AXBOROT TEXNOLOGIYALARINING RIVOJLANISHI VA GLOBAL XAVFSIZLIKKA TA’SIRI

Sattorov Nazarbek Odiljonovich
Toshkent Shahar adliya boshqarmasi
bosh mutaxassisi

Annotatsiya:

Axborot texnologiyalarining (AT) tezkor rivojlanishi, internet va raqamli infratuzilmaning global miqyosda kengayishi bilan bog‘liq ravishda, milliy va global xavfsizlik masalalarini yangi, murakkab va ko‘p qirrali jihatlardan ko‘rib chiqishni talab qilmoqda. Ushbu ilmiy ishda axborot texnologiyalarining rivojlanishi va uning global xavfsizlikka ta’siri tahlil qilinadi. Asosan, kiberxavfsizlik, kiberhujumlar, axborot urushlari, ma'lumotlarni himoya qilish va global raqamli infrastrukturaga tahdidlar kabi muammolarni o‘rganish ko‘zda tutilgan.

Axborot texnologiyalarining kengayishi davlatlar o‘rtasidagi yangi xavfsizlik tahdidlarini yuzaga keltirmoqda, ayniqsa, kiberhujumlar va axborot manipulyatsiyasi sohasida. Ushbu ishda global xavfsizlik tizimi, xalqaro hamkorlik va kiberxavfsizlik siyosatining roli, shuningdek, davlatlarning milliy xavfsizlikni ta'minlashda axborot texnologiyalarini qo‘llashda duch keladigan qiyinchiliklar muhokama qilinadi. Shuningdek, yangi xavfsizlik paradigmasi, kiberterrorizm va raqamli suverenitet kabi yangi masalalar ko‘rib chiqiladi.

Ilmiy ishda texnik va huquqiy yondashuvlarning o‘zaro aloqasi, davlatlarning kiberxavfsizlik bo‘yicha olib borayotgan siyosati, shifrlash, autentifikatsiya va raqamli infratuzilmani himoya qilish usullari tahlil qilinadi. Global xavfsizlikni ta'minlashda xalqaro hamkorlik, kiberurushlar va raqamli iqtisodiyotning ta'siri, shuningdek, raqamli tahdidlar va kiberjinoyatchilikning yangi shakllari ham o‘ziga xos o‘rganiladigan masalalardir.

Ushbu ilmiy ish axborot texnologiyalarining xavfsizlikka ta'sirini yanada chuqurroq tushunishga yordam beradi va kelajakdagi xavfsizlik strategiyalarini shakllantirishda muhim ma'lumotlar taqdim etadi.

Kalit so‘zlar: Axborot texnologiyalari (IT), global xavfsizlik, kiberxavfsizlik, kiberhujumlar, internet xavfsizligi, axborot urushi, global xavfsizlikni ta'minlash, davlatlararo kiberhujumlar, global raqamli tahdidlar, ijtimoiy tarmoqlar.

Axborot oqimlarining globallashuvi: Bugungi kunda axborot global ravishda tez va oson tarqalmoqda, bu esa barcha davlatlar uchun yangi xavflar keltirib chiqarmoqda. Kiberhujumlar, axborot manipulyatsiyasi va ta’sir o‘tkazish texnikalari (masalan, "fake news") global miqyosda xavfsizlikni tahdid qilmoqda.

Global kiberhujumlar: Kiberhujumlar davlatlar o‘rtasidagi yangi turdagi

urushga aylanishi mumkin. Shu sababli, axborot texnologiyalari nafaqat milliy xavfsizlik, balki global xavfsizlikni ta’minlashda ham muhim ahamiyat kasb etadi.

Ijtimoiy tarmoqlar va siyosat: Axborot texnologiyalari siyosiy manipulyatsiyalarga, yalan ma’lumotlarning tarqalishiga va hatto davlatlar o‘rtasidagi diplomatik munosabatlarga ta’sir ko‘rsatmoqda. Ijtimoiy tarmoqlar va internetning keng tarqalishi demokratik tizimlarga tahdid solmoqda.

