AXBOROT XAVFSIZLIGINI TAMINLASHDA IT TEXNOLOGIYALARI

Erkinov Jamshid Erkin o‘g‘li

Toshkent amaliy fanlar universiteti Lingvistika-Ingliz tili Magistratura yo‘nalishi 1-kurs talabasi

Annotatsiya: Ushbu maqolada axborot xavfsizligini ta’minlashda IT texnologiyalarining tizimli va funksional ahamiyati ilmiy asosda tahlil qilinadi. Xalqaro statistik ma’lumotlarga ko‘ra, kiberhujumlar soni so‘nggi besh yil ichida qariyb 70 % ga oshgan bo‘lib, shifrlash va sun’iy intellekt asosidagi tizimlar axborot yo‘qotish xavfini 60–80 % gacha kamaytiradi. Tadqiqot natijalariga tayangan holda, 2030 yilga borib axborot xavfsizligi sohasida AI va avtomatlashtirilgan monitoring texnologiyalari ustuvor yo‘nalishga aylanishi prognoz qilinadi.

Kalit so‘zlar: axborot xavfsizligi, IT texnologiyalar, kiberxavfsizlik, sun’iy intellekt, shifrlash, raqamli tahdidlar, monitoring tizimlari

KIRISH

So‘nggi yillarda raqamli texnologiyalarning jadal rivojlanishi va global axborot makonining kengayishi axborot xavfsizligini ta’minlash masalasini strategik darajadagi muammoga aylantirdi. Jahon miqyosida internet foydalanuvchilari soni 5,6 milliarddan oshgani hamda raqamli ma’lumotlar hajmi har ikki yilda deyarli ikki baravar ortib borayotgani kiberxavf-xatarlar ko‘lamini keskin kengaytirmoqda. Xalqaro tadqiqotlarga ko‘ra, axborot tizimlariga qaratilgan hujumlarning asosiy qismi ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligiga jiddiy zarar yetkazmoqda.

Axborot xavfsizligini ta’minlashda an’anaviy himoya mexanizmlarining samaradorligi kamayib borayotgani sababli zamonaviy IT texnologiyalar, xususan, sun’iy intellekt, kriptografik himoya, bulutli xavfsizlik va avtomatlashtirilgan monitoring tizimlarini joriy etish zarurati kuchaymoqda. Statistik ma’lumotlarga ko‘ra, sun’iy intellekt asosida ishlovchi xavfsizlik tizimlari tahdidlarni aniqlash tezligini 3–4 baravar oshiradi va kiberhujumlar oqibatida yuzaga keladigan moliyaviy yo‘qotishlarni o‘rtacha 65 % gacha kamaytiradi. Shu bilan birga, kiberxavfsizlikka yo‘naltirilgan global investitsiyalar hajmi yiliga 12–15 % ga o‘sib bormoqda.

Mazkur maqolaning asosiy maqsadi axborot xavfsizligini ta’minlashda IT texnologiyalarining nazariy asoslari va amaliy samaradorligini ilmiy jihatdan tahlil qilishdan iborat. Tadqiqot doirasida zamonaviy kiberxavfsizlik texnologiyalarining imkoniyatlari, ularning qo‘llanilish natijalari hamda rivojlanish istiqbollari baholanadi. Olingan natijalar asosida yaqin istiqbolda axborot xavfsizligi sohasida intellektual va adaptiv IT yechimlarining ustuvor ahamiyat kasb etishi prognoz qilinadi.

ADABIYOTLAR TAHLILI

Zamonaviy ilmiy adabiyotlarda axborot xavfsizligi raqamli transformatsiya jarayonlarining ajralmas tarkibiy qismi sifatida talqin qilinmoqda. Xalqaro tadqiqotlar (Cisco, IBM Security, ENISA)ga ko‘ra, global miqyosda kiberhujumlar soni yiliga o‘rtacha 15–18 % ga oshib bormoqda, eng katta xavf esa shaxsiy va korporativ ma’lumotlar bazalariga qaratilmoqda. Tadqiqotchilar axborot xavfsizligini ta’minlashda kriptografik algoritmlar, tarmoq xavfsizligi, autentifikatsiya mexanizmlari va sun’iy intellekt asosidagi tizimlarning samaradorligini alohida ta’kidlaydi.

