

KIBERJINOYATLARGA QARSHI KURASHISH TIZIMI: O'ZBEKISTONDA VA XALQARO TAJIRIBADA DAVLAT ORGANLARI VA HUQUQIY MEXANIZMLAR

*O'zbekiston Respublikasi IIV Akademiyasi Huquqbuzarliklar Profilaktikasi fakulteti 3-
o'quv kursi 313-guruh kursanti*

Butunboyev Bobosher Qahramon o'g'li

*IIV Akademiyasi Raqamli texnologiyalar va axborot xavfsizligi kafedrasi boshlig'i, fizika-
matematika fanlari nomzodi, dotsent, podpolkovnik*

A.A. Iminov

Annotatsiya: Mazkur maqola kiberjinoyatlar zamonaviy xavfsizlikka tahdid solayotgan global muammo sifatida e'tirof etilayotgan bir sharoitda, O'zbekiston Respublikasi va qator xorijiy davlatlar tajribasi asosida ushbu jinoyat turlariga qarshi kurashishda davlat organlari va muassasalarining huquqiy va tashkiliy rolini tahlil qilishga bag'ishlangan. Maqolada kiberjinoyatlarga oid zamonaviy tahdidlar turlari, ularning o'sish dinamikasi, milliy xavfsizlik va huquqiy tizimga ko'rsatayotgan ta'siri, mavjud yondashuvlarning samaradorligi hamda xorijiy davlatlarda qo'llanilayotgan ilg'or mexanizmlar qiyosiy yondashuv asosida tahlil qilingan. Xususan, O'zbekistonda 2025-yilda qabul qilingan PQ-153-sonli Prezident farmoni asosida shakllantirilgan yangi huquqiy mexanizmlar va ularning amaliy tatbiqi ko'rib chiqilgan. Shuningdek, AQSh va Buyuk Britaniya kabi rivojlangan mamlakatlarning kiberxavfsizlik sohasidagi qonunchiligi va huquqni muhofaza qilish tizimi bilan solishtirma tahlil o'tkazilgan. Maqola yakunida mavjud muammolar aniqlanib, ularni bartaraf etishga qaratilgan aniq taklif va tavsiyalar berilgan.

Anotation: This article is dedicated to the legal and institutional analysis of state bodies and institutions responsible for combating cybercrime in the Republic of Uzbekistan and selected foreign countries, in the context of the growing global threat of cybercrime to national and international security. The paper provides an overview of modern types of cyber threats, their rapid increase, and their impact on legal systems and public safety. It analyzes the effectiveness of existing national measures and compares them with international best practices. Special attention is given to the recent reforms introduced by Presidential Decree No. PQ-153 (April 30, 2025), which established a new legal and organizational framework for fighting cybercrime in Uzbekistan. The article also provides a comparative analysis of the legal infrastructure and enforcement mechanisms in countries such as the United States and the United Kingdom. It concludes by identifying key problems and offering targeted recommendations for improving national cybercrime prevention systems, including the development of inter-agency cooperation and public-private partnerships.

Аннотация: Настоящая статья посвящена правовому и институциональному анализу роли государственных органов и учреждений в борьбе с киберпреступностью в Республике Узбекистан и ряде зарубежных стран в условиях нарастающей глобальной угрозы цифровым атакам. В работе рассмотрены современные виды

киберугроз, динамика их роста, влияние на национальную безопасность и правовую систему, а также эффективность применяемых мер. Особое внимание уделено Указу Президента Республики Узбекистан № ПҚ-153 от 30 апреля 2025 года, которым предусмотрено внедрение новых правовых механизмов и координирующих структур в области противодействия преступлениям, совершаемым с использованием информационных технологий. Также проведен сравнительный анализ опыта таких стран, как США и Великобритания, в части законодательства, институтов и механизмов правоприменения в сфере кибербезопасности. В завершение статьи представлены основные выявленные проблемы и конкретные рекомендации по совершенствованию национальной системы борьбы с киберпреступностью, включая развитие межведомственного взаимодействия и сотрудничества с частным сектором.

