

JOURNAL OF DIGITAL LAW AND INNOVATION (JDLI)

LAW • TECHNOLOGY • INNOVATION • JUSTICE

 OPEN
ACCESS

INTERNATIONAL
PEER-REVIEWED
JOURNAL



OUR FIELDS

- Digital law
- Cybersecurity law
- Artificial intelligence and robotics law
- Intellectual property law
- LegalTech and legal innovations
- E-government and digital public services
- Legal aspects of AgroTech and GreenTech
- Smart city and digital governance



OUR INDEXING



Google Scholar



zenodo Zenodo



DOI



OpenAIRE



Open Access



SYSTEM
BREACH

UNAUTHORIZED
ACCESS

CYBER ATTACK

DIGITAL LAW



<https://unireview.uz/index.php/jdli>



Published by
UniLex Global, Uzbekistan



VOLUME 1

ISSUE 1



JUNE 2026



“UNILEX GLOBAL” LLC

**Raqamli huquq va innovatsiya
jurnali**

**Journal of Digital Law and
Innovation**

June, 2026

VOLUME 1, ISSUE 1



EDITORIAL TEAM

Editor-in-Chief, Tukhtashev Hikmatilla Ismatillaevich - Head of the Department of Legal Sciences, Doctor of Philosophy in Legal Sciences (PhD), TIAME National Research University, Tashkent, Republic of Uzbekistan.

1. **Editorial Board Member Borotov Mirodiljon Xomudjonovich** — Doctor of Legal Sciences, Professor, Head of the Department of Civil Law, International Law and International Organizations, Institute of State and Law of the Academy of Sciences of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
2. **Editorial Board Member Maripova Sevarxon Aribjanovna** — Doctor of Philosophy in Legal Sciences (PhD), Associate Professor, Department of Social Sciences, Cyber University State University, Tashkent, Republic of Uzbekistan.
3. **Editorial Board Member Kaharova Munira Maxamajanovna** — Doctor of Political Sciences (DSc), Researcher, Institute of Criminology of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
4. **Editorial Board Member Yuldashev Mutalib Ibrohimovich** — Doctor of Economic Sciences, Professor, Department of Economics, Tashkent University of Science and Technology, Tashkent, Republic of Uzbekistan.
5. **Editorial Board Member Bafaev Shukhrat Gafurovich** — Doctor of Legal Sciences, Head of the Tashkent City Branch, Center for the Analysis of Democratic Processes, Tashkent, Republic of Uzbekistan.
6. **Editorial Board Member Khodjaeva Aziza Bakhtiyarovna** — Doctor of Philosophy in Legal Sciences (PhD), “Academy of Labor and Social Relations” under the Federation of Trade Unions of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
7. **Editorial Board Member Khudoyberdieva Viloyat Jabbrovanovna** — Candidate of Legal Sciences (PhD), Olmazor District Department of Public Education, Tashkent City, Republic of Uzbekistan.
8. **Editorial Board Member Boboumarova Munira Kurbonovna** — Doctor of Philosophy in Legal Sciences (PhD), Department for Organization of Investigative Activities, Investigation Division, Tashkent City Internal Affairs Department, Tashkent, Republic of Uzbekistan.
9. **Editorial Board Member Usmonov Vosid Muhammadievich** — Doctor of Philosophy in Legal Sciences (PhD), Diplomatic University, Tashkent, Republic of Uzbekistan.
10. **Editorial Board Member Mirzayeva Malika Baxadirovna** — Doctoral Researcher, PhD, Associate Professor, Department of Digital Technologies and Artificial Intelligence, Tashkent Institute of Irrigation and Agricultural Mechanization Engineers – National Research University, Tashkent, Republic of Uzbekistan.
11. **Editorial Board Member Allayorov Tulqin Ruziqulovich** — Doctor of Philosophy in Philology (PhD), Associate Professor, Nizami Named Tashkent State Pedagogical University, Tashkent, Republic of Uzbekistan.
12. **Editorial Board Member Tosheva Maftuna Anvar kizi** — Doctor of Philosophy in Legal Sciences (PhD), Tashkent Institute of Irrigation and Agricultural Mechanization Engineers – National Research University, Tashkent, Republic of Uzbekistan.
13. **Editorial Board Member Askarov Jaloliddin Toychievich** — Doctor of Philosophy in Legal Sciences (PhD), Deputy Head, Department of Business Law, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
14. **Editorial Board Member Abdixakimov Islombek Bahodir o'g'li** — Master of Law (LL.M), Head of the Artificial Intelligence and Legal Tech Laboratory, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
15. **Editorial Board Member Kalandarov Aminjon Amondullayevich** — Doctor of Philosophy in Legal Sciences (PhD), Acting Associate Professor, Department of Business Law, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
16. **Editorial Board Member Hakimov Komil Bakhtiyarovich** — Doctor of Legal Sciences (DSc), Professor, Head of the Department of Criminal Law, Criminology and Anti-Corruption, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.