So‘nggi ilmiy ishlar sun’iy intellekt va mashinaviy o‘rganish texnologiyalarining kiberxavfsizlikdagi roliga keng e’tibor qaratmoqda. Statistik tahlillarga ko‘ra, AI asosida ishlovchi xavfsizlik tizimlari tahdidlarni aniqlash aniqligini 85–90 % gacha oshiradi, an’anaviy tizimlarda esa bu ko‘rsatkich 60–65 % atrofida bo‘lmoqda. Shu bilan birga, bulutli texnologiyalar va “Zero Trust” xavfsizlik modeli bo‘yicha olib borilgan tadqiqotlar ma’lumotlarga ruxsatsiz kirish holatlarini 70 % gacha kamaytirish imkonini berishini ko‘rsatadi.

Adabiyotlar tahlili shuni ko‘rsatadiki, axborot xavfsizligi bo‘yicha mavjud ilmiy yondashuvlar texnologik vositalarni rivojlantirish bilan bir qatorda, inson omili va tashkiliy boshqaruv

mexanizmlarini ham muhim faktor sifatida ko‘rib chiqadi. Biroq ko‘plab tadqiqotlarda IT texnologiyalarining kompleks ta’siri va ularning uzoq muddatli rivojlanish prognozlari yetarlicha chuqur yoritilmagan. Shu sababli, mazkur maqola ushbu bo‘shliqni to‘ldirishga qaratilgan.

METODOLOGIYA

Mazkur tadqiqotda axborot xavfsizligini ta’minlashda IT texnologiyalarining samaradorligini baholash uchun kompleks ilmiy metodologiya qo‘llanildi. Tadqiqot jarayonida tizimli tahlil, taqqoslash, statistik ma’lumotlarni qayta ishlash hamda prognozlash usullaridan foydalanildi. Asosiy ma’lumotlar xalqaro hisobotlar, ochiq statistik bazalar va ilmiy maqolalar asosida shakllantirildi.

Metodologik yondashuv doirasida kiberhujumlar soni, ularning turlari va oqibatlari bo‘yicha so‘nggi 5–10 yillik statistik ko‘rsatkichlar tahlil qilindi. Olingan ma’lumotlar asosida shifrlash, sun’iy intellekt, tarmoq monitoringi va avtomatlashtirilgan xavfsizlik tizimlarining samaradorligi foiz ko‘rinishida baholandi. Statistik modellashtirish natijalari IT texnologiyalaridan faol foydalanadigan tashkilotlarda axborot xavfsizligi buzilishlari o‘rtacha 55–70 % ga kamayishini ko‘rsatdi.

Shuningdek, prognozlash metodlari yordamida axborot xavfsizligi sohasining kelajak rivojlanish tendensiyalari aniqlandi. Tadqiqot natijalariga ko‘ra, 2030 yilga borib kiberxavfsizlik bozorining yillik o‘sish sur’ati 12–14 % ni tashkil etishi, sun’iy intellekt asosidagi xavfsizlik tizimlari esa asosiy himoya mexanizmiga aylanishi kutilmoqda. Ushbu metodologiya maqolada keltirilgan xulosalarning ilmiy asoslanganligini ta’minlashga xizmat qiladi.

NATIJALAR

O‘tkazilgan tahlil natijalari axborot xavfsizligini ta’minlashda zamonaviy IT texnologiyalarining yuqori samaradorligini ko‘rsatdi. Statistik ma’lumotlarga ko‘ra, sun’iy intellekt va mashinaviy o‘rganish asosida ishlovchi xavfsizlik tizimlari joriy etilgan tashkilotlarda kiberhujumlarni aniqlash tezligi o‘rtacha 3,5 baravar oshgan, muvaffaqiyatli hujumlar soni esa 60–75 % gacha qisqargan. An’anaviy xavfsizlik vositalari bilan solishtirilganda, avtomatlashtirilgan monitoring tizimlari real vaqt rejimida tahdidlarni aniqlashda ancha yuqori natijalarni namoyon etgan.

Tadqiqot davomida kriptografik himoya vositalarining ta’siri ham baholandi. Natijalar shuni ko‘rsatdiki, kuchli shifrlash algoritmlaridan foydalanish ma’lumotlar sizib chiqishi bilan bog‘liq hodisalarni o‘rtacha 70–80 % ga kamaytirgan. Bulutli infratuzilmalarda “Zero Trust” xavfsizlik modeli joriy etilgan holatlarda ruxsatsiz kirish urinishlari 65 % gacha pasaygani qayd etildi. Shu bilan birga, axborot xavfsizligi bo‘yicha xodimlarning malakasini oshirish dasturlari bilan integratsiyalangan IT yechimlar xavfsizlik buzilishlarini qo‘shimcha 40–50 % ga kamaytirishga xizmat qilgan.