KIRISH

Kiberjinoyatlar – axborot- kommunikatsiya texnologiyalaridan foydalangan holda sodir etiladigan, odatda transmilliy, murakkab va tez rivojlanayotgan huquqbuzarliklar toifasiga kiradi. Zamonamizda kiberjinoyatlar axborot xavfsizligi, moliyaviy barqarorlik, inson huquqlari va davlat suvereniteti uchun keskin tahdid sanalmoqda. Masalan, O'zbekistonda oxirgi yillarda kiberjinoyatlar soni keskin oshgani haqida ma'lumotlar mavjud: 2024 yilda barcha jinoyatlar orasida kiberjinoyatlar 44,4 % ni tashkil qilgani qayd etilgan. monitor.kun.uz+1

Shu jihatdan, kiberjinoyatlarga qarshi samarali kurashish uchun mazkur soha bo'yicha davlat organlari va muassasalarning huquqiy- tashkiliy bazasi va amaliy mexanizmlari muhimdir. Maqolaning maqsadi — O'zbekistonda kiberjinoyatlarga qarshi kurashuvchi davlat organlari va muassasalarning huquqiy va tashkiliy holatini tahlil etish hamda xalqaro tajribalarni solishtirish orqali takomillashtirish bo'yicha tavsiyalar ishlab chiqishdir. Vazifalar: (1) O'zbekistonda kiberjinoyatlarga qarshi huquqiy hujjatlar va organlar tizimini tashkil etish jihatlari; (2) xorijiy davlatlar (masalan, Buyuk Britaniya, AQSh) tajribasini ko'rib chiqish; (3) tizimdagi muammolarni aniqlash va takliflar ishlab chiqish.

Asosiy qism

1. O'zbekistonda kiberjinoyatlarga qarshi kurashning huquqiy- tashkiliy bazasi

1.1. Huquqiy hujjatlar

O'zbekistonda kiberjinoyatlarga qarshi kurash bilan bog'liq bir qator huquqiy hujjatlar qabul qilingan. Masalan, 2025 yil 30 aprel kuni qabul qilingan Prezident farmoni – PQ- 153 Decree of the President of the Republic of Uzbekistan “On Measures to Further Strengthen the Fight Against Crimes Committed Using Information Technologies” — kiberjinoyatlar

bilan kurashish sohasida muhim hujjatlardan biridir. topdatatech.uz+2Dentons+2 Ushbu hujjat bilan:

- Ministry of Internal Affairs of the Republic of Uzbekistan (MIA) kiberjinoyatlarni ishlab chiqish va kurashish bo'yicha vakolatli organ sifatida belgilandi. [UzDaily.uz](https://uzdaily.uz)+1
- Bank kartalar, elektron hamyonlar, SIM- kartalar orqali sodir etiladigan jinoyatlar uchun yuridik (ma'muriy va jinoiy) javobgarlik qo'yildi. [Tashkent Times](https://tashkenttimes.uz)+1
- Moliyaviy tashkilotlar va to'lov tizimlari kiberxavfsizlik talablariga rioya qilmaslik holatlarida zararlarni qoplash majburiyatiga ega bo'ldi. [Dentons](https://dentons.com)
- Ma'lumotlarni uzatish, kartalarni bloklash va huquqni muhofaza qilish organlari bilan elektron axborot almashinuvi tizimi joriy etilishi belgilandi. topdatatech.uz+1

Shuningdek, O'zbekistonda "On the Protection of the Rights of Users of Online Platforms and Websites" nomli yangi loyihaviy qonun hujjati ishlab chiqilmoqda, unda onlayn faoliyat, spam, phishing kabi zamonaviy kiberxavf jihatlarini ko'rib chiqilmoqda. [Zamin.uz](https://zamin.uz)

