GLOBAL JOURNAL OF CROSS-DISCIPLINARY INNOVATIONS
Multidisciplinary peer-reviewed scholarly journal
GJCDI
Vol. 1 | Issue 3
Year: 2026

BULUTLI TEXNOLOGIYALAR VA SUN'IY INTELLEKT DAVRIDA KIBERXAVFSIZLIK TAHDIDLARI VA ULARNING OLDINI OLISH CHORALARI

Bektoyev Behzod Mirmuhsin o`g`li
Farg`ona davlat texnika universiteti "telekommunikatsiya va kiber xavfsizlik injineringi talabasi

Annotatsiya
Ushbu maqolada zamonaviy axborot texnologiyalari, xususan, bulutli hisoblash tizimlari (Cloud Computing) va sun'iy intellekt (AI) rivojlanishi davridagi kiberxavfsizlik muammolari tadqiq etilgan. Maqolada eng ko'p uchrayotgan kiberhujum turlari, ularning tizimlarga yetkazadigan zarari va zamonaviy himoya mexanizmlari tahlil qilingan. Shuningdek, ma'lumotlar xavfsizligini ta'minlashda "Nol ishonch" (Zero Trust) arxitekturasi va sun'iy intellektga asoslangan xavfsizlik tizimlarining roli yoritilgan.
Kalit so'zlar: Kiberxavfsizlik, bulutli texnologiyalar, sun'iy intellekt, fishing, Zero Trust, fishing hujumlari, ma'lumotlar sizib chiqishi.

KIRISH

Raqamli transformatsiya davrida davlat tashkilotlari, bank-moliya sektori va xususiy kompaniyalar o`z faoliyatini bulutli platformalarga ko`chirmoqda. Bu jarayon ish unumdorligini oshirsa-da, kiberjinoyatchilar uchun yangi zaifliklarni (vulnerabilities) keltirib chiqarmoqda.

Bugungi kunda kiberhujumlar nafaqat oddiy foydalanuvchilarga, balki strategik muhim infratuzilmalarga ham jiddiy tahdid solmoqda. Shuning uchun, kiberxavfsizlikni ta'minlashning yangi innovatsion usullarini ishlab chiqish zamon talabidir.

ZAMONAVIY KIBERTAHDIDLAR TAHLILI

So`nggi yillarda kiberhujumlarning tabiati va murakkabligi keskin o`zgardi. Asosiy tahdidlar quyidagilardan iborat:

• Fishing (Phishing) va Ijtimoiy muhandislik: Sun'iy intellekt (masalan, Deepfake va ilg'or matn generatorlari) yordamida fishing xatlari shunday tayyorlanmoqdaki, ularni oddiy foydalanuvchi haqiqiysidan ajrata olmaydi.

• To'lov dasturlari (Ransomware): Tizimlarni bloklab, ma'lumotlarni qaytarish evaziga kriptovalyutada pul talab qilish holatlari ko`paygan.

• Bulutli muhitdagi zaifliklar: API kalitlarining noto`g`ri sozlanishi yoki bulutli omborlarga kirish huquqlarining noto`g`ri taqsimlanishi yirik ma'lumotlar sizib chiqishiga (Data Breach) sabab bo'lmoqda. Bunga aniq dalillardan biri respublikmizga yaqinda bo`lgan hujumlardan biri "Butterfly" xakkerlarlar jamoasi tarafidan 27mlnga yaqin fuqarolarni shaxsiy malumotlari o`g`irlanishidir bu ma`lumotlardir ammo bu xakkerlik amali Respublika amaldorlarini shu kabi kamchiliklar borligi to`g`risida ogohlantirish maqsadida amalga oshirilgan "oq xakkerlik" amaliyoti ekanligi ma'lum bo`ldi

SUN’IY INTELLEKT: KIBERXAVFSIZLIKDA QUROL VA QALQON

Sun’iy intellekt (AI) kiberxavfsizlikda ikki tomonlama rol o‘ynamoqda:

1. Hujum vositasi sifatida: Xakerlar tizimlardagi zaif nuqtalarni avtomatik tarzda qidirish va aqlli zararli dasturlarni (malware) yaratishda AIdan foydalanmoqda.
2. Himoya vositasi sifatida: Zamonaviy Antivirus va SIEM (Security Information and Event Management) tizimlari tarmoq trafigini real vaqt rejimida tahlil qilib, noodatiy harakatlarni (anomaliyalarni) aniqlaydi va hujumni inson aralashuvisiz to‘xtatadi.

SAMARALI HIMOYALANISH STRATEGIYALARI

Kiberxavfsizlikni yangi bosqichga ko`tarish uchun quyidagi konseptual yondashuvlarni joriy etish zarur:

• "Zero Trust" (Nol ishonch) modeli: "Hech qachon ishonma, doim tekshir" tamoyili. Tarmoq ichidagi har bir foydalanuvchi va qurilma har safar qaytadan autentifikatsiyadan o‘tishi shart.
• Ko`p bosqichli autentifikatsiya (MFA): Faqat parolgadir, balki biometrik ma’lumotlar yoki bir martalik kodlar yordamida himoyani kuchaytirish.
• Kibergigiyena madaniyati: Xodimlarni muntazam ravishda kiberxavfsizlik bo‘yicha o`qitish va fishing testlaridan o‘tkazish.

XULOSA

Kiberxavfsizlik — bu tugaydigan jarayon emas, balki doimiy rivojlanib boruvchi kurashdir. Texnologiyalar rivojlangani sari kiberhujumlar ham murakkablashib boraveradi. Bulutli tizimlar va sun’iy intellekt davrida xavfsizlikni ta’minlash uchun faqatgina an’anaviy dasturlar bilan cheklanib qolmasdan, Zero Trust arxitekturasini joriy etish va sun’iy intellektga asoslangan himoya tizimlaridan keng foydalanish lozim.

Adabiyotlar ro`yxati (References)

1. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley & Sons.
2. Nakamoto, S. (2019). Cyber Security Threats in the Age of Cloud Computing. International Journal of Computer Science, 45(2), 112-120.
3. O`zbekiston Respublikasining "Kiberxavfsizlik to‘g‘risida"gi Qonuni, 2022-yil.
4. UzDaily.uz “BUTTERFLY guruhi O‘zbekiston tizimlarida zaifliklar aniqlanganini bildirdi”// UzDaily.uz, 03.11.2026.