CONTENTS

03

**XUDOYBERDIYEV XUMOYUNBEK XABIBULLA O'G'LI,
QURVONBOYEV ASLBEK AZIZJON O'G'LI**

KIBERXAVFSIZLIKNING KONSTITUTSIYAVIY ASOSLARI
VA MILLIY XAVFSIZLIKKA TA'SIRI

13

SATTAROV ULUG'BEK UMED O'G'LI

RAQAMLI IQTISODIYOT SHAROITIDA KIBERXAVFSIZLIK
MUAMMOLARI: ZAMONAVIY XAVFLAR VA BARQAROR
RIVOJLANISH YONDASHUVLARI

20

MANNABJONOVA DURDONA ABDUXALIL QIZI

DAVLAT IDORALARIDA SUN'IY INTELEKTDAN
FOYDALANISHNI HUQUQIY TARTIBGA SOLISH

34

HUSANOVA SHABBONA BAHROMOVNA

RAQAMLI MUHITDA INTELEKTUAL MULK
HUQUQINING MUHOFAZASI

40

RIXSIYEV MUHAMMADAZIZ MUZAFFAR O'G'LI

O'ZBEKISTON RESPUBLIKASIDA
KIBERJINOYATCHILIKKA QARSHI KURASHISHNING
KONSITUTSIYAVIY-HUQUQIY VA XALQARO-
HUQUQIY ASOSLARI

54

BOYMIRZAYEVA MADINA IBROHIM QIZI

SUN'IY INTELEKTNING HUQUQ TIZIMLARI VA ODIL
SUDLOV FAOLIYATIGA TA'SIRI



O‘ZBEKISTON RESPUBLIKASIDA KIBERJINOYATCHILIKKA QARSHI KURASHISHNING KONSITUTSIYAVIY-HUQUQIY VA XALQARO-HUQUQIY ASOSLARI

Rixsiyev Muhammadaziz Muzaffar o‘g‘li

*“TIQXMMI” Milliy tadqiqot universiteti “Ekologiya va
huquq” fakulteti Yurisprudensiya yo‘nalishi 3-kurs talabasi*

MAQOLA MA'LUMOTI

Kalit so‘zlar:

kiberjinoatchilik,
kiberxavfsizlik,
axborot xavfsizligi,
konstitutsiyaviy huquqlar,
shaxsga doir ma'lumotlar,
raqamli texnologiyalar,
xalqaro huquq,
Budapesht konvensiyasi,
axborot makoni,
kiberhujumlar,
milliy qonunchilik,
xalqaro hamkorlik.