1.2. Tashkiliy tuzilma va vakolatli organlar

Kiberjinoyatlarga qarshi kurashishda O'zbekistonda bir nechta davlat organlari va muassasalar faoliyat yuritadi. Masalan, MIA ustuvor organ sifatida ko'rsatilgan. Farmonda, shuningdek, Prosecutor General's Office of the Republic of Uzbekistan tarkibida Kiberjinoyatlarga qarshi kurash va qonuniylikni nazorat qilish vakolatli bo'limi tashkil etilishi belgilandi. topdatatech.uz Moliyaviy tashkilotlar (masalan, Central Bank of the Republic of Uzbekistan) ham to'lov tizimlari operatorlari bilan hamkorlikda faoliyat olib boradi. [Tashkent Times](https://tashkenttimes.uz)

1.3. Amaliy muammolar va tanqidiy jihatlar

Kiberjinoyatlar sonining keskin oshishi xavotirli. Masalan, O'zbekistonda so'nggi besh yil ichida kiberjinoyatlar 68 baravarga oshgani ma'lum qilindi va 1 trillion 909 milliard so'm zarar ko'rilgani qayd etildi. monitor.kun.uz Bu holat tizimning hozirgi holati bilan kurashishning yetarli emasligini ko'rsatadi. Shuningdek, huquqiy hujjatlar bilan amaliy mexanizmlarning to'liq mos emasligi, kiberjinoyatlar bilan kurashdagi axborot almashuvi va xalqaro hamkorlikdagi yetishmovchiliklar muammo sifatida ko'rinmoqda.

2. Xorijiy davlatlarda kiberjinoyatlarga qarshi kurash: Britaniya va AQSh misollari

2.1. Buyuk Brytaniya tajribasi

National Crime Agency (NCA) Buyuk Brytaniyada kiberjinoyatlar bilan kurashda markaziy huquqni muhofaza qiluvchi organ hisoblanadi. U saytida kiberjinoyatlar qatorida tajovuzkor hujumlar, ransomware, phishing va boshqa tahdidlar ustida faoliyat yuritishini bildiradi. nationalcrimeagency.gov.uk+1 Britaniyada ham – Cybersecurity Act 2018 kabi

qonuniy hujjatlar mavjud bo'lib, unda muhim infratuzilmalarga xizmat ko'rsatuvchi tashkilotlar va raqamli xizmat provayderlari uchun majburiyatlar belgilangan. cyberly.org+1 Bu tajriba davlat huquqni muhofaza qilish va maxsus axborot- xavfsizlik organlari hamkorligini tashkil etishda namuna bo'lishi mumkin.

2.2. Qo'shma Shtatlar tajribasi

AQShda kiberjinoyatlarga qarshi kurash bir necha huquqni muhofaza qilish organlari (masalan, United States Department of Justice (DOJ), Federal Bureau of Investigation (FBI)) tomonidan olib boriladi. DOJning "Strategic Approach to Countering Cybercrime" hujjatida asosiy maqsadlar qatorida "ransomware", ma'lumot o'g'irlanishi, botnet'lar, dasturchilar va boshqa kiberjinoyatchilarni aniqlash va javobgarlikka tortish" ko'rsatilgan. justice.gov Bundan tashqari, qonunchilik jihatdan masalan, Cybersecurity Information Sharing Act of 2015 (CISA) – xususiy sektor va hukumat o'rtasida kiberxavfsizlik tahdidlarini ma'lumot almashish mexanizmini mustahkamlashga mo'ljallangan. Википедия

3. Solishtirma tahlil

O'zbekistonda ham, xorijiy davlatlarda ham kiberjinoyatlarga qarshi kurashishda organlar vakolatlari, huquqiy hujjatlar va tashkiliy mexanizmlarning mavjudligi muhim. Ammo ba'zi jihatlar bilan farqlanadi:

- Britaniya va AQSh tajribasida maxsus texnik, razvedka va xalqaro hamkorlik tizimlari allaqachon tashkillashtirilgan. O'zbekistonda esa amaliy jihatlar — masalan, bank tizimlari, to'lov operatorlari bilan axborot almashuvi va birlashtirilgan platformaning joriy etilishi — 2025 yil sentabrga belgilangan. UzDaily.uz+1

- Xorijiy tajribada xususiy sektor bilan hamkorlik (public-private partnership) keng qo'llaniladi. O'zbekistonda esa bu jihat hali tatbiq bosqichida.

