O‘ZBEKISTON RESPUBLIKASI

OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

FARG‘ONA DAVLAT UNIVERSITETI

FarDU. ILMIY XABARLAR-

1995-yildan nashr etiladi
Yilda 6 marta chiqadi

1-2025

IJTIMOIY FANLAR

НАУЧНЫЙ ВЕСТНИК. ФерГУ

Издаётся с 1995 года
Выходит 6 раз в год

MUNDARIJA

FALSAFA

SIYOSAT

FarDU. Ilmiy xabarlar – Scientific journal of the Fergana State University

Volume 31 Issue 1, 2025-yil DOI: 10.56292/SJFSU/vol31_iss1/a57

UO‘K: 004.056:351.75

KIBERXAVFSIZLIKNING DAVLAT SIYOSAT DARAJASIGA KO‘TARILISHI: ZAMONAVIY TAHDIDLAR VA STRATEGIYALAR

ПОВЫШЕНИЕ КИБЕРБЕЗОПАСНОСТИ ДО ГОСУДАРСТВЕННОЙ ПОЛИТИКИ: СОВРЕМЕННЫЕ УГРОЗЫ И СТРАТЕГИИ

RAISING CYBERSECURITY TO THE LEVEL OF STATE POLICY: MODERN THREATS AND STRATEGIES

Shokirov Boburjon Tohirjon o‘g‘li
Farg‘ona davlat universiteti, yurisprudensiya yo‘nalishi talabasi

Annotatsiya

Raqamli asrda kiberxavfsizlik nafaqat texnik masala, balki milliy xavfsizlikning muhim jihatiga aylanib bormoqda. Har yili kiberhujumlarning soni ortib, ularning iqtisodiy va ijtimoiy oqibatlari ham jiddiylashib bormoqda. Ushbu maqolada kiberxavfsizlikning davlat siyosati darajasiga ko‘tarilishining zarurligi, zamonaviy tahdidlar va ularning turlari, jumladan ransomware hujumlari, sun’iy intellekt asosida avtomatlashtirilgan tajovuzlar va ta’minot zanjiri xavfsizligiga doir masalalar atroflicha ko‘rib chiqiladi. Shuningdek, Zero Trust arxitekturasi, sun’iy intellekt va mashinali o‘rganish vositalaridan foydalanish kabi zamonaviy strategik yondashuvlar tahlil qilinib, ularning samaradorligi baholanadi. Maqolada xalqaro tajribalar bilan bir qatorda milliy kiberxavfsizlik siyosatining shakllanish bosqichlari va amaliyotdagi kamchiliklar ham yoritib berilgan. Fuqarolar, xususiy sektor va davlat tashkilotlari o‘rtasida o‘zaro hamkorlik, texnologik rivojlanish va samarali siyosat orqali barqaror kiberxavfsizlik tizimini yaratish zarurligi asosiy e’tiborda bo‘lgan. Ushbu tadqiqot orqali mamlakatlar kiberxavfsizlik tahdidlariga qarshi tizimli yondashuvlar ishlab chiqishda nazariy va amaliy asos yaratishga harakat qilinadi.

Аннотация

В эпоху цифровых технологий кибербезопасность становится не просто технической проблемой, а важным аспектом национальной безопасности. С каждым годом количество кибератак увеличивается, а их экономические и социальные последствия становятся все серьезнее. В этой статье более подробно рассматривается необходимость поднять кибербезопасность на уровень государственной политики, современные угрозы и их типы, включая атаки программ-вымогателей, автоматизированные атаки на основе искусственного интеллекта и проблемы безопасности цепочки поставок. Также анализируются современные стратегические подходы, такие как архитектура Zero Trust, использование искусственного интеллекта и машинного обучения, и оценивается их эффективность. Помимо международного опыта, в статье освещены этапы формирования национальной политики кибербезопасности и недостатки на практике. Основное внимание было уделено необходимости создания устойчивой системы кибербезопасности посредством сотрудничества между гражданами, частным сектором и государственными организациями, технологического развития и эффективной политики. Целью данного исследования является создание теоретической и практической основы для разработки странами систематических подходов к угрозам кибербезопасности.