Ijtimoiy tarmoqlar bugungi kunda har bir insonning hayotida muhim o‘rin tutmoqda. Ammo ularning o‘rni va ta’siri ortgan sari, bu platformalarda yuzaga keladigan turli tahdidlar ham oshmoqda. Ijtimoiy tarmoqlarga bo‘lgan tahdidlar quyidagi asosiy yo‘nalishlarda namoyon bo‘lishi mumkin, bularga misol qilib oladigan bo‘lsak:

Shaxsiy ma’lumotlarning o‘g‘irlanishi va tarqatilishi. Ijtimoiy tarmoqlarda foydalanuvchilarning shaxsiy ma’lumotlari, xususan, email manzillari, telefon raqamlari, yashash joyi kabi ma’lumotlar to‘plangan holda, ular maxfiylik va xavfsizlik jihatidan tahdidlarga duchor bo‘ladi. Hakerlar bu ma’lumotlarni o‘g‘irlab, ular orqali firibgarlik va boshqa jinoyatlarni sodir etishlari mumkin.

Onlayn ta’qib va kiberhujumlar. Ijtimoiy tarmoqlarda anonimlikka ega bo‘lgan shaxslar boshqalarga qarshi ta’qib, haqorat va kiberhujumlar qilishlari mumkin. Bu esa, ayniqsa, yoshlar, mashhurlar yoki boshqaruvchilar uchun katta xavf tug‘diradi.

Fake news va disinformatsiya. Ijtimoiy tarmoqlarda noto‘g‘ri ma’lumotlar tarqatilishi, odamlarni aldagan holda jamiyatda noaniqlik va ishonchsizlikni yuzaga keltiradi. Bu jarayon ko‘pincha siyosiy yoki iqtisodiy maqsadlar uchun ishlatiladi.

Emotsional va psixologik salbiy ta’sirlar. Ijtimoiy tarmoqlarda bo‘lish, ayniqsa, yoshlar o‘rtasida o‘zini o‘zgalar bilan solishtirish, depressiya yoki stressga olib kelishi mumkin. Boshqa odamlarning faqat yaxshi taraflarini ko‘rish, o‘zini past baholash yoki kamchiliklarini his qilishga olib keladi.

Tarmoqlar orqali noqonuniy faoliyatlar. Ijtimoiy tarmoqlarda narkotik, qurol yoki boshqa noqonuniy mahsulotlarni sotish yoki tarqatish kabi noqonuniy faoliyatlar amalga oshirilishi mumkin. Bu nafaqat platformalarning xavfsizligiga tahdid soladi, balki jamiyatning qonunlariga ham zarar yetkazadi.

Internet orqali bullying (kichik ta'qib yoki hakoratlar). Onlayn bullyng yoki kiberbullying, ayniqsa, o‘smirlar o‘rtasida keng tarqalgan. Shaxslar ijtimoiy tarmoqlarda beqaror yoki haqoratli xabarlar yuborish orqali boshqalarga zarar yetkazishlari mumkin.

Kiberhujumlar va davlat xavfsizligi: Milliy xavfsizlikni ta'minlashda davlatlar o‘z infratuzilmasi va axborot tizimlarini himoya qilishga katta e’tibor qaratmoqdalar. Kiberxavfsizlik siyosati va strategiyasi milliy xavfsizlikning ajralmas qismiga aylanib bormoqda.

Davlatlararo kiberhujumlar — bu davlatlar o'rtasida internet orqali amalga oshiriladigan raqamli hujumlardir. Bunday hujumlar odatda davlat tomonidan yoki

davlatning manfaatlariga xizmat qiluvchi guruhlar tomonidan amalga oshiriladi va ularning maqsadi raqib davlatning infratuzilmasini buzish, ma'lumotlar o'g'irlash, davlat xavfsizligini tahdid qilish yoki boshqa turli xil siyosiy va iqtisodiy maqsadlarni amalga oshirish bo'lishi mumkin.

Kiberhujumlar (yoki kiberhujumlar) internet yoki boshqa tarmoqlar orqali amalga oshiriladigan zararli faoliyatlardir. Ushbu hujumlar maqsadga qaratilgan tizimlarni buzish, shaxsiy yoki moliyaviy ma'lumotlarni o‘g‘irlash, shuningdek, xizmatlarni yoki tizimlarni ishlamay qolishiga olib kelishdir. Kiberhujumlar turli shakllarda bo'lishi mumkin va ular nafaqat yirik kompaniyalar, balki oddiy foydalanuvchilarni ham nishon qilishi mumkin.

