

KIBERJINOYATLAR VA KIBERXAVFSIZLIKNING XALQARO MAYDONDAGI O'RNINI VA OLDINI OLIISH TENDENSIYALARI**Raximova Azizaxon Anvar qizi**

Toshkent davlat yuridik universiteti

Xalqaro huquq va qiyosiy huquqshunoslik fakulteti talabasi.

rahimovaazizaxon12@gmail.com<https://doi.org/10.5281/zenodo.23457096>

Annotatsiya. Mazkur maqolada kiberjinoiyatlar va kiberxavfsizlikning xalqaro maydondagi o'rnini, zamonaviy tahdidlar, ularning davlatlar, xalqaro tashkilotlar va jamiyat hayotiga ta'siri hamda ushbu tahdidlarning oldini olish bo'yicha shakllanayotgan tendensiyalar tahlil qilinadi. Maqolada kiberjinoiyatlarning rivojlanish dinamikasi, xalqaro huquqiy mexanizmlar, davlatlararo hamkorlikning ahamiyati va kiberxavfsizlikni ta'minlashning istiqbolli yo'nalishlari yoritilgan. Shuningdek, xalqaro huquqiy hujjatlar, jumladan, Budapesht konvensiyasi va BMTning tegishli rezolyutsiyalari o'rganildi. Tadqiqot natijalari shuni ko'rsatadiki, sun'iy intellekt, bulutli texnologiyalar va raqamli iqtisodiyotning rivojlanishi bilan kiberxavfsizlik masalalari global xavfsizlikning ajralmas qismiga aylangan. Mazkur maqolaning maqsadi kiberjinoiyatlar va kiberxavfsizlikning xalqaro maydondagi ahamiyatini o'rganish, mavjud huquqiy mexanizmlarni tahlil qilish hamda kiberjinoiyatlarning oldini olish bo'yicha zamonaviy tendensiyalarni aniqlashdan iborat.

Kalit so'zlar: kiberjinoiyat, kiberxavfsizlik, xalqaro huquq, Budapesht konvensiyasi, sun'iy intellekt, raqamli xavfsizlik, xalqaro hamkorlik.

INTRODUCTION

XXI asrda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi insoniyat uchun mislsiz imkoniyatlar yaratdi. Internet, sun'iy intellekt, bulutli hisoblash tizimlari va raqamli iqtisodiyotning keng tarqalishi davlat boshqaruvi, biznes, ta'lim va kundalik hayotning ajralmas qismiga aylandi. Shu bilan birga, texnologik taraqqiyot yangi turdagi tahdidlarni ham yuzaga keltirdi. Xususan, kiberjinoiyatlar bugungi kunda xalqaro xavfsizlikka tahdid solayotgan eng dolzarb muammolardan biri hisoblanadi.

Kiberjinoiyat deganda kompyuter tizimlari, tarmoqlar yoki elektron ma'lumotlarga qarshi qaratilgan noqonuniy harakatlar tushuniladi. Bunga noqonuniy kirish, ma'lumotlarni o'g'irlash, moliyaviy firibgarlik, zararli dasturlar tarqatish, shaxsiy ma'lumotlarni noqonuniy yig'ish va kiberterrorizm kabi harakatlar kiradi.

Globalashuv sharoitida kiberjinoiyatlar milliy chegaralarni tan olmaydi. Bir davlat hududida sodir etilgan hujum bir vaqtning o'zida boshqa qit'adagi minglab foydalanuvchilarga zarar yetkazishi mumkin. Shu sababli kiberxavfsizlik masalasi nafaqat milliy, balki xalqaro xavfsizlikning ham muhim elementi sifatida qaralmoqda. So'nggi yillarda davlat muassasalari, banklar, sog'liqni saqlash tizimlari va strategik infratuzilmalarga qilingan kiberhujumlar sonining ortishi ushbu muammoning naqadar jiddiy ekanligini ko'rsatmoqda. Ayniqsa, tovlamachilik dasturlari (ransomware, phishing), DDoS hujumlari va sun'iy intellekt yordamida amalga oshirilayotgan murakkab kiberjinoiyatlar yangi xavfsizlik choralarni ishlabchiqishni talab qilmoqda.

METHODS

Tadqiqot davomida qiyosiy-huquqiy, statistik, tizimli va mantiqiy tahlil usullaridan foydalanildi.

Qiyosiy-huquqiy metod yordamida turli davlatlarning kiberxavfsizlik sohasidagi qonunchilik tajribalari o'rganildi. Xususan, Yevropa Ittifoqi, Amerika Qo'shma Shtatlari, Buyuk Britaniya va Osiyo mamlakatlarining normativ-huquqiy hujjatlari tahlil qilindi. Statistika metod orqali xalqaro tashkilotlar tomonidan e'lon qilingan kiberjinoyatlar bo'yicha ma'lumotlar o'rganildi. Ushbu ma'lumotlar kiberjinoyatlarning o'sish dinamikasini va ularning iqtisodiy oqibatlarini baholash imkonini berdi. Tizimli yondashuv asosida kiberxavfsizlikning texnika, huquqiy va institutsional jihatlari kompleks ravishda tahlil qilindi. Shuningdek, xalqaro huquqiy hujjatlar, jumladan, Budapesht konvensiyasi va BMTning tegishli rezolyutsiyalari o'rganildi.