Abstract

In the digital age, cybersecurity is becoming not only a technical issue, but also an important aspect of national security. The number of cyberattacks is increasing every year, and their economic and social consequences are becoming more serious. This article examines in detail the need to elevate cybersecurity to the level of state policy, modern threats and their types, including ransomware attacks, automated attacks based on artificial intelligence, and issues related to supply chain security. It also analyzes modern strategic approaches such as Zero Trust architecture, the use of artificial intelligence and machine learning tools, and evaluates their effectiveness. The article, along with international experience, highlights the stages of formation of national cybersecurity policies and shortcomings in practice. The main focus is on the need to create a sustainable cybersecurity system through cooperation between citizens, the private sector, and government organizations, technological development, and effective policies. This study attempts to create a theoretical and practical basis for developing systematic approaches to cybersecurity threats in countries.

Kalit so‘zlar: *Internet, ransomware, ijtimoiy tarmoq, shaxsiy ma’lumotlar, sun’iy intellekt, veb-sayt, antivirus, elektron pochta, kiberxavfsizlik.*

Ключевые слова: *Интернет, программы-вымогатели, социальная сеть, персональные данные, искусственный интеллект, веб-сайт, антивирус, электронная почта, кибербезопасность.*

Keywords: *Internet, ransomware, social network, personal data, artificial intelligence, website, antivirus, email, cybersecurity.*

KIRISH

Bugungi kunda raqamli texnologiyalar nafaqat har bir shaxsning kundalik hayotida, balki, davlat organlari va mansabdor shaxslar ish faoliyatining ham ajralmas qismiga aylangan. Bu haqida Smith shunday deydi: “Kompyuterlar, smartfonlar va internet orqali biz nafaqat muloqot qilamiz, balki iqtisodiy, ijtimoiy va siyosiy faoliyatlarimizni ham amalga oshiramiz. Ammo bunday texnologik rivojlanish kiberxavfsizlik tahdidlarini ham o‘z navbatida kuchaytirib yubordi. Kiberxavfsizlik davlat siyosatining ajralmas qismiga aylanishi zarur, chunki kiberhujumlar davlatlar, korxonalar va fuqarolarning xavfsizligiga tahdid soladi”[8]. Raqamli asrda kiberxavfsizlik endi nafaqat texnik masala, balki tashkilotning mustahkamligi va milliy xavfsizlikning asosiy jihati hisoblanadi. Kibertahdidlarning tobora takomillashib borishi korxonalar, hukumatlar va jismoniy shaxslarni doimiy ravishda moslashishga majbur qilib, jiddiy muammo tug‘dirmoqda. Biz kompyuterlar, smartfonlar, ijtimoiy tarmoqlar va boshqa raqamli qurilmalardan kundalik hayotimizda, ish faoliyatimiz va ta’lim jarayonlarida keng foydalanamiz. Shuningdek, bu texnologiyalar bizning shaxsiy ma’lumotlarimiz va iqtisodiy resurslarimizni himoya qilishda katta mas’uliyat yuklaydi. Kiberxavfsizlik bu sohada juda muhim rol o‘ynaydi. O‘zbekiston Respublikasi “Kiberxavfsizlk to‘g‘risida” gi qonuninida ushbu soha davlat siyosati darajasiga ko‘tarilganligi va va unda belgilab qo‘yilgan kiberxavfsizlikni ta’minlashning asosiy prinsiplari haqida qonunda shunday deyilgan:

“Kiberxavfsizlikni ta’minlashning asosiy prinsiplari quyidagilardan iborat:

