



**RAQAMLI TEXNOLOGIYALAR ASRIDA KIBER
JINOYATLARNING SIYOSIY BARQARORLIKKA
DESTRUKTIV TA'SIRI**

A.A. Iminov

*O'zbekiston Respublikasi IIV Akademiyasi Raqamli texnologiyalar va
axborot xavfsizligi kafedrasi boshlig'i*

A.F. Isaqov

*O'zbekiston Respublikasi IIV Akademiyasi Raqamli texnologiyalar va
axborot xavfsizligi kafedrasi boshlig'i o'rinbosari*

SH.K.Kamolov

O'zbekiston Respublikasi IIV Akademiyasi 3-kurs kursanti

Toshkent. sh

<https://doi.org/10.5281/zenodo.20693924>

Annotatsiya: Maqolada raqamli transformatsiya jarayonlari jadallashib borayotgan hozirgi sharoitda kiber jinoyatlarning davlatning ijtimoiy,iqtisodiy siyosiy tizimi va siyosiy barqarorlikka ko'rsatayotgan salbiy ta'siri kompleks tahlil qilinadi. Tadqiqotda kiber jinoyatlar siyosiy xavfsizlikka tahdid sifatida talqin qilinib, ularning davlat boshqaruvi, siyosiy institutlar legitimligi va jamoatchilik ongiga ta'sir mexanizmlari ochib beriladi. Shuningdek, O'zbekiston Respublikasida kiber jinoyatlarga qarshi olib borilayotgan kompleks siyosiy-huquqiy choralar samaradorligini oshirish bo'yicha ilmiy asoslangan xulosalar ilgari suriladi.

Kalit so'zlar: kiber jinoyatlar, siyosiy xavfsizlik, raqamli makon, dezinformatsiya, siyosiy barqarorlik, axborot tahdidlari.

XXI asrda raqamli texnologiyalarning jadal rivojlanishi jamiyatning siyosiy, ijtimoiy va huquqiy munosabatlar tizimini tubdan o'zgartirdi. Davlat boshqaruvi jarayonlarining raqamlashtirilishi davlat boshqaruvini mukammallashtirish va siyosiy strategik qarorlar qabul qilish samaradorligini oshirish bilan bir qatorda, yangi turdagi

Contact: 99 826 99 56





jamiyat va davlatga xavf-xatarlarni ham yuzaga chiqardi. Mazkur xavflarning eng murakkab va kam o'rganilgan shakllaridan biri kiber jinoyatlardir.

Bugungi kunda kiber jinoyatlar yuqori natijalar bilan ajralib turganligi bilan bir qatorda an'anaviy jinoyatchilik doirasidan chiqib, davlat suvereniteti, siyosiy barqarorlik va milliy xavfsizlikka tahdid soluvchi omil sifatida namoyon bo'lmoqda. Ayniqsa, axborot makonining ochiqqligi va siyosiy kommunikatsiyaning raqamli platformalarga ko'chishi kiber jinoyatlarning siyosiy vaziyatga ta'sir doirasini kengaytirmoqda. Shu bois, rivojlanib borayotgan kiber jinoyatlarning mamlakatimiz siyosiy barqarorligiga salbiy ta'sirini ilmiy jihatdan tahlil qilish dolzarb ilmiy-amaliy ahamiyat kasb etadi.

Ilmiy manbalarda kiber jinoyatlar axborot-kommunikatsiya texnologiyalari yordamida sodir etiladigan, axborot resurslari va tizimlariga zarar yetkazishga qaratilgan noqonuniy harakatlar sifatida izohlanadi. Ularning o'ziga xos jihati — hududiy chegaralarning mavjud emasligi va aniqlash mexanizmlarining murakkabligidir.

Siyosiy xavfsizlik nuqtayi nazaridan kiber jinoyatlar davlat hokimiyati organlari faoliyatiga noqonuniy aralashuv, siyosiy axborot oqimlarini buzish hamda siyosiy qarorlar legitimligiga putur yetkazish orqali namoyon bo'ladi. Mazkur jarayonlar siyosiy institutlarga bo'lgan ishonchni zaiflashtiradi va siyosiy tizimning barqaror faoliyat yuritishiga salbiy ta'sir ko'rsatadi.