- Huquqiy ta'minot: O'zbekistonda so'nggi o'zgarishlar (farmonlar, loyihaviy qonunlar) bilan amalga oshirilmoqda. Xorijda esa muayyan aktlar uzoq yillardan beri amal qilmoqda.

- Axborot almashuvi va real- vaqtli monitoring: O'zbekistonda 2025 yilga mo'ljallangan platforma joriy etilishi belgilangan. Xorijda esa bu kabi tizimlar barqaror ishlamoqda.

4. Takliflar

- O'zbekistonda kiberjinoyatlarga qarshi kurashuvchi organlar va muassasalar vakolatlari, o'zaro hamkorligi va axborot almashuvi mexanizmlarini yanada mustahkamlash lozim.

- Xorijiy tajribaga muvofiq, davlat va xususiy sektor o'rtasida PPP (public-private partnership) mexanizmini rivojlantirish tavsiya etiladi.

- Kiberjinoyatlarga qarshi kurashda ma'lumotlarni real vaqtda yig'ish, tahlil qilish va javob choralari ko'rishga qaratilgan birlashtirilgan platforma joriy etilishi zarur — O'zbekistonda bunday loyihalar 2025 yilda boshlanmoqda.

- Huquqiy bazani kengaytirish: Onlayn platformalar, phishing, deep- fake, kriptoaktivlar bilan bog'liq jinoyatlar uchun maxsus huquqiy modellar ishlab chiqilishi muhim. O'zbekistonda shunday qonunchilik tashabbuslari bor. live.kun.uz

•Xalqaro hamkorlikni rivojlantirish: Kiberjinoyatlar ko'pincha chet el bilan bog'liq bo'lganligi sababli, xalqaro konvensiyalar (masalan, Budapest Convention on Cybercrime)ga qo'shilish va tajriba almashish muhim.

Xulosa

Kiberjinoyatlarga qarshi kurash sohasida davlat organlari va muassasalarning huquqiy-tashkiliy tizimi markaziy ahamiyatga ega. O'zbekistonda so'nggi yillarda mazkur sohada sezilarli qonunchilik va tashkiliy o'zgarishlar amalga oshirilmoqda: MIAga vakolat berilishi, bank va to'lov tizimlari bilan hamkorlik, axborot almashuvi platformasi joriy etilishi belgilanishi — ularning barchasi ijobiy. Biroq, tajriba ko'rsatadiki, samarali kurash uchun faqat hujjatlar emas, balki amaliy mexanizmlar, xususiyl sektor bilan hamkorlik, xalqaro tajriba va uzluksiz monitoring tizimi ham zarur. Xorijiy davlatlar tajribasi (Buyuk Britaniya, AQSh) bunday tizimlar yanada rivojlanganligini ko'rsatadi.

Kelgusida O'zbekistonda kiberjinoyatlarga qarshi kurashni mustahkamlash maqsadida huquqiy hujjatlar — ayrim hollarda yangi qonunlar, tashkilotlarning vakolatlari kengaytirish, axborot- tahlil tizimlarini yaratish hamda xalqaro hamkorlik mexanizmlarini yanada chuqurlashtirish yo'lida ishlar davom etishi lozim.

FOYDALANILGAN ADABIYOTLAR:

1. President of the Republic of Uzbekistan Decree No PQ- 153 «On Measures to Further Strengthen the Fight Against Crimes Committed Using Information Technologies». [topdatatech.uz+2UzDaily.uz+2](#)
2. Dentons Insights “Uzbekistan tightens cybersecurity obligations”. Dentons
3. Kun.uz “Uzbekistan sees 68- fold surge in cybercrime...” [monitor.kun.uz](#)
4. National Crime Agency – Cybercrime. [nationalcrimeagency.gov.uk+1](#)
5. Cyberly “What Laws Address Cyberattacks In The UK?” [cyberly.org](#)