- qonuniylik;
- kibermakonda shaxs, jamiyat va davlat manfaatlarini himoya qilishning ustuvorligi;
- kiberxavfsizlik sohasini tartibga solishga nisbatan yagona yondashuv;
- kiberxavfsizlik tizimini yaratishda mahalliy ishlab chiqaruvchilar ishtirokining ustuvorligi;
- O‘zbekiston Respublikasining kiberxavfsizlikni ta’minlashda xalqaro hamkorlik uchun ochiqligi” [5]

O‘z o‘rnida I.M.Karimov axborot xavfsizligi va undagi davlat siyosati to‘g‘risida shunday ma’lumot beradi: “Axborot xavfsizligi – ko‘p qirrali faoliyat sohasi bo‘lib, unga faqat tizimli, kompleks yondashuv muvaffaqiyat keltirishi mumkin. Ushbu muammoni hal etish uchun huquqiy, ma’muriy, protsedurali va dasturiy-texnik choralar qo‘llaniladi. Davlatning axborot xavfsizligini ta’minlash muammosi milliy xavfsizlikni ta'minlashning asosiy va ajralmas qismi bo‘lib, axborotni muhofaza qilish esa davlatning birlamchi masalalariga, davlat siyosati darajasiga aylanmoqda” [2].

ADABIYOTLAR TAHLILI VA METODLAR

Kiberxavfsizlik bo‘yicha so‘nggi yillardagi ilmiy va amaliy tadqiqotlar mazkur mavzuning dolzarbligini yaqqol namoyon etadi. Smith[8] o‘z tadqiqotida ransomware hujumlarining davlat infratuzilmasiga ta’sirini yoritgan bo‘lsa, Brown “Zero Trust arxitekturasining samaradorligini ko‘rsatgan. Zero Trust modeli kiberxavfsizlikni mustahkamlashda dolzarb bo‘lib, har bir foydalanuvchi va qurilma uchun doimiy autentifikatsiyani talab qiladi.” [3] Aliyev sun’iy intellekt (AI) va mashinali o‘rganish (ML) vositalarining ikki tomonlama ta’sirini tahlil qiladi. Unga ko‘ra, AI bir tomondan kiber tahdidlarni aniqlash va himoyani mustahkamlashda qo‘llanilsa, boshqa tomondan, hujumlarni avtomatlashtirishda xavfli vosita sifatida ishlatilmoqda [1]. SolarWinds (2020) kabi “ta’minot zanjiri hujumlari bu yo‘nalishda xavfsizlik choralarini kuchaytirish zarurligini ko‘rsatadi.”[9].

Metodologiya sifatida maqolada sifatli adabiy tahlil, statistik ma’lumotlar va holat tahlilidan foydalanilgan. Asosiy ma’lumotlar xalqaro ilmiy maqolalar, tahliliy hisobotlar va kiberxavfsizlik tashkilotlarining rasmiy manbalaridan olindi. Jumladan, O‘zbekistonning Kiberxavfsizlik markazi (2021) hisobotlari mahalliy tajribalarni o‘rganishda asos bo‘lib xizmat qildi[10]. Shuningdek, metodologiya qismida taqqoslash usuli ham qo‘llanilgan bo‘lib, xalqaro tajribalar O‘zbekistonning kiberxavfsizlik strategiyasi hamda, amaldagi davlat siyosati bilan solishtirildi. Bunday yondashuv tahdidlarning o‘ziga xos jihatlarini aniqlash va milliy strategiyani takomillashtirishda muhim vosita hisoblanadi.