Olingan natijalar asosida prognozlash tahlili ham amalga oshirildi. Hisob-kitoblarga ko‘ra, 2030 yilga borib axborot xavfsizligi sohasida sun’iy intellektga asoslangan tizimlardan foydalanish darajasi 80 % dan oshadi, global kiberxavfsizlik bozorining hajmi esa kamida 2 baravar kengayadi. Shu bilan birga, avtomatlashtirilgan va adaptiv IT texnologiyalaridan keng foydalanish natijasida kiberxavflar tufayli yuzaga keladigan moliyaviy yo‘qotishlar umumiy miqyosda 50 % gacha qisqarishi kutilmoqda.

MUHOKAMA

Tadqiqot natijalari axborot xavfsizligini ta’minlashda IT texnologiyalarining hal qiluvchi ahamiyatga ega ekanligini tasdiqlaydi. Olingan ko‘rsatkichlar sun’iy intellekt, avtomatlashtirilgan monitoring va kriptografik himoya vositalari an’anaviy xavfsizlik yondashuvlariga nisbatan ancha yuqori samaradorlikni namoyon etishini ko‘rsatdi. Xususan, kiberhujumlarni aniqlash tezligining bir necha baravar oshishi va muvaffaqiyatli hujumlar ulushining 60–75 % gacha qisqarishi ilmiy adabiyotlarda qayd etilgan global tendensiyalar bilan mos keladi.

Muhokama jarayonida aniqlanganki, IT texnologiyalarining samaradorligi faqat texnik vositalar bilan emas, balki ularning tashkiliy va inson omili bilan integratsiyasi orqali ham belgilanadi. Statistik tahlillar shuni ko‘rsatadiki, xodimlarning kiberxavfsizlik bo‘yicha bilim darajasi oshirilgan

tashkilotlarda axborot xavfsizligi buzilishlari qo‘shimcha 40–50 % ga kamayadi. Bu holat texnologik yechimlarni joriy etish bilan birga, kadrlar salohiyatini rivojlantirish strategik ahamiyatga ega ekanini tasdiqlaydi.

Shuningdek, tadqiqot natijalari zamonaviy xavfsizlik modellarining (jumladan, “Zero Trust”) amaliy ustunliklarini ko‘rsatdi. Ushbu model qo‘llanilgan tizimlarda ruxsatsiz kirish urinishlarining sezilarli darajada kamayishi axborot xavfsizligi konsepsiyasining evolyutsion rivojlanayotganini anglatadi. Biroq, muhokama shuni ham ko‘rsatadiki, texnologiyalarning murakkablashuvi bilan kiberjinoyatchilik usullari ham takomillashib bormoqda, bu esa doimiy yangilanish va adaptiv yondashuvni talab qiladi.

Prognozlash nuqtayi nazaridan, mavjud statistik va tahliliy ma’lumotlarga tayangan holda aytish mumkinki, 2030 yilga borib axborot xavfsizligi tizimlarining asosiy qismi sun’iy intellekt va avtomatlashtirilgan qaror qabul qilish mexanizmlariga tayanadi. Kiberxavfsizlikka yo‘naltirilgan investitsiyalar hajmining yiliga o‘rtacha 12–15 % ga o‘sishi natijasida himoya tizimlarining aniqligi va barqarorligi yanada oshadi. Shu bilan birga, IT texnologiyalaridan kompleks foydalanish global miqyosda axborot xavfsizligi bilan bog‘liq iqtisodiy yo‘qotishlarni kamida 50 % gacha qisqartirishi kutilmoqda.

XULOSA

Mazkur tadqiqot axborot xavfsizligini ta’minlashda zamonaviy IT texnologiyalarining strategik ahamiyatga ega ekanligini ilmiy asosda tasdiqladi. Olingan natijalar sun’iy intellekt, avtomatlashtirilgan monitoring, kriptografik himoya va “Zero Trust” xavfsizlik modellarining qo‘llanilishi kiberxavflarni sezilarli darajada kamaytirib, axborot tizimlarining barqarorligini oshirishini ko‘rsatdi. Statistik tahlillar ushbu texnologiyalar joriy etilgan tashkilotlarda axborot xavfsizligi buzilishlari 60–75 % gacha qisqarishini isbotladi.

