kabi algoritmlar ma'lumotlarni saqlash va uzatish vaqtida xavfsizligini ta'minlaydi.
- **Ko'p faktorli autentifikatsiya (MFA):** Foydalanuvchilardan tizimga kirish uchun paroldan tashqari qo'shimcha tasdiq (masalan, SMS-kod yoki biometriya) talab qilib, ruxsatsiz kirishni qiyinlashtiradi.
- **Firewall (Tarmoq ekranlari):** Kiruvchi va chiquvchi tarmoq trafigini tahlil qilib, shubhali ulanishlarni bloklaydi va xakerlik hujumlarini oldini oladi.
- **SIEM (Xavfsizlik hodisalarini boshqarish):** Tizimdagi voqealarni real vaqt rejimida tahlil qilib, g'ayritabiiy harakatlarni (masalan, zararli dastur faolligini) aniqlaydi.
- **Zero Trust (Nol ishonch) arxitekturasi:** Tarmoq ichidagi yoki tashqarisidagi hech bir foydalanuvchi yoki qurilmaga avtomatik tarzda ishonmaydigan zamonaviy himoya konsepsiyasi.

- **VPN (Virtual xususiy tarmoq):** Internet tarmog'ida ma'lumotlarni shifrlangan tunnel orqali uzatib, shaxsiy ma'lumotlarni yashirin saqlaydi.
  Axborot xavfsizligini ta'minlash jarayonida tizimni muntazam yangilab turish va xodimlarning kiberxavfsizlik bo'yicha savodxonligini oshirish eng asosiy himoya vositalaridan hisoblanadi.
- KIBER XAVFSIZLIK VA AXBOROT TIZIMLARIDA MA ...
  U xavfsiz kompyuter tizimlarini yaratish, amalga oshirish, tahlillash va testlashni o'z ichiga oladi. Kiberxavfsizlik ta'limning m...
- KIBERXAVFSIZLIK-SHAXSIY MA'LUMOTLARNI HIMOYA ...
  1 июл. 2025 г. — Mazkur maqolada kiberxavsizlikning elementlari va uning kompyuterlar, serverlar, mobil qurilmalar, elektron tizimlar, tarmoqlar va...

kiberxavfsizlik obyekti — axborotning kiberhimoya qilinishini hamda milliy axborot tizimlari va resurslarining kiberxavfsizligini ...

Zamonaviy kibertahdidlar

Hozirgi kunda eng keng tarqalgan tahdidlar quyidagilardir:

- **Ransomware** — ma’lumotlarni shifrlab, to‘lov talab qilish;
- **Phishing va spear-phishing** — ijtimoiy muhandislik orqali hisob ma’lumotlarini o‘g‘irlash;
- **DDoS-hujumlar** — xizmatni rad etish;
- **Advanced Persistent Threats (APT)** — uzoq muddatli, murakkab hujumlar;
- **Supply chain attacks** (masalan, SolarWinds hujumi);

- **IoT va 5G tarmoqlaridagi zaifliklar**.

Statistikaga ko‘ra, 2025 yilda bitta ma’lumotlar buzilishi o‘rtacha 4,88 million AQSh dollariga tushadi (IBM Cost of a Data Breach Report).

3. Ma’lumotlarni himoya qilishning asosiy texnologiyalari

Kriptografiya Ma’lumotlar himoyasining asosiy vositasi.

- **Simmetrik kriptografiya**: AES-256 — eng ishonchli standart;
- **Asimmetrik kriptografiya**: RSA, ECC (Elliptic Curve Cryptography);
- **End-to-End Encryption (E2EE)**: Signal, WhatsApp kabi ilovalarda qo‘llaniladi;
- **Homomorphic Encryption** — shifrlangan holatda hisoblash imkonini beradi;
- **Post-Quantum Cryptography** — kvant kompyuterlar tahdidiga qarshi NIST standartlari (Kyber, Dilithium).

Kirishni boshqarish va autentifikatsiya

- **Multi-Factor Authentication (MFA) va Passwordless** (biometrik, FIDO2);
- **Role-Based Access Control (RBAC)** va **Attribute-Based Access Control (ABAC)**;
- **Zero Trust Architecture** — “hech kimga ishonma, har doim tekshir” tamoyili. Har bir so‘rov alohida tekshiriladi.

Tarmoq va tizim himoyasi

- **Next-Generation Firewall (NGFW)**;
- **Intrusion Detection/Prevention Systems (IDS/IPS)**;
- **Endpoint Detection and Response (EDR)** va **Extended Detection and Response (XDR)**;
- **Security Information and Event Management (SIEM)** tizimlari.

Sun’iy intellekt va mashinaviy o‘qitish

Sun’iy intellekt kibertahdidlarni real vaqtda aniqlashda inqilobiy rol o‘ynaydi:

- Anomaliyalarni aniqlash;
- Avtomatik javob berish;
- Bashoratli tahlil (predictive analytics);
- Deepfake va AI-generated hujumlariga qarshi kurash.

Bulutli va distribyutiv tizimlar xavfsizligi

- CASB (Cloud Access Security Broker);
- Container Security (Docker, Kubernetes);
- Data Loss Prevention (DLP) tizimlari.

Qonuniy va axloqiy jihatlar

Ma’lumotlarni himoya qilishda GDPR (Yevropa), CCPA (Kaliforniya), O‘zbekiston Respublikasining “Axborotlashtirish to‘g‘risida”gi Qonuni va “Shaxsiy ma’lumotlar to‘g‘risida”gi Qonuni muhim o‘rin tutadi. Xalqaro standartlar (ISO/IEC 27001, NIST Cybersecurity Framework) keng qo‘llanilmoqda.

Dolzarb muammolar va kelajak yo‘nalishlari

- Kvant kompyuterlarning klassik kriptografiyani buzish xavfi;
- AI qurollari o‘rtasidagi “qurollanish poygasi”;
- Inson omili (insider threats);
- Ma’lumotlar suvereniteti va geosiyosiy xavflar.

Kelajakda **Quantum Key Distribution (QKD)**, **Blockchain-based** identifikatsiya, **Confidential Computing** va **Autonomous Cybersecurity Systems** ustuvor yo‘nalishlar bo‘ladi.

Xulosa

Kiberxavfsizlik va ma’lumotlarni himoya qilish texnologiyalari nafaqat texnik, balki strategik ahamiyatga ega. Texnologik yechimlar bilan birga inson

resurslarini oshirish, xalqaro hamkorlik va doimiy innovatsiyalar talab etiladi. O‘zbekiston kabi rivojlanayotgan mamlakatlar uchun milliy kiberxavfsizlik strategiyasini kuchaytirish, mahalliy mutaxassislar tayyorlash va zamonaviy texnologiyalarni joriy etish dolzarb vazifadir.

Adabiyotlar

1. IBM Security. (2025). *Cost of a Data Breach Report*.
2. NIST. (2024). *Post-Quantum Cryptography Standardization*.
3. Gartner. (2025). *Top Security and Risk Management Trends*.
4. Stallings, W. (2020). *Cryptography and Network Security*. Pearson.
5. O‘zbekiston Respublikasi Qonunlari: “Shaxsiy ma’lumotlar to‘g‘risida” (2021).
6. National Cyber Security Centre (NCSC) va ENISA hisobotlari.