MUHOKAMA VA NATIJALAR

Ransomware hujumlari so‘nggi yillarda eng keng tarqalgan kiberxavfsizlik muammolaridan biriga aylandi. Ushbu zararli dasturlar qurbonning ma’lumotlarini shifrlab, ularni qaytarish uchun to‘lov talab qiladi. "Ikki marta tovlamachilik" taktikasi keng tarqaldi. Tajovuzkorlar ma’lumotlarni shifrlash bilan birga, to‘lov to‘lanmasa, maxfiy ma'lumotlarni ommaga oshkor qilish bilan tahdid qilishadi

Zamonaviy tahdidlar haqida Aliyev shunday ma'lumot beradi: "Sun'iy intellekt (AI) va mashinali o'rganish (ML) kiberxavfsizlik sohasida ikki tomonlama rol o'ynamoqda. Bir tomondan, AI tahdidlarni aniqlash va xavfli harakatlarga qarshi samarali choralar ko'rish uchun ishlatilmoqda. Ammo boshqa tomondan, AI kiber jinoyatchilar tomonidan ham keng qo'llanilmoqda. Murakkab fishing elektron pochta xabarlari, zararli dasturlarni avtomatlashtirish kabi hujumlar AI orqali yanada samarali va xavfli bo'lib bormoqda" [1]. Dastlab ushbu atamalar mazmuniga to'xtalib o'tsak, sun'iy intellekt (AI) - bu kompyuterlar va raqamli qurilmalarga o'rganish, o'qish, yozish, yaratish va tahlil qilish imkonini beruvchi texnologiya, Machine Learning esa inglizchadan tarjima qilinganda, "Mashinani o'rganish" - bu sun'iy intellektning (AI) kichik to'plami bo'lib, u ma'lumotlarni o'rganadigan va vaqt o'tishi bilan ularning aniqligini yaxshilaydigan dastur. Bir tomondan, ular tahdidni aniqlash va javob berish uchun ilg'or vositalarni taklif qilishadi. Boshqa tomondan, ular hujumlarini kuchaytirish uchun kiber jinoyatchilar tomonidan ham qo'llanilmoqda. AI tomonidan boshqariladigan tahdidlar murakkab fishing elektron pochta xabarlarini yaratish yoki tizimlardagi zaifliklarni misli ko'rilmagan tezlikda aniqlash kabi hujumlarni avtomatlashtirishi va kuchaytirishi mumkin. Masalan, AI algoritmlari individual maqsadlarga moslashtirilgan ishonchli nayza-fishing xabarlarini yaratishi mumkin, bu esa muvaffaqiyatli buzilish ehtimolini oshiradi. Ta'minot zanjiri hujumlari tashkilotlar uchun muhim zaiflik sifatida paydo bo'ldi. Ushbu hujumlar asosiy maqsad "tarmog'iga kirish uchun uchinchi tomon sotuvchilari yoki xizmat ko'rsatuvchi provayderlarning zaif tomonlariga qaratilgan. 2020-yilgi SolarWinds voqeasi kabi ta'minot zanjiri hujumlari yirik tashkilotlarga katta zarar yetkazmoqda" [9]. Bunday hujumlarda xakerlar uchinchi tomon dasturiy ta'minoti orqali asosiy tizimlarga kirishga erishadilar.

Kibertahdidlarning o'sib borayotgan murakkabligiga javoban, ko'plab tashkilotlar Zero Trust Architecture (ZTA) ni qabul qilmoqdalar. Brown Zero Trust modeli haqida shunday deydi: "ZTA – "hech qachon ishonmang, doim tekshiring" tamoyiliga asoslanadi. Bu strategiya foydalanuvchilar, qurilmalar va ilovalardan qat'i nazar, doimiy autentifikatsiya va nazoratni talab qiladi. Zero Trust arxitekturasi lateral harakatlanish xavfini kamaytirib, tashqi va ichki tahdidlardan himoya qilishni ta'minlaydi" [3].

