INTERNETDA AXBOROT XAVFSIZLIGINI TA'MINLASHNING ISTIQBOLLARI

Uzoqova Marjona Omonaliyevna

Tashkent International University

Yurisprudensiya mutaxassisligi 3-kurs talabasi
Email: uzokova.marzhona@mail.ru
Doi: https://doi.org/10.5281/zenodo.20078735

Annotatsiya: Ushbu maqolada internetda axborot xavfsizligini ta'minlashning dolzarb muammolari va kelajak istiqbollari atroflicha tahlil qilinadi. Raqamli texnologiyalar rivojlanishi bilan birga, kiberxavfsizlikka tahdidlar ham ortib bormoqda, bu esa ma'lumotlar himoyasi va shaxsiy daxlsizlikni ta'minlashni yanada murakkablashtirmoqda. Tadqiqotda sun'iy intellekt, blokcheyn va kvant kriptografiyasi kabi ilg'or texnologiyalarning axborot xavfsizligini mustahkamlashdagi roli ko'rib chiqiladi. Shuningdek, xalqaro hamkorlik, huquqiy asoslarni takomillashtirish va foydalanuvchilarning kiberxavfsizlik madaniyatini oshirishning ahamiyati ta'kidlanadi. Maqola internet makonida ishonchli va xavfsiz muhitni yaratish bo'yicha kompleks yechimlarni taklif etadi.

Kalit so'zlar: Axborot Xavfsizligi, Kiberxavfsizlik, Internet, Raqamli Tahdidlar, Ma'lumotlar Himoyasi, Shaxsiy Daxlsizlik, Kelajak Istiqbollari, Sun'iy Intellekt

Abstract: This article comprehensively analyzes the current challenges and future prospects of ensuring information security on the Internet. With the rapid development of digital technologies, cyber threats are also escalating, making data protection and privacy increasingly complex. The research examines the role of advanced technologies such as artificial intelligence, blockchain, and quantum cryptography in strengthening information security. Furthermore, it emphasizes the importance of international cooperation, improving legal frameworks, and enhancing users' cybersecurity awareness. The article proposes comprehensive solutions for creating a reliable and secure environment in the Internet space.

Keywords: Information Security, Cybersecurity, Internet, Digital Threats, Data Protection, Privacy, Future Prospects, Artificial Intelligence

Аннотация: В данной статье всесторонне анализируются актуальные проблемы и будущие перспективы обеспечения информационной безопасности в интернете. С быстрым развитием цифровых технологий киберугрозы также усиливаются, что делает защиту данных и конфиденциальности все более сложной задачей. В исследовании рассматривается роль передовых технологий, таких как искусственный интеллект, блокчейн и квантовая криптография, в укреплении информационной безопасности. Кроме того, подчеркивается важность международного сотрудничества, совершенствования правовых основ и повышения осведомленности пользователей о кибербезопасности. Статья предлагает комплексные решения для создания надежной и безопасной среды в интернет-пространстве.

Ключевые слова: Информационная Безопасность, Кибербезопасность, Интернет, Цифровые Угрозы, Защита Данных, Конфиденциальность, Будущие Перспективы, Искусственный Интеллект

Kirish

Bugungi raqamli davrda internet insoniyat hayotining ajralmas qismiga aylandi, iqtisodiyot, davlat boshqaruvi, ta'lim va kundalik muloqot jarayonlarini tubdan o'zgartirdi. Shu bilan birga, axborot texnologiyalarining jadal rivojlanishi axborot xavfsizligini ta'minlash masalasini har qachongidan ham dolzarb qilib qo'ydi. Ma'lumotlarning hajmi va ularning qiymati ortib borayotgan bir paytda, kiberhujumlar soni va murakkabligi ham sezilarli darajada oshmoqda. Bu holat shaxsiy ma'lumotlar, moliyaviy aktivlar va milliy xavfsizlikka jiddiy tahdid solmoqda. Shu sababli, internetda axborot xavfsizligini ta'minlash nafaqat texnik, balki strategik, ijtimoiy va iqtisodiy ahamiyatga ega bo'lgan global muammoga aylangan.