ANNOTATSIYA

Mazkur maqolada O‘zbekiston Respublikasida kiberjinoatchilikka qarshi kurashishning konstitutsiyaviy-huquqiy va xalqaro-huquqiy asoslari tahlil qilinadi. Tadqiqotda kiberjinoatchilik tushunchasi, uning zamonaviy ko‘rinishlari hamda jamiyat va davlat xavfsizligiga ta’siri yoritilgan. Shuningdek, O‘zbekiston Respublikasi Konstitutsiyasi, jinoyat va axborot qonunchiligida nazarda tutilgan kiberxavfsizlikni ta’minlash mexanizmlari o‘rganilgan. Maqolada xalqaro-huquqiy normalar, xususan kiberjinoatchilikka qarshi kurashishga qaratilgan xalqaro hujjatlar va xorijiy davlatlar tajribasi tahlil qilinib, milliy qonunchilikni takomillashtirish bo‘yicha ilmiy-amaliy takliflar ishlab chiqilgan. Tadqiqot natijalari kiberxavfsizlikni ta’minlash, fuqarolarning axborot sohasidagi konstitutsiyaviy huquqlarini himoya qilish hamda kiberjinoatchilikka qarshi kurashishning samarali huquqiy mexanizmlarini rivojlantirishga xizmat qiladi.

CONSTITUTIONAL-LEGAL AND INTERNATIONAL-LEGAL FOUNDATIONS FOR COMBATING CYBERCRIME IN THE REPUBLIC OF UZBEKISTAN

ARTICLE INFO

Keywords:

cybercrime, cybersecurity,
information security,
constitutional rights,
personal data,
digital technologies,
international law,
Budapest Convention,

ABSTRACT

This article analyzes the constitutional and international legal foundations of combating cybercrime in the Republic of Uzbekistan. The study examines the concept of cybercrime, its modern forms, and its impact on the security of society and the state. It also explores the mechanisms for ensuring cybersecurity established by the Constitution of the Republic of Uzbekistan, criminal legislation, and information-related laws. The article analyzes international legal norms, including international instruments aimed at combating cybercrime, as well as

information space,
cyberattacks,
national legislation,
international cooperation.

the experience of foreign countries in this field. Based on the analysis, scientific and practical recommendations for improving national legislation are proposed. The findings contribute to strengthening cybersecurity, protecting the constitutional rights of citizens in the information sphere, and developing effective legal mechanisms for combating cybercrime.

ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ: СОВРЕМЕННЫЕ РИСКИ И ПОДХОДЫ УСТОЙЧИВОГО РАЗВИТИЯ

ИНФОРМАЦИЯ СТАТЬИ

Ключевые слова:

киберпреступность,
кибербезопасность,
информационная
безопасность,
конституционные права,
персональные данные,
цифровые технологии,
международное право,
Будапештская конвенция,
информационное
пространство,
кибератаки,
национальное
законодательство,
международное
сотрудничество.

АННОТАЦИЯ

В данной статье анализируются конституционно-правовые и международно-правовые основы противодействия киберпреступности в Республике Узбекистан. В исследовании раскрываются понятие киберпреступности, ее современные проявления, а также влияние на безопасность общества и государства. Кроме того, изучены механизмы обеспечения кибербезопасности, предусмотренные Конституцией Республики Узбекистан, уголовным законодательством и законодательством в сфере информации. В статье проанализированы международно-правовые нормы, включая международные документы, направленные на борьбу с киберпреступностью, а также опыт зарубежных государств. На основе проведенного анализа разработаны научно-практические предложения по совершенствованию национального законодательства. Результаты исследования направлены на укрепление кибербезопасности, защиту конституционных прав граждан в информационной сфере и развитие эффективных правовых механизмов противодействия киберпреступности.

KIRISH

XXI asrda raqamli texnologiyalar va axborot-kommunikatsiya tizimlarining jadal rivojlanishi jamiyat hayotining barcha sohalarini tubdan o'zgartirmoqda. Davlat boshqaruvi, iqtisodiyot, moliya, ta'lim, sog'liqni saqlash hamda boshqa muhim tarmoqlarning raqamlashtirilishi insoniyat taraqqiyotiga yangi imkoniyatlar yaratish bilan birga, kiberxavfsizlik bilan bog'liq yangi tahdidlarni ham yuzaga keltirmoqda. Xususan, kompyuter tizimlariga noqonuniy kirish,

ma'lumotlarni o'g'irlash, zararli dasturlar tarqatish, internet firibgarligi, shaxsga doir ma'lumotlardan noqonuniy foydalanish kabi kiberjinoyatlar davlatlar va jamiyatlar oldida turgan dolzarb muammolardan biriga aylanmoqda.