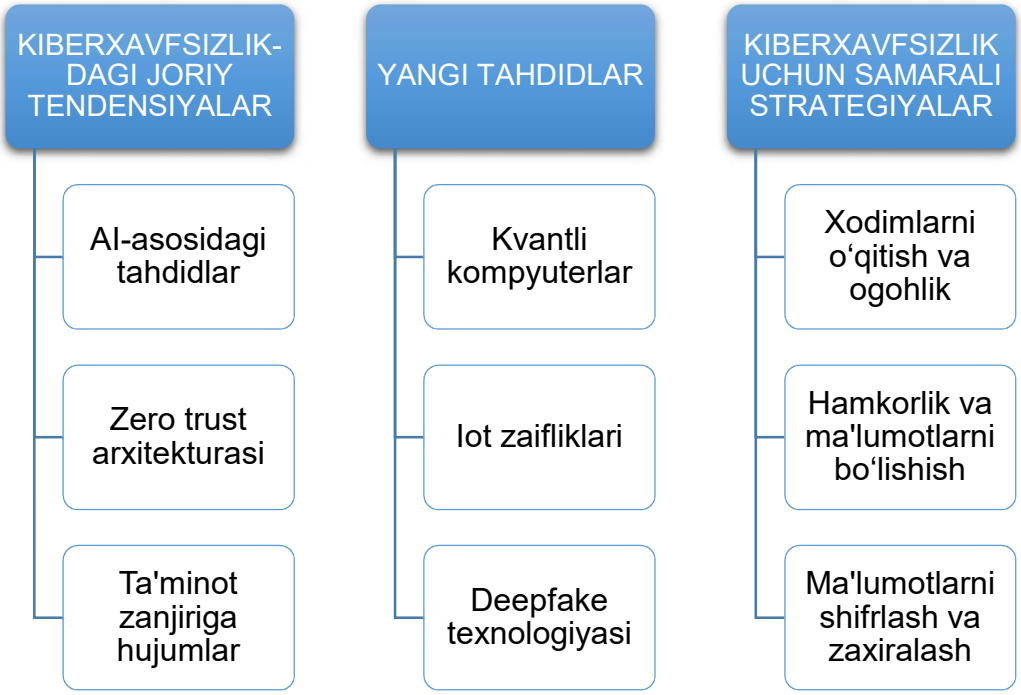
Narsalar Interneti (IoT – Internet of things) qurilmalarining ko'payishi kiberxavfsizlik landshaftiga yangi zaifliklarni kiritadi. Bu haqida Smith shunday deydi: "Narsalar Interneti (IoT) qurilmalarining ko'payishi yangi kiberxavfsizlik muammolarini keltirib chiqarmoqda. Ko'plab IoT qurilmalari kuchli xavfsizlik mexanizmlariga ega emas, bu esa ularni kiberjinoyatchilar uchun oson nishonga aylantiradi. Bunga qarshi kuchli autentifikatsiya, dasturiy ta'minotni yangilash va tarmoq segmentatsiyasi kabi choralar ko'rish zarur"[8]. Haqiqiy, ammo soxta audio va video kontent yaratish uchun sun'iy intellektdan foydalanadigan Deepfake texnologiyasi kiberxavfsizlik va axborot yaxlitligiga jiddiy tahdid soladi. Deepfakes noto'g'ri ma'lumot tarqatish, firibgarlik qilish va jamoatchilik fikrini manipulyatsiya qilish uchun ishlatilishi mumkin. Deepfakes bilan kurashish ko'p qirrali yondashuvni, jumladan, aniqlash vositalarini ishlab chiqish, jamoatchilikni xabardor qilish kampaniyalarini o'tkazish va ushbu texnologiyadan noto'g'ri foydalanishni bartaraf etish uchun huquqiy asoslarni amalga oshirishni talab qilmoqda.