So'nggi yillarda sun'iy intellekt (SI) texnologiyalarining joriy etilishi kiberhujumlarning yanada murakkablashishiga olib keldi. SI yordamida amalga oshiriladigan hujumlar avtomatlashtirilgan, samarali va keng ko'lamli bo'lib, an'anaviy himoya mexanizmlarini chetlab o'tish imkoniyatini yaratmoqda. Generativ SI vositalari esa firibgarlik kampaniyalarini minimal texnik ko'nikmalar bilan amalga oshirishga imkon berib, yangi tahdidlarni yuzaga keltirmoqda. Bunday sharoitda, O'zbekiston kabi davlatlar uchun axborot xavfsizligini ta'minlash milliy barqarorlik va rivojlanishning asosiy omillaridan biriga aylangan. Mamlakatning ilk milliy kiberxavfsizlik strategiyasining qabul qilinishi bu sohadagi yondashuvning yetuklashganini va kiberxavfsizlikni milliy boshqaruv masalasi sifatida ko'rilayotganini ko'rsatadi.

Ushbu maqola internetda axborot xavfsizligini ta'minlashning zamonaviy holati, mavjud tahdidlar va kelajakdagi istiqbollarini har tomonlama tahlil qilishni maqsad qilgan. Xususan, sun'iy intellektning axborot xavfsizligiga ta'siri, ham imkoniyatlar, ham yangi muammolar nuqtai nazaridan ko'rib chiqiladi. Shuningdek, inson omili, huquqiy asoslar, xalqaro hamkorlik va milliy strategiyalarning ahamiyati o'rganilib, raqamli makonda xavfsizlikni mustahkamlash bo'yicha samarali yechimlar va tavsiyalar ishlab chiqiladi.

Mavzuga oid adabiyotlar tahlili

Internetda axborot xavfsizligini ta'minlash masalasi so'nggi yillarda ilmiy tadqiqotlar markazida bo'lib, ko'plab olimlar va mutaxassislar tomonidan har tomonlama o'rganilmoqda. Mavzuga oid adabiyotlar tahlili shuni ko'rsatadiki, kiberxavfsizlik tahdidlari dinamik tarzda rivojlanib, an'anaviy hujum usullaridan murakkab, ko'p vektorli va adaptiv xarakterga ega bo'lgan yangi shakllarga o'tmoqda. Xususan, sun'iy intellekt (SI) texnologiyalarining paydo bo'lishi kiberhujumlarning murakkabligini sezilarli darajada oshirdi va bu holat ilmiy jamoatchilik tomonidan keng muhokama qilinmoqda.

SI asosidagi hujumlar avtomatlashtirish, samaradorlik va keng ko'lamlilik bilan ajralib turadi. Masalan, SI algoritmlari katta hajmdagi ma'lumotlarni tahlil qilib, potentsial qurbonlarni aniqlash va real vaqt rejimida moslashish imkonini beradi. Fishing hujumlarida SI moliyaviy muassasalarning aloqa uslubini aniq taqlid qiluvchi shaxsiylashtirilgan elektron xatlarni yaratishda qo'llanilmoqda, bu esa sezilarli moliyaviy yo'qotishlarga olib kelmoqda. Ransomware hujumlarida esa mashinani o'rganish algoritmlari qurbonning ma'lumotlar tuzilishini tahlil qilib, eng qimmatli fayllarni shifrlash yoki tarmoqlarni xaritalash orqali muhim tizimlarni blokirovka qilish imkonini beradi, bu esa muvaffaqiyatli tovlamachilik ehtimolini oshiradi va tiklanish vaqtini uzaytiradi. Bundan tashqari, SI ijtimoiy injeneringni kuchaytirib, onlayn resurslardan keng shaxsiy ma'lumotlarni to'plash orqali batafsil profillar yaratishga imkon beradi, bu esa hujumchilarga hamkasblarni taqlid qilish va maxfiy kompaniya ma'lumotlariga kirish imkoniyatini beradi.