Raqamli makonning siyosiy hayotga chuqur integratsiyalashuvi kiber jinoyatlarning ta'sir doirasini sezilarli darajada kengaytirdi. Zamonaviy sharoitda kiber jinoyatlar nafaqat texnik infratuzilmaga zarar yetkazuvchi hodisa, balki siyosiy jarayonlarning barqarorligiga bevosita tahdid soluvchi omil sifatida namoyon bo'lmoqda. Ularning destruktiv ta'siri bir qator murakkab va o'zaro bog'liq mexanizmlar orqali amalga oshadi.





Kiber jinoyatlarning eng xavfli ta'sir mexanizmlaridan biri davlat boshqaruvi va siyosiy institutlarga xizmat qiluvchi axborot tizimlariga qaratilgan hujumlardir. Davlat organlarining axborot resurslariga noqonuniy kirish, ma'lumotlarni o'zgartirish yoki yo'q qilish siyosiy qarorlar qabul qilish jarayonining uzluksizligini buzadi. Natijada boshqaruv samaradorligi pasayadi, siyosiy institutlarning funksional barqarorligi

Kiber jinoyatlarning siyosiy jarayonlarga destruktiv ta'siri, ayniqsa, axborot makonida dezinformatsiya va feyk kontent tarqatish orqali yaqqol namoyon bo'ladi. Ijtimoiy tarmoqlar va raqamli platformalar orqali noto'g'ri, buzib ko'rsatilgan yoki ataylab yolg'on axborot tarqatilishi jamoatchilik ongini manipulyatsiya qilishga va aholi orasida norozi kayfiyat uyg'onishiga xizmat qiladi. Bunday jarayonlar fuqarolarda siyosiy beqarorlik kayfiyatini kuchaytirib, davlat siyosatiga bo'lgan ishonchning pasayishiga olib keladi.

Kiber jinoyatlar siyosiy institutlarning obro'-e'tibori va legitimligiga ham salbiy ta'sir ko'rsatadi. Davlat organlari faoliyati haqida soxta ma'lumotlar tarqatish yoki ularning axborot tizimlariga muvaffaqiyatli hujumlar amalga oshirilishi hokimiyatning himoyasizligi haqidagi tasavvurni shakllantiradi. Bu holat siyosiy tizimning mustahkamligiga nisbatan shubha uyg'otib, aholini davlat organlariga bo'lgan ishonchini yo'qotadi, jamiyatda siyosiy ishonchsizlik muhitini kuchaytiradi.

Saylov jarayonlari siyosiy tizimning eng muhim va eng zaif bo'g'inlaridan biri hisoblanadi. Raqamli texnologiyalarning joriy etilishi bilan birga, saylov tizimlariga qaratilgan kiber jinoyatlar xavfi ham ortmoqda. Saylov ma'lumotlarini buzish, ovoz berish jarayoniga aralashish yoki natijalar haqida noto'g'ri axborot tarqatish demokratik tamoyillarga putur yetkazadi hamda siyosiy barqarorlikni izdan chiqaruvchi omilga aylanadi.

Kiber jinoyatlar mavjud ijtimoiy va siyosiy muammolarni sun'iy ravishda keskinlashtirish vositasi sifatida ham qo'llaniladi. Etnik, diniy yoki siyosiy qarama-qarshiliklarga oid provokatsion axborotlarning tarqatilishi jamiyatda ijtimoiy





ziddiyatlarni kuchaytiradi. Natijada siyosiy muhitda beqarorlik yuzaga kelib, davlatning ichki xavfsizligiga tahdid kuchayadi.

Transmilliy xarakterga ega bo'lgan kiber jinoyatlar davlatlarning siyosiy suverenitetiga ham jiddiy xavf tug'diradi. Tashqi subyektlar tomonidan amalga oshiriladigan kiber hujumlar ichki siyosiy jarayonlarga noqonuniy ta'sir ko'rsatish imkonini beradi. Bu holat milliy siyosiy mustaqillik va davlat xavfsizligi masalalarini yangi ilmiy-nazariy yondashuv asosida ko'rib chiqishni taqozo etadi.