Global raqamli tahdidlar — bu butun dunyo bo'ylab turli davlatlar, tashkilotlar va shaxslar tomonidan amalga oshiriladigan, raqamli infratuzilma va tizimlar orqali yo'naltirilgan tahdidlar va hujumlardir. Raqamli tahdidlar turli shakllarda bo‘lishi mumkin, ularning ba’zilari xavfsizlikka, iqtisodiyotga, shaxsiy ma’lumotlarga, huquqlarga, va hatto demokratik institutlarga ham jiddiy tahdid soladi.

Xalqaro hamkorlik: Kiberxavfsizlik bo‘yicha xalqaro hamkorlikni kuchaytirish, BMT, NATO va boshqa xalqaro tashkilotlar orqali xavfsizlikni ta’minlash, kiberhujumlarni oldini olishda muhim rol o‘ynaydi.

Kiberqonunchilik: Davlatlar kiberjinoyatlarga qarshi qonunlar ishlab chiqib, jinoyatchilarni jazolash va xalqaro sudlarga olib chiqish imkoniyatlarini yaratadilar.

Kiberhujumlarga qarshi himoya tizimlarini rivojlantirish: Avtomatlashtirilgan xavfsizlik tizimlari, kiberhujumlarga qarshi mudofaa vositalarini ishlab chiqish va ularni amaliyotga tatbiq etish zarur. Shu bilan birga, tashkilotlar va davlatlar o'z xodimlarini kiberhujumlarga qarshi o'qitib, xabardorlikni oshirishi kerak.

Internet xavfsizligi (yoki **kiberxavfsizlik**) — bu internet tarmog‘idan foydalanishda shaxsiy va tashkilotlar ma’lumotlarini himoya qilish, onlayn tahdidlardan saqlanish va raqamli infratuzilmani xavfsiz holda ishlatish bo‘yicha chora-tadbirlarni o‘z ichiga oladi. Internet xavfsizligi faqatgina texnik masalalarni hal qilishdan iborat emas, balki odamlarning xatti-harakatlari, ma’lumotlarga ehtiyotkorlik bilan yondashuvlari va zamonaviy xavfsizlik tizimlaridan foydalanishlari ham muhim rol o‘ynaydi.

Ma’lumotlar xavfsizligi — bu shaxsiy va tijorat ma’lumotlarini muhofaza qilishni anglatadi. Bu, ma'lumotlarni o‘g‘irlash, yo‘q qilish yoki buzilishiga yo‘l qo‘ymaslik uchun turli usullarni (ma’lumotlarni shifrlash, parollarni himoya qilish, va hokazo) o‘z ichiga oladi. Ma’lumotlar xavfsizligi quyidagilarga e’tibor qaratadi:

Shifrlash: Ma'lumotlarni o‘qish yoki tushunish qiyin qilish uchun ularni shifrlash.

Backup (zahira nusxalari): Muqobil nusxalar yaratish va ma’lumotlarni yo‘qotishdan himoya qilish.

Axborotning maxfiyligini saqlash: Shaxsiy ma’lumotlarni himoya qilish va

noto‘g‘ri qo‘llanilishiga yo‘l qo‘ymaslik.

Tizim xavfsizligi — bu kompyuter tizimlarining ishlashini xavfsizligini ta'minlash va tizimlarga kirishni nazorat qilish. Tizimlar odatda zararli dasturlardan (viruslar, trojanlar, wurmlar) himoya qilish uchun antivirus va boshqa xavfsizlik dasturlari bilan himoyalanadi. Tizim xavfsizligini ta'minlash uchun:

Zarur xavfsizlik devorlari (firewall): Tizimlarga kirishning noxush yoki zararli harakatlaridan himoya qilish.

Tizim va dasturlarni muntazam yangilash: Ular xavfsizlik yamoqlari va patch-lari yordamida himoya qilish.

Tarmoq xavfsizligi — bu kompyuter tarmoqlaridagi ma’lumotlarni himoya qilish, zararli trafikdan va hujumlardan himoyalanishdir. Bu turdagi xavfsizlik, ayniqsa, korporativ tarmoqlarda muhim ahamiyatga ega. Tarmoq xavfsizligi quyidagilarni o‘z ichiga oladi:

Firewall va Intrusion Detection Systems (IDS): Tarmoqni monitoring qilish va zararli hujumlarni aniqlash.

VPN (Virtual Private Network): Tarmoqni himoya qilish va maxfiylikni saqlash.