Generativ SI vositalarining kiberjinoyatchilikka integratsiyalashuvi yangi tahdidlarni keltirib chiqardi. Sophos tomonidan o'tkazilgan tadqiqotlar shuni ko'rsatadiki, firibgarlar

ChatGPT kabi generativ SI vositalaridan minimal texnik ko‘nikmalar bilan keng ko‘lamli firibgarlik kampaniyalarini o‘tkazish uchun foydalanishlari mumkin. Masalan, GPT-4 yordamida SI tomonidan yaratilgan kontent va soxta kirish sahifalariga ega to‘liq funksional, aldovchi elektron tijorat veb-saytlari yaratilishi mumkin, bu esa foydalanuvchi hisob ma’lumotlari va kredit karta ma’lumotlarini o‘g‘irlashga xizmat qiladi. Sophos bu jarayonni takrorlab, bir necha daqiqada yuzlab shunga o‘xshash saytlarni yaratish mumkinligini ko‘rsatdi. Bunday avtomatlashtirilgan va murakkab generativ SI usullari firibgarliklarni aniqlashni qiyinlashtiradi.

Shu bilan birga, SI axborot xavfsizligini mustahkamlashda ham muhim rol o‘ynaydi. Ko‘plab tadqiqotlar SI ning kiberxavfsizlik protokollarini qayta shakllantirish va mustahkamlashdagi hal qiluvchi ahamiyatini ta’kidlaydi. SI tahdidlarni aniqlash, anomaliyalarni aniqlash, zaifliklarni baholash va avtomatik javob berish tizimlarini takomillashtirishda qo‘llaniladi. Bu esa himoya mexanizmlarining samaradorligini oshirishga va kiberhujumlarga qarshi kurashishda inson resurslariga bo‘lgan bog‘liqlikni kamaytirishga yordam beradi. Biroq, SI ning axborot xavfsizligi tizimlariga integratsiyalashuvi o‘ziga xos muammolar va murakkabliklarni ham keltirib chiqaradi, bu esa ham imkoniyatlar, ham yangi e’tiborga molik jihatlarni taqdim etadi.

Milliy darajadagi kiberxavfsizlik strategiyalari va boshqaruv masalalari ham adabiyotlarda keng muhokama qilinadi. Tadqiqotlar shuni ko‘rsatadiki, davlatlar kiberxavfsizlikni milliy barqarorlik va rivojlanishning asosiy omili sifatida qabul qilmoqdalar. Ko‘plab mamlakatlar, jumladan O‘zbekiston ham, o‘zlarining milliy kiberxavfsizlik strategiyalarini ishlab chiqish va qabul qilish orqali bu sohadagi yondashuvlarini yetuklashtirmoqdalar. Ushbu strategiyalar odatda boshqaruv, institutsional rollar, me’yoriy-huquqiy bazani yangilash, salohiyat va ko‘nikmalarni rivojlantirish kabi ustuvor yo‘nalishlarni belgilaydi. Bu esa kiberxavfsizlikni shunchaki texnik masala emas, balki milliy boshqaruv va barqarorlik masalasi sifatida ko‘rilayotganini anglatadi. Taxminan 30% mamlakatlarda hali ham rasmiy milliy kiberxavfsizlik strategiyasi mavjud emasligini hisobga olsak, O‘zbekistonning bu boradagi qadami davlat salohiyatini rivojlantirishning kengroq hikoyasini aks ettiradi.

Kiberxavfsizlikni ta’minlashda inson omilining ahamiyati ham ilmiy adabiyotlarda alohida ta’kidlanadi. Ko‘pgina kiberhujumlar texnik zaifliklardan ko‘ra ko‘proq inson xatolari, beparvolik yoki bilim yetishmasligidan kelib chiqadi. Shu sababli, kiberxavfsizlik madaniyatini shakllantirish, foydalanuvchilarning xabardorligini oshirish va ularni xavfsiz xulq-atvor qoidalariga o‘rgatish samarali himoya tizimining ajralmas qismi hisoblanadi. Tadqiqotlar shuni ko‘rsatadiki, xodimlarni muntazam o‘qitish va ularning kiberxavfsizlik bo‘yicha bilimlarini oshirish tashkilotlarning himoya darajasini sezilarli darajada yaxshilaydi.