Hozirgi davrda inson xatosi kiberxavfsizlikdagi eng muhim zaifliklardan biri bo'lib qolmoqda. Doimiy o'qitish va xabardorlik dasturlari xodimlarni fishing hujumlari, ijtimoiy muhandislik taktikasi va xavfsizlikni ta'minlashning ilg'or amaliyotlari haqida o'rgatish uchun zarurdir. Simulyatsiya qilingan fishing mashqlari va interaktiv treninglar xodimlarga potentsial tahdidlarni aniqlash va ularga nisbatan samaraliroq javob berishga yordam beradi. Tashkilot ichida xavfsizlikni anglaydigan madaniyatni rivojlantirish xavflarni minimallashtirish uchun juda muhimdir. Kiberhujumlar ta'sirini boshqarish va yumshatish uchun kuchli hodisalarga javob berish rejasini ishlab chiqish va qo'llab-quvvatlash zarur. Hodisalarga qarshi samarali chora-tadbirlar rejasi xavfsizlik hodisalarini aniqlash, bartaraf etish, yo'q qilish va qayta tiklash tartib-qoidalarini ko'rsatishi kerak. Hodisalarga javob berish rejasini muntazam ravishda sinovdan o'tkazish va yangilash uning samarali bo'lishini va barcha manfaatdor tomonlarning mumkin bo'lgan buzilishlarni bartaraf etishga tayyorligini ta'minlaydi. Stol usti mashqlari va simulyatsiya mashqlarini o'tkazish javob jarayonini takomillashtirish va umumiy tayyorgarlikni yaxshilashga yordam beradi.

Maxfiy ma'lumotlarni shifrlash va muntazam zaxira nusxalarini saqlash axborotni himoya qilish va biznes uzluksizligini ta'minlashning asosiy amaliyotidir. Shifrlash ma'lumotlarni dam olishda ham, tranzitda ham himoya qiladi, bu esa ruxsatsiz shaxslarga kamroq kirish imkonini beradi. Zaxira tizimlarini muntazam ravishda yangilash va sinovdan o'tkazish to'lov dasturi hujumi yoki boshqa

ma’lumotlar yo‘qolishi holatlarida muhim ma’lumotlarni qayta tiklashni ta’minlaydi. Ma’lumotlarni himoya qilishda ko‘p qatlamli yondashuvni amalga oshirish umumiy xavfsizlikni oshiradi. Tashkilotlar, sanoat guruhlari va davlat idoralari o‘rtasida hamkorlik va axborot almashish paydo bo‘layotgan tahdidlar va ilg‘or tajribalar haqida xabardor bo‘lish uchun muhim ahamiyatga ega. Tahdidlar haqida ma'lumot almashish platformalarida va kiberxavfsizlik forumlarida ishtirok etish qimmatli tushunchalarni taqdim etishi va jamoaviy mudofaa sa’y-harakatlarini kuchaytirishi mumkin. Davlat-xususiy sheriklik bilan shug‘ullanish va sanoat miqyosidagi tashabbuslarga hissa qo‘shish umumiy muammolarni hal qilish va umumiy kiberxavfsizlik barqarorligini oshirishga yordam beradi.

Quyidagi diagrammada ushbu maqolaning mazmuni va unda aytib o‘tilgan asosiy tushunchalar keltirib o‘tilgan.



1 – diagramma

XULOSA

Kiberxavfsizlikning davlat siyosati darajasiga ko‘tarilishi zamonaviy dunyoning ajralmas zaruriyatiga aylanib bormoqda. Raqamli texnologiyalar rivojlanishi bilan birga, kiberxavfsizlik tahdidlarining murakkabligi va ko‘lami keskin oshib borayotgani kuzatilmoqda. Jumladan, ransomware hujumlari, sun’iy intellekt asosida avtomatlashtirilgan kiberhujumlar va IoT qurilmalaridagi zaifliklar nafaqat davlat infratuzilmasiga, balki korporativ tarmoqlar va xususiy foydalanuvchilarga ham jiddiy tahdid tug'dirmoqda. Kiberxavfsizlik strategiyasini ishlab chiqishda Zero Trust arxitekturasi, mashinali o‘rganish (ML) va sun’iy intellekt (AI) kabi zamonaviy texnologiyalardan samarali foydalanish dolzarb ahamiyat kasb etadi. “Zero Trust yondashuvi har bir foydalanuvchi va qurilma uchun doimiy tekshirishni ta’minlab, ichki va tashqi tahdidlardan himoya qilish imkonini beradi. Ta’minot zanjiri hujumlari kabi yangi tahdidlar kompaniya va tashkilotlarning xavfsizlik siyosatini kuchaytirishni talab qiladi. SolarWinds voqeasi misolida ko‘rsatilganidek, uchinchi tomon dasturlarining zaifliklari tizimlarning keng miqyosda buzilishiga olib keladi” [9]. Shu bois, yetkazib beruvchilarni doimiy nazorat qilish, xavfsizlik monitoringi va kuchli siyosatni ishlab chiqish zarur. IoT qurilmalari xavfsizligi ham bugungi kunning asosiy masalalaridan biri bo‘lib, kuchli autentifikatsiya, dasturiy ta’minot yangilanishlari va tarmoq segmentatsiyasi kabi chora-tadbirlar orqali ularning himoyasini ta'minlash lozim.