Tarmoq tahlili: Tarmoqdagi harakatlarni tahlil qilish va xavf-xatarlarni oldindan aniqlash.

Ilova xavfsizligi — bu dastur va ilovalarning zaifliklaridan foydalangan kiberhujumlardan himoya qilish. Dasturlarni rivojlantirishda xavfsizlikni boshidan boshlash, kodni tekshirish, va zaifliklarni aniqlash juda muhimdir. Ilova xavfsizligini ta'minlash uchun:

Kodni tekshirish: Dasturlarni yaratish jarayonida zaifliklarni aniqlash va ularni tuzatish.

Xavfsiz ma’lumot almashish: Ilovalar va serverlar o‘rtasida xavfsiz va shifrlangan ma'lumot uzatishni ta'minlash.

Identifikatsiya va autentifikatsiya — foydalanuvchilarni tizimga kirishini tasdiqlash va faqat ruxsat etilgan foydalanuvchilarga tizimga kirish imkonini berish. Bu, odatda, parollar, ikki faktorli autentifikatsiya (2FA), biometrik tizimlar (barmoq izi, yuzni tanib olish) orqali amalga oshiriladi.

Kiberxavfsizlik nafaqat texnologiya bilan, balki inson resurslari bilan ham bog‘liq. Xodimlar va foydalanuvchilarga xavfsiz onlayn faoliyat haqida ta'lim berish, phishing xabarlari, zararli havolalar va boshqa tahdidlardan qanday himoyalanishni o‘rgatish juda muhim.

Kiberxavfsizlikni ta'minlash usullari:

Yangi xavfsizlik devorlarini o‘rnatish (Firewalls)

Tarmoqga kirishni nazorat qilish va zararli trafikka qarshi himoya qilish.

Shifrlash (Encryption)

Ma’lumotlarni xavfsiz tarzda saqlash va uzatish uchun shifrlash texnologiyalaridan

foydalanish.

Ikki faktorga autentifikatsiya (2FA)

Foydalanuvchilarning tizimga kirishini qo‘shimcha xavfsizlik qatlamlari yordamida tasdiqlash.

Zahira nusxalari yaratish

Ma’lumotlar yo‘qolgan yoki zarar ko‘rgan holatda ularni tiklash uchun muntazam zahira nusxalarini saqlash.

Xavfsizlik yangilanishlarini muntazam amalga oshirish

Tizimlar va dasturlarni doimiy ravishda yangilab turish va xavfsizlik teshiklarini yopish.

Foydalanuvchilarni ta'limlash

Xavfsizlik bilan bog‘liq qoidalar va amaliyotlarni foydalanuvchilarga o‘rgatish.

Xulosa qilib aytadigan bo‘lsak axborot texnologiyalarining rivojlanishi global xavfsizlikka katta ta’sir ko'rsatmoqda, bu ijobiy va salbiy tomonlarni o'z ichiga oladi. Ularning samarasini ta'minlash uchun xalqaro hamkorlik, ilg'or xavfsizlik tizimlari, innovatsiyalar va qonunchilikni takomillashtirish zarur. Shu bilan birga, yangi xavflar va tahdidlarga qarshi kurashish uchun doimiy ravishda yangi texnologiyalarni ishlab chiqish va global xavfsizlikni himoya qilishga qaratilgan choralar ko'rish lozim. Bunday yondashuv orqali axborot texnologiyalaridan global xavfsizlikni yaxshilash va rivojlantirishda samarali foydalanish mumkin.

Foydalanilgan adabiyotlar:

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W.W. Norton & Company.

Parker, D. B. (2002). *Fighting Computer Crime: A New Framework for Protecting Information*. Wiley.

Cybersecurity & Infrastructure Security Agency (CISA) - https://www.cisa.gov/cybersecurity

Koller, D., & Schmid, M. (2019). *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*. CRC Press.

Gartzke, E. (2014). *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. International Security.

Libicki, M. C. (2007). *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press.

Kaspersky Lab. (2021). *The State of Cybersecurity in the World: Global Cyber Threats and Trends*. Kaspersky Lab Blog.

OWASP (Open Web Application Security Project) - https://owasp.org/

CISA (Cybersecurity and Infrastructure Security Agency) - https://www.cisa.gov/

Krebs on Security - https://krebsonsecurity.com/

SANS Institute - https://www.sans.org/

US-CERT (United States Computer Emergency Readiness Team) - https://us-cert.cisa.gov/