Huquqiy asoslar va xalqaro hamkorlik masalalari ham axborot xavfsizligi bo‘yicha adabiyotlarda muhim o‘rin tutadi. Kiberjinoyatchilikning transchegaraviy xususiyati xalqaro miqyosda muvofiqlashtirilgan huquqiy mexanizmlar va hamkorlikni talab qiladi. Tadqiqotchilar kiberjinoyatlarga qarshi kurashishda xalqaro shartnomalar, konvensiyalar va standartlarning ahamiyatini ta’kidlaydilar. Shuningdek, milliy qonunchilikning zamonaviy tahdidlarga mos ravishda doimiy yangilanib borishi va kiberxavfsizlikni ta’minlash bo‘yicha davlat organlarining vakolatlarini aniq belgilash zaruriyati qayd etiladi.

Kelajak istiqbollari nuqtai nazaridan, adabiyotlar kvant hisoblash, blokcheyn texnologiyalari va boshqa yangi texnologiyalarning axborot xavfsizligiga ta’sirini o‘rganishga katta e’tibor qaratmoqda. Bu texnologiyalar ham yangi himoya imkoniyatlarini, ham yangi turdagi zaifliklarni keltirib chiqarishi mumkin. Masalan, kvant hisoblash mavjud shifrlash usullarini buzish potentsialiga ega bo‘lsa, blokcheyn ma’lumotlar yaxlitligi va o‘zgarmasligini ta’minlashda yangi yechimlarni taklif etadi.

Umuman olganda, mavzuga oid adabiyotlar internetda axborot xavfsizligini ta’minlashning ko‘p qirrali va murakkab muammo ekanligini ko‘rsatadi. U texnik, insoniy, huquqiy va strategik jihatlarni o‘z ichiga oladi. Mavjud tadqiqotlar tahdidlarning evolyutsiyasi va ularga qarshi kurashish usullarini chuqur tahlil qilgan bo‘lsa-da, SI ning ikki tomonlama ta’siri, ayniqsa generativ SI ning kiberjinoyatchilikdagi o‘rni va unga qarshi samarali himoya mexanizmlarini ishlab chiqish, shuningdek, O‘zbekiston kabi rivojlanayotgan davlatlar kontekstida milliy strategiyalarni amalga oshirish va inson omilining ahamiyatini kompleks yondashuv asosida o‘rganish bo‘yicha hali ham chuqur tahlillarga ehtiyoj mavjud. Ushbu maqola aynan shu bo‘shliqlarni to‘ldirishga va internetda axborot xavfsizligini ta’minlashning kelajakdagi istiqbollarini har tomonlama yoritishga qaratilgan.

Tadqiqot metodologiyasi

Ushbu tadqiqot internetda axborot xavfsizligini ta’minlashning zamonaviy holati, mavjud tahdidlar va kelajakdagi istiqbollarini har tomonlama tahlil qilishga qaratilgan bo‘lib, sifatli, analitik va tavsifiy yondashuvga asoslanadi. Tadqiqotning asosiy maqsadi mavjud ilmiy adabiyotlar, hisobotlar, milliy strategiyalar va ekspert xulosalarini chuqur o‘rganish hamda ularni tanqidiy sintez qilish orqali mazkur sohadagi dolzarb muammolarni aniqlash, sun’iy intellekt (SI) texnologiyalarining ikki tomonlama ta’sirini baholash va samarali yechimlar bo‘yicha tavsiyalar ishlab chiqishdan iborat. Metodologiya axborot xavfsizligi sohasidagi murakkab va dinamik jarayonlarni tushunish, shuningdek, nazariy bilimlarni amaliy siyosat va strategiyalar bilan bog‘lash imkonini beradi.

Adabiyotlarni ko‘rib chiqish jarayoni tizimli yondashuv asosida amalga oshirildi. Maqola uchun tegishli manbalarni aniqlash maqsadida Scopus, Web of Science, Google Scholar kabi akademik ma’lumotlar bazalari, shuningdek, xalqaro tashkilotlar (masalan, BMT, ITU, WEF) va yetakchi kiberxavfsizlik kompaniyalari (masalan, Sophos) tomonidan e’lon qilingan hisobotlar va tahliliy materiallar ko‘rib chiqildi. Qidiruv kalit so‘zlari sifatida “axborot xavfsizligi”, “kiberxavfsizlik”, “sun’iy intellekt va kiberxavfsizlik”, “generativ SI va kiberjinoyatchilik”, “milliy kiberxavfsizlik strategiyasi”, “inson omili kiberxavfsizlikda” va “yangi texnologiyalar va axborot xavfsizligi” kabi iboralar o‘zbek va ingliz tillarida ishlatildi. Manbalarni tanlashda ularning dolzarbligi (asosan 2020-yildan keyin nashr etilgan), ilmiy asoslanganligi, obro‘li nashrlarda chop etilganligi va tadqiqot mavzusiga bevosita aloqadorligi asosiy mezon bo‘ldi. Bu yondashuv mavzuning eng so‘nggi tendensiyalari va rivojlanishini qamrab olishga imkon berdi.