O'zbekiston Respublikasida axborot xavfsizligini ta'minlash davlat siyosatining ustuvor yo'nalishlaridan biri hisoblanadi. So'nggi yillarda kiber jinoyatlarga qarshi kurashish borasida normativ-huquqiy baza shakllantirilib, maxsus institutlar faoliyati yo'lga qo'yildi.

Biroq kiber jinoyatlarning siyosiy jarayonlarga ta'siri faqat huquqiy yoki texnik choralar bilan cheklanib qolmasdan, jamiyatning axborot madaniyatini rivojlantirishni ham talab etadi. Fuqarolarning tanqidiy fikrlash qobiliyatini oshirish, axborotni tahlil qilish ko'nikmalarini shakllantirish siyosiy barqarorlikni ta'minlashda muhim omil bo'lib xizmat qiladi.

Raqamli texnologiyalarning keng joriy etilishi bilan bog'liq xavf-xatarlar, xususan kiber jinoyatlar sonining oshishi davlat xavfsizligi va siyosiy barqarorlik uchun muhim tahdidga aylanmoqda. Shu sababli O'zbekiston Respublikasi hukumati va davlat organlari **kiber jinoyatlarga qarshi kurashish uchun kompleks chora-tadbirlar tizimini shakllantirmoqda va uni ilmiy asosda takomillashtirmoqda.**

1. Siyosiy qarorlar va normativ-huquqiy bazani mustahkamlash

2025-yil 30 aprel kuni Prezident Shavkat Mirziyoyev tomonidan imzolangan **PQ-153-sonli "Axborot texnologiyalari yordamida sodir etilgan jinoyatlarga qarshi kurashni yanada kuchaytirish"** to'g'risidagi qaror O'zbekistonning kiber jinoyatlarga qarshi kurash strategiyasini yangi bosqichga olib chiqdi. Mazkur hujjat bir qator muhim vazifalarni belgilaydi: Ichki ishlar vazirligi kiber jinoyatlarga qarshi





kurashish bo'yicha vakolatli organ etib tayinlanadi, jinoiy holatlar aniqlanganda IT vositalardan foydalanganlik og'irlashtiruvchi holat sifatida ko'rib chiqiladi va shaxsiy axborot vositalaridan suiiste'mol qilgan shaxslarga nisbatan ham huquqiy choralar belgilaydi.

Bundan tashqari hukumat tomonidan ishlab chiqilayotgan **axborot texnologiyalaridan jinoyat maqsadlarida foydalanishni tartibga soluvchi maxsus qonun loyihasi** ham mavjud bo'lib, u kiber jinoyatlar uchun alohida huquqiy asos yaratishni ko'zda tutadi.

2. Milliy huquqiy mexanizmlar

O'zbekiston Respublikasining amaldagi qonunchiligi kiber jinoyatlarni turli huquqbuzarlik turlariga mos ravishda tartibga soladi, xususan:

- **Jinoyat kodeksida** axborot texnologiyalari yordamida sodir etilgan jinoyatlar uchun javobgarlik mexanizmlari mavjudligi huquqiy asos sifatida belgilangan.
- 2022-yilda qabul qilingan **“Kiberxavfsizlik to'g'risida”gi Qonun** milliy axborot makonining umumiy xavfsizligini ta'minlash bo'yicha normativ mexanizmlarini belgilaydi.
- Shaxsga doir ma'lumotlarning himoyasi, elektron hujjatlar ma'muriyati va axborot tarqatish tartiblari bo'yicha alohida qonunlar mavjud bo'lib, ular kiber jinoyatlarni oldini olish va fuqarolarning huquqlarini himoya qilishi uchun muhim huquqiy zamin yaratadi.

Bu qonunlarning birgalikdagi tizimi mamlakatda kiber jinoyatlarga qarshi kurashni tabiiy va tushunarli me'yoriy-huquqiy struktura asosida amalga oshirish imkonini beradi.