Mantiqiy-huquqiy metod yordamida kiberjinoyatlar bilan kurashishning zamonaviy tendensiyalari va istiqboldagi rivojlanish yo'nalishlari yuzasidan ilmiy xulosalar shakllantirildi.

RESULTS

Tadqiqot natijalari kiberjinoyatlar soni va murakkabligi yil sayin ortib borayotganligini ko'rsatdi. Raqamli iqtisodiyotning rivojlanishi bilan birga yangi tahdidlar ham yuzaga kelmoqda.

Bugungi kunda eng ko'p uchraydigan kiberjinoyatlar foydalanuvchilarning shaxsiy ma'lumotlarini aldov yo'li bilan qo'lga kiritish (Phishing), ma'lumotlarni bloklab, ularni tiklash evaziga pul talab qilish (Ransomware), server va tarmoqlar faoliyatini izdan chiqarish (Ddos hujumlari), shaxsni identifikatsiya qiluvchi ma'lumotlarni o'g'irlash (Identity theft), davlat yoki korporativ sirlarni noqonuniy qo'lga kiritish (kiberjosuslik), kiberterrorizm kabilari hisoblanadi.

Tahlillar shuni ko'rsatadiki, kiberjinoyatlar tufayli jahon iqtisodiyoti har yili trillionlab dollar zarar ko'rmoqda. kiberjinoyatlar tufayli jahon iqtisodiyotiga yetkazilayotgan zarar yildan-yilga keskin ortib bormoqda. Xususan, 2019-yilda 3 trillion AQSH dollarini tashkil etgan iqtisodiy zarar 2023-yilga kelib 8 trillion AQSH dollariga yetgan bo'lib, bu ko'rsatkich qariyb 2,7 baravar oshganligini anglatadi. Mavjud prognozlarga ko'ra, 2025-yilga borib ushbu zarar 10,5 trillion AQSH dollariga yetishi kutilmoqda.

Mazkur tendensiya kiberjinoyatlar nafaqat axborot xavfsizligi, balki global iqtisodiy barqarorlikka ham jiddiy tahdid solayotganligini tasdiqlaydi. Shuningdek, statistik o'sish sur'atlari raqamli iqtisodiyot, elektron tijorat va onlayn xizmatlar hajmining kengayishi bilan bevosita bog'liq ekanligini ko'rsatadi. Natijalar kiberxavfsizlikka yo'naltirilayotgan investitsiyalarni ko'paytirish, xalqaro hamkorlikni kuchaytirish va zamonaviy himoya mexanizmlarini joriy etish zarurligini namoyon etadi.

Demak, kiberjinoyatlar keltirayotgan iqtisodiy zararlarning muntazam ortib borishi davlatlar va xalqaro hamjamiyat tomonidan kiberxavfsizlikni strategik ustuvor yo'nalish sifatida ko'rib chiqishni talab etadi. Natijalar shuni ko'rsatadiki, kiberjinoyatlar global iqtisodiyot uchun eng qimmat tahdidlardan biriga aylanmoqda.

Xalqaro huquqiy mexanizmlarga keladigan bo'lsak, kiberjinoyatlarga qarshi kurashishda xalqaro hamkorlik muhim ahamiyatga ega.

Bu borada eng muhim xalqaro hujjatlardan biri — Budapesht konvensiyasi hisoblanadi. Mazkur konvensiya kiberjinoyatlarning yagona tasnifini belgilaydi, davlatlar o'rtasida huquqiy yordamni kuchaytiradi, tergov va ekstraditsiya jarayonlarini soddalashtiradi, elektron dalillar bilan ishlash standartlarini belgilaydi. Shuningdek, Birlashgan millatlar tashkiloti tomonidan kiberjinoyatlarga qarshi kurashish bo'yicha qator tashabbuslar ilgari surilgan.

Yuqoridagi kiberjinoyatlarni oldini olish uchun sun'iy intellekt asosidagi himoya tizimlarini joriy etish, "Zero Trust" xavfsizlik modeliga o'tish, bulutli infratuzilmalarning himoyasini kuchaytirish, kiberxavfsizlik bo'yicha xalqaro hamkorlikning kengayishi, kibergigiyena va foydalanuvchilar savodxonligini oshirish kabi vositalar tavsiya etiladi.