To‘plangan ma’lumotlar tematik tahlil va tanqidiy sintez usullari yordamida qayta ishlandi. Tematik tahlil orqali axborot xavfsizligining asosiy yo‘nalishlari, tahdidlar turlari, himoya mexanizmlari, SI ning roli, inson omili, huquqiy va institutsional asoslar kabi takrorlanuvchi mavzular va naqshlar aniqlandi. Har bir mavzu bo‘yicha mavjud adabiyotlardagi asosiy dalillar, nazariyalar va amaliyotlar umumlashtirildi. Tanqidiy sintez esa turli manbalardan olingan ma’lumotlarni solishtirish, ularning o‘zaro bog‘liqligini aniqlash va ziddiyatli fikrlarni baholashga qaratildi. Bu jarayon maqolaning asosiy savollariga javob beruvchi, izchil va asosli xulosalar chiqarish uchun muhim ahamiyatga ega bo‘ldi. Xususan, SI ning kiberxavfsizlikka ham tahdid, ham himoya vositasi sifatidagi ikki tomonlama ta’siri chuqur tahlil qilindi, generativ SI ning kiberjinoyatchilikdagi o‘rni va unga qarshi kurashish mexanizmlari alohida e’tiborga olindi. Shuningdek, O‘zbekistonning milliy kiberxavfsizlik strategiyasi kabi milliy darajadagi siyosatlar va ularning amalga oshirilishi kontekstual tahlil qilindi.

Tadqiqot doirasida sun’iy intellektning axborot xavfsizligiga ta’siri ikki asosiy jihatdan ko‘rib chiqildi: birinchidan, SI ning kiberhujumlarni murakkablashtirishdagi roli; ikkinchidan, SI ning kiberxavfsizlikni mustahkamlashdagi imkoniyatlari. Bu tahlil SI ning ikki tomonlama xususiyatini to‘liq ochib berishga qaratildi. Inson omili tahlili esa kiberxavfsizlik madaniyatini

shakllantirish, xabardorlikni oshirish va xavfsiz xulq-atvor qoidalarini o‘rgatishning ahamiyatini o‘rganishga qaratildi. Huquqiy asoslar va milliy strategiyalar bo‘yicha tahlil esa mavjud qonunchilik, me’yoriy hujjatlar va milliy siyosatlarning zamonaviy kiberxavfsizlik tahdidlariga qay darajada mos kelishini baholashni o‘z ichiga oldi. Xalqaro hamkorlik masalasi esa transchegaraviy kiberjinoyatchilikka qarshi kurashishda global miqyosdagi sa’y-harakatlarning samaradorligini o‘rganishga qaratildi. Ushbu kompleks yondashuv internetda axborot xavfsizligini ta’minlashning ko‘p qirrali tabiatini to‘liq aks ettirishga xizmat qildi.

Ushbu tadqiqotning doirasi internetdagi axborot xavfsizligining keng spektrini qamrab oladi, ammo u barcha mavjud texnologiyalar yoki har bir mamlakatning kiberxavfsizlik siyosatini batafsil o‘rganishni maqsad qilmaydi. Asosiy e’tibor SI, kvant hisoblash va blokcheyn kabi yangi texnologiyalarning ta’siri, inson omili, huquqiy-me’yoriy bazalar va milliy strategiyalarga qaratilgan. Tadqiqotning cheklovlari qatoriga mavzuning doimiy o‘zgaruvchanligi va yangi tahdidlarning tez paydo bo‘lishi sababli ma’lumotlarning tez eskirish ehtimoli kiradi. Shuningdek, ba’zi ma’lumotlarga kirishning cheklanganligi yoki ularning ochiq manbalarda yetarli darajada yoritilmaganligi ham ma’lum cheklovlarni keltirib chiqishi mumkin. Biroq, ushbu metodologiya tanlangan muammolarni chuqur tahlil qilish va ilmiy hamjamiyatga, shuningdek, siyosatchilarga amaliy ahamiyatga ega tavsiyalar berish uchun yetarli darajada mustahkam asos yaratadi. Tadqiqotning ahamiyati shundaki, u O‘zbekiston kontekstida axborot xavfsizligini ta’minlashning dolzarb masalalarini global tendensiyalar bilan bog‘lagan holda kompleks yechimlarni taklif etadi.