Kiberxavfsizlik strategiyalarini muvaffaqiyatli amalga oshirish uchun davlat, xususiy sektor va fuqarolik jamiyati o‘rtasidagi hamkorlik muhim ahamiyatga ega. Xalqaro tajribalarni o‘rganish va ularni milliy siyosatga integratsiya qilish orqali barqaror va xavfsiz kiber ekotizim yaratish mumkin. Ushbu maqola milliy kiberxavfsizlik strategiyasini takomillashtirish va zamonaviy tahdidlarga qarshi samarali yechimlarni ishlab chiqishga nazariy va amaliy asos yaratishni maqsad qilgan. davlat siyosati darajasiga ko‘tarilishi zamonaviy tahdidlarga qarshi kurashda muhim ahamiyat kasb etadi.

Ransomware hujumlarining o‘sishi, sun’iy intellekt yordamida murakkablashtirilgan hujumlar va IoT qurilmalarining zaifligi bu sohada samarali strategiyalar ishlab chiqishni talab qiladi. Zero Trust modeli, AI va ML asosida tahdidlarni aniqlash, ta’minot zanjirlarini mustahkamlash kabi yondashuvlar kiberxavfsizlikni ta'minlashda asosiy vosita hisoblanadi. Davlat, xususiy sektor va jamiyat o‘rtasidagi hamkorlik, samarali siyosat va yangi texnologiyalarni qo‘llash kiberxavfsizlikning barqarorligini ta’minlash uchun zarurdir. Ushbu maqola kelgusida milliy kiberxavfsizlik strategiyasini shakllantirish va zamonaviy tahdidlarga qarshi tizimli choralarni ishlab chiqishda nazariy va amaliy asos bo‘lib xizmat qiladi.

ADABIYOTLAR RO‘YXATI

1. Aliyev, S. (2021). Sun’iy intellekt va uning kiberxavfsizlikdagi roli. Toshkent: Ma'naviyat Press.
2. Axborot xavfsizligi asoslari: Darslik / I. M. Karimov, N. A. Turgunov. T.: O‘zbekiston Respublikasi IIV Akademiyasi, 2016.
3. Brown, L. (2019). Zero trust networks: principles and practices. London: Cybertech Publications.
4. GDPR. (2018). General Data Protection Regulation. European Union.
5. https://lex.uz/uz/docs/-5960604 - O‘zbekiston Respublikasi “Kiberxavfsizlk to‘g‘risida” gi qonunini.
6. National cybersecurity center. (2020). Cybersecurity trends and solutions. Washington, DC.
7. O‘zbekiston Respublikasining Konstitutsiyasi.
8. Smith, J. (2020). Cybersecurity threats in the digital age. New York: Tech Press.
9. SolarWinds hisoboti (2020). Cybersecurity Breaches in Supply Chains. Tech Industry Journal.
10. O‘zbekiston kiberxavfsizlik markazi hisoboti (2021). Kiberxavfsizlik holati va strategiyalari. Toshkent.