3. Institutsional mexanizmlar

Ichki ishlar vazirligi doirasida shakllantirilayotgan **Kiberxavfsizlik markazi va maxsus bo'linmalar** jinoyatlarni aniqlash, tergov va oldini olish bo'yicha markazlashtirilgan mexanizm sifatida xizmat qiladi. Qarorda Ichki ishlar vazirligi va





Markaziy bank birgalikda **suspekt tranzaksiyalar monitoringi hamda tezkor javob tizimlarini** yo'lga qo'yish belgilangan.

Bundan tashqari, prokuratura idoralari kiber jinoyatlar bo'yicha huquqiy nazoratni kuchaytiradi hamda amaldagi tartib-qoidalarga rioya etilishini ta'minlashda rol o'ynaydi.

4. Xalqaro hamkorlik va standartlarni joriy etish

O'zbekiston transmilliy kiber jinoyatlar bilan kurashishda xalqaro hamkorlikni ham mustahkamlashga intilmoqda. Milliy kiberxavfsizlik siyosati doirasida xalqaro tajriba, jumladan Budapesht konvensiyasi kabi xalqaro hujjatlar ham inobatga olinmoqda, bu esa xalqaro darajadagi ma'lumotlar almashinuvi va hamkor tergov operatsiyalarini amalga oshirishga zamin yaratadi.

5. Kadrlar tayyorlash va profilaktika choralari

Yangi chora-tadbirlarning yana bir muhim yo'nalishi — **kiberxavfsizlik bo'yicha malakali kadrlar tayyorlash** tizimini yo'lga qo'yishdir. Xususan, Ichki ishlar vazirligi Akademiyasida "Raqamli texnologiyalar sohasida jinoyatlarga qarshi kurashish" ta'lim yo'nalishi joriy etildi va magistratura bosqichida "*Kiberxavfsizlikni huquqiy ta'minlash*" mutaxassisligi ochildi, bu esa milliy kiberxavfsizlik sohasida professional kadrlar salohiyatini oshirishga xizmat qiladi.

Tadqiqot natijalari shuni ko'rsatadiki, kiber jinoyatlar zamonaviy siyosiy tizim uchun kompleks va ko'p qirrali tahdid sifatida namoyon bo'lmoqda. Davlat axborot resurslariga qaratilgan hujumlar, dezinformatsiya jarayonlari va siyosiy kommunikatsiyaga noqonuniy aralashuvlar mamlakat siyosiy barqarorligiga sezilarli darajada salbiy ta'sir ko'rsatadi.

Shu sababli, kiber jinoyatlarga qarshi kurashni faqat texnik masala sifatida emas, balki siyosiy xavfsizlikning muhim tarkibiy qismi sifatida ko'rib chiqish zarur. Kompleks yondashuv asosida olib boriladigan siyosiy-huquqiy va ma'rifiy chora-tadbirlar mamlakat siyosiy barqarorligini mustahkamlashga xizmat qiladi.





REFERENCES

1. O‘zbekiston Respublikasi Konstitutsiyasi. — Toshkent, 2023.
2. O‘zbekiston Respublikasining “Axborotlashtirish to‘g‘risida”gi Qonuni.
3. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni.
4. O‘zbekiston Respublikasi Jinoyat kodeksi. — Toshkent.
5. O‘zbekiston Respublikasi Prezidentining axborot xavfsizligini ta‘minlashga oid farmon va qarorlari.
6. Saidov A.X. Huquqiy davlat va fuqarolik jamiyati. — Toshkent, 2019.
7. Karimov I.A. Yuksak ma‘naviyat – yengilmas kuch. — Toshkent: Ma‘naviyat, 2008.
8. Nye J.S. Cyber Power. — Cambridge: Harvard University Press, 2010.
9. Wall D.S. Cybercrime: The Transformation of Crime in the Information Age. — Polity Press, 2007.
10. Brenner S.W. Cybercrime and the Law. — Northeastern University Press, 2012.
11. Klimburg A. Cybersecurity and Cyberpower. — Brussels, 2011.
12. Zamonaviy ilmiy jurnallar va elektron axborot resurslaridagi tahliliy maqolalar.