DISCUSSION

Kiberjinoyatlar bugungi kunda davlat suvereniteti, iqtisodiy barqarorlik va inson huquqlariga jiddiy tahdid solmoqda. Ayniqsa, muhim infratuzilmalar – energetika, transport, moliya va sog‘liqni saqlash tizimlariga qilingan hujumlar milliy xavfsizlik masalasiga aylanib bormoqda. Kiberjinoyatlarning transmilliy xarakterga ega ekanligi ularga qarshi kurashishda davlatlararo hamkorlik zarurligini bildiradi. Bitta davlat tomonidan ko‘rilayotgan choralar global tahdidlarni to‘liq bartaraf eta olmaydi. Shu sababli xalqaro tashkilotlar va milliy hukumatlar o‘rtasida axborot almashinuvi mexanizmlarini rivojlantirish muhimdir.

So‘nggi yillarda sun‘iy intellekt texnologiyalarining rivojlanishi ikki tomonlama ta‘sir ko‘rsatmoqda. Bir tomondan, SI yordamida murakkab kiberhujumlar tashkil etilmoqda. Ikkinchi tomondan esa, aynan SI asosidagi xavfsizlik tizimlari tahdidlarni tezkor aniqlash va bartaraf etish imkonini bermoqda.

Kiberxavfsizlikni ta‘minlashda “Zero Trust” konsepsiyasi alohida ahamiyat kasb etmoqda. Ushbu modelga ko‘ra, tizim ichidagi hech bir foydalanuvchi yoki qurilma avtomatik ravishda ishonchli deb hisoblanmaydi. Har bir kirish alohida tekshiriladi va autentifikatsiya qilinadi. Shuningdek, kiberxavfsizlik sohasida inson omili ham muhim rol o‘ynaydi. Statistik ma‘lumotlarga ko‘ra, kiberhujumlarning katta qismi foydalanuvchilarning ehtiyotsizligi yoki yetarli bilimga ega emasligi natijasida muvaffaqiyatli amalga oshiriladi. Shu sababli kiberjigiyena va raqamli savodxonlikni oshirish strategik ahamiyatga ega.

O‘zbekiston uchun ham mazkur masala dolzarb hisoblanadi. Mamlakatda raqamlashtirish jarayonlarining jadallashuvi davlat organlari va xususiy sektor tomonidan kiberxavfsizlik choralari yanada kuchaytirishni talab etmoqda. Milliy qonunchilikni xalqaro standartlarga moslashtirish, malakali mutaxassislar tayyorlash va xalqaro hamkorlikni rivojlantirish kiberxavfsizlikni ta‘minlashning ustuvor yo‘nalishlari hisoblanadi. Kelajakda kvant texnologiyalari, sun‘iy intellekt va Internet of Things (IoT) tizimlarining keng rivojlanishi bilan yangi xavfsizlik muammolari yuzaga kelishi mumkin. Shu sababli kiberxavfsizlik sohasida proaktiv yondashuvni qo‘llash va tahdidlarni oldindan prognoz qilish mexanizmlarini rivojlantirish muhimdir.

XULOSA

Kiberjinoyatlar zamonaviy dunyoning eng jiddiy transmilliy tahdidlaridan biri hisoblanadi. Raqamli texnologiyalar rivojlangani sari kiberjinoyatlar soni va murakkabligi ham ortib bormoqda. Tadqiqot natijalari kiberxavfsizlikning nafaqat texnik, balki huquqiy va institutsional masala ekanligini ko‘rsatdi.

Xalqaro tajribalardan shuni xulosa qilish mumkinki, kiberjinoyatlarga qarshi samarali kurashish uchun davlatlararo hamkorlik, yagona huquqiy standartlar va zamonaviy texnologiyalardan foydalanish zarur. Budapesht konvensiyasi kabi xalqaro hujjatlar bu borada muhim huquqiy asos yaratmoqda. Kiberxavfsizlikni ta‘minlashning istiqbolli yo‘nalishlari sifatida sun‘iy intellekt asosidagi himoya tizimlari, “Zero Trust” modeli, xalqaro axborot almashinuvi va raqamli savodxonlikni oshirishni ko‘rsatish mumkin. Ushbu choralar kiberjinoyatlarning oldini olish va global raqamli makonda xavfsizlikni ta‘minlashga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR:

1. Budapesht konvensiyasi.
2. United Nations. Reports on Cybercrime and Digital Security.

3. International Telecommunication Union. Global Cybersecurity Index Reports.
4. European Union Agency for Cybersecurity. Threat Landscape Reports.
5. INTERPOL. Global Cybercrime Assessment Reports.
6. World Economic Forum. Global Risks Reports.
7. Goodman M. Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It. New York, 2015.
8. Brenner S. Cybercrime and the Law. Boston, 2012.
9. Wall D. Cybercrime: The Transformation of Crime in the Information Age. Cambridge, 2007.
10. Yar M., Steinmetz K. Cybercrime and Society. London, 2019.