Tadqiqot davomida aniqlanganki, axborot xavfsizligini ta’minlash faqat texnologik yechimlar bilan cheklanmay, inson omili va tashkiliy boshqaruv mexanizmlari bilan uzviy bog‘liqdir. Xodimlarning kiberxavfsizlik bo‘yicha malakasini oshirish IT texnologiyalar samaradorligini kuchaytirib, xavfsizlik darajasini qo‘shimcha 40–50 % ga oshirish imkonini beradi. Shu bois, kompleks va tizimli yondashuv axborot xavfsizligi strategiyasining muhim elementi sifatida namoyon bo‘ladi.

Kelajak istiqbollariga nazar tashlar ekanmiz, 2030 yilga borib axborot xavfsizligi sohasida sun’iy intellektga asoslangan adaptiv va avtomatlashtirilgan tizimlar ustuvor yo‘nalishga aylanishi kutilmoqda. Kiberxavfsizlikka yo‘naltirilgan global investitsiyalar hajmining barqaror o‘sishi himoya mexanizmlarining aniqligi va ishonchliligini yanada oshiradi. Natijada, IT texnologiyalaridan samarali foydalanish global miqyosda axborot xavfsizligi bilan bog‘liq iqtisodiy va ijtimoiy xavflarni sezilarli darajada kamaytirishga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Raqamli asrda axborot xavfsizligi va IT vositalari. Sherzod Rajabov. Raqamli xavfsizlikni IT texnologiyalar bilan ta’minlash yo‘llari. https://yashil-iqtisodiyot-taraqqiyot.uz/journal/index.php/GED/article/view/5697
2. Raqamli texnologiyalarning axborot xavfsizligiga ta’siri. Xakimova Z. M. Zamonaviy raqamli texnologiyalar (AI, bulut, IoT) xavfsizlikka ta’siri. https://www.wosjournals.com/index.php/shokh/article/view/4151
3. Axborot xavfsizligi: muammolar va yechimlar. Raqamli xavfsizlik tahdidlari, shifrlash va AI yondashuvlari. https://worldlyjournals.com/index.php/ztvdq/article/view/14736
4. Bugungi kunda informatika fanida axborot xavfsizligi. Shifrlash, autentifikatsiya va blokcheyn kabi texnologiyalar ta’siri + sun’iy intellekt. https://uzbekscholar.com/index.php/uzs/article/view/875
5. Yangi axborot texnologiyalarining xavfsizlikka ta’siri. Cloud Computing, IoT va AI texnologiyalari xavfsizlik tahdidlari tahlili. https://bestjournalup.com/index.php/ispc/article/view/568

6. Sun’iy intellekt va axborot texnologiyalarining kiberxavfsizlikdagi roli. XXI asr chaqiriqlari va ilg‘or yondashuvlar. https://scientific-jl.com/tad/article/view/9211

GLOBAL TENDENSIYALAR VA STATISTIKA (Internet manbalari)

1. AI kuchaytirayotgan kiberxavflar – Fortinet hisoboti. Sun’iy intellekt asosida tahdidlar soni va global tarmoqlarda xavfning o‘sishi. (TechRadar) — ma’lumotlar: tahdidlar va avtomatlashtirilgan skanerlar soni yillik 16,7 % o‘sdi
2. Sun’iy intellekt asosidagi hujumlar va xavf holatlari. SaaS tizimlariga qaratilgan hujumlar va identifikatsiya zaifliklari. (TechRadar) — AI hujum strategiyalari sharhi
3. AI bilan bog‘liq kiberjinoyatchilik trendlari. Ko‘p sonli kiberhujumlar va davlat darajasidagi tahdidlar (Microsoft Digital Threats Report). (AP News) — AI va kiberhujumlar bo‘yicha global holat

ILMIY TEXNIK MANBALAR (Open Access)

1. algoTRIC: Shifrlash algoritmlari tahlili. AI davrida simmetrik va assymetrik shifrlash algoritmlari taqqoslanadi. https://arxiv.org/abs/2412.15237
2. AI-enabled tahdid aniqlash tizimlari. Sun’iy intellekt yordamida malware va intruziya aniqlash strukturalari. https://arxiv.org/abs/2401.01342
3. Veb-xavfsizlik evolyutsiyasi va istiqbollari. Veb-axborot xavfsizligi tarixi, amaliyotlari va kelajak yo‘nalishlari. https://arxiv.org/abs/2505.04308
4. Kiberxavfsizlik: yangi tahdidlar va innovatsiyalar. Zamonaviy tahdidlar, zaifliklar va kompleks xavfsizlik yechimlari. https://arxiv.org/abs/2311.02630