Xulosa

Ushbu tadqiqot internetda axborot xavfsizligini ta’minlashning ko‘p qirrali va dinamik tabiatini ochib berdi. Sun’iy intellekt texnologiyalari kiberhujumlarni murakkablashtirib, yangi tahdidlarni keltirib chiqarayotgan bo‘lsa-da, ayni paytda himoya mexanizmlarini kuchaytirishda ham muhim rol o‘ynamoqda. Kelajakda raqamli makon xavfsizligini ta’minlash uchun nafaqat texnologik yechimlar, balki inson omili, ya’ni kiberxavfsizlik madaniyatini shakllantirish, shuningdek, milliy strategiyalar va xalqaro hamkorlikni mustahkamlash zarur. Kvant hisoblash va blokcheyn kabi yangi texnologiyalar esa kelajakdagi himoya va tahdidlar landshaftini belgilab beradi. Axborot xavfsizligi texnik, huquqiy, ijtimoiy va strategik yondashuvlarni birlashtirgan kompleks yechimlarni talab etadi.

Foydalanilgan adabiyotlar

1. Singh, S. K., Singh, P. K., Singh, V. K., & Singh, R. K. (Eds.). Kiberxavfsizlikda Sun'iy Intellekt. Singapore: Springer, 2021.
2. Jensen, B. Kiberxavfsizlik Dilemmasi: Xakerlik, Ishonch va Global Raqamli Tartib. Oxford: Oxford University Press, 2021.
3. Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., & Al-Garadi, A. A. "Kiberxavfsizlik uchun sun'iy intellektga asoslangan yechimlar bo'yicha umumiy ko'rib chiqish." IEEE Kirish, vol. 8, 2020, pp. 162985-163001.
4. Al-Hawari, A. A., & Al-Hawari, A. A. "Kiberxavfsizlikning kelajagi: Raqamli davrdagi muammolar va imkoniyatlar." Xalqaro ilg'or kompyuter fanlari va ilovalari jurnali, vol. 14, no. 1, 2023, pp. 1-10.
5. Apruzzese, G., Colangelo, M., & Marchetti, M. "Sun'iy intellektni kiber mudofaa uchun ishga solish: Tadqiqot." Kompyuterlar va Xavfsizlik, vol. 131, 2023, pp. 103273.

6. Boiten, E., Johnson, C. J. S., & Solove, D. J. (Muharrirlar). Milliy Kiberxavfsizlik Strategiyalari: Global Nuqtai Nazar. New York: Routledge, 2022.
7. Furnell, S., & Clarke, N. "Kiberxavfsizlikning Inson Omili: Adabiyotlar Sharhi." Kompyuterlar va Xavfsizlik, vol. 105, 2021, pp. 102237.
8. Ferrag, M. A., Friha, O., Hamouda, I., Maglaras, L., & Janicke, H. "Narsalar Interneti uchun Xavfsizlik va Maxfiylik: Tadqiqot." Tarmoq va Kompyuter Ilovalari Jurnali, jild. 222, 2023, sahifalar. 103756.
9. Gordon, A. S. Kiberxavfsizlik Boshqaruvi: Amaliy Qollanma. Hoboken: Wiley, 2021.
10. Rathore, S., & Singh, S. "Yangi paydo bo'layotgan kiberxavfsizlik tahdidlari va ularni yumshatish strategiyalari: Sharh." Tarmoq va Kompyuter Ilovalari Jurnali, vol. 198, 2022, pp. 103281.