Kiberjinoyatchilikning o'ziga xos xususiyati uning transmilliy xarakterga egaligidadir. Kiberjinoyatlar davlat chegaralari bilan cheklanmaydi, ular bir vaqtning o'zida bir nechta mamlakatlarning axborot infratuzilmasiga zarar yetkazishi mumkin. Shu sababli mazkur turdagi huquqbuzarliklarga qarshi kurashishda nafaqat milliy qonunchilikni takomillashtirish, balki xalqaro hamkorlikni rivojlantirish ham muhim ahamiyat kasb etadi. Zamonaviy sharoitda kiberjinoyatchilikka qarshi samarali kurashish davlatlarning o'zaro axborot almashinuvi, huquqiy yordam ko'rsatishi va xalqaro standartlarni milliy qonunchilikka implementatsiya qilish darajasiga bevosita bog'liqdir.

O'zbekiston Respublikasida ham raqamli iqtisodiyot va elektron davlat xizmatlarini rivojlantirish bo'yicha keng ko'lamli islohotlar amalga oshirilmoqda. Natijada axborot tizimlari va telekommunikatsiya tarmoqlarining ahamiyati ortib bormoqda. Biroq raqamlashtirish jarayonlarining jadallashuvi kiberxavfsizlikni ta'minlash va kiberjinoyatchilikka qarshi kurashishning huquqiy mexanizmlarini yanada takomillashtirish zaruratini yuzaga keltirmoqda. Shu nuqtai nazardan, fuqarolarning axborot olish huquqi, shaxsiy hayot daxlsizligi, shaxsga doir ma'lumotlarning himoyasi hamda davlatning axborot xavfsizligini ta'minlash borasidagi majburiyatlari alohida ahamiyat kasb etadi.

Mamlakatimizda kiberxavfsizlikni ta'minlashga qaratilgan qator normativ-huquqiy hujjatlar qabul qilingan bo'lib, ular orasida O'zbekiston Respublikasi Konstitutsiyasi, Jinoyat kodeksi, "Kiberxavfsizlik to'g'risida"gi Qonun, "Shaxsga doir ma'lumotlar to'g'risida"gi Qonun hamda axborotlashtirish sohasidagi boshqa normativ-huquqiy hujjatlar muhim o'rin tutadi. Biroq kiberjinoyatchilikning yangi shakllari va usullarining paydo bo'layotgani ushbu sohadagi huquqiy tartibga solish mexanizmlarini doimiy ravishda takomillashtirib borishni talab etmoqda.

O'zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashishning konstitutsiyaviy-huquqiy va xalqaro-huquqiy asoslarini tahlil qilish, amaldagi milliy qonunchilik va xalqaro standartlarning o'zaro uyg'unligini o'rganish hamda mavjud muammolarni aniqlash orqali ularni bartaraf etishga qaratilgan ilmiy-amaliy takliflar ishlab chiqish bo'yicha tadqiqot olib borildi. Tadqiqot davomida qiyosiy-huquqiy, tizimli, formal-yuridik va tahliliy metodlardan foydalanildi.

METODOLOGIYA

Mazkur tadqiqotda O'zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashishning konstitutsiyaviy-huquqiy va xalqaro-huquqiy asoslarini o'rganishda umumilmiy va maxsus yuridik tadqiqot metodlaridan foydalanildi. Xususan, formal-yuridik metod yordamida

O'zbekiston Respublikasi Konstitutsiyasi, Jinoyat kodeksi, "Kiberxavfsizlik to'g'risida"gi Qonun hamda axborot xavfsizligi sohasidagi boshqa normativ-huquqiy hujjatlarning mazmuni va huquqiy mohiyati tahlil qilindi.

Qiyosiy-huquqiy metod asosida O'zbekiston Respublikasining kiberjinoyatchilikka qarshi kurashish sohasidagi qonunchiligi xalqaro-huquqiy standartlar hamda ayrim xorijiy davlatlar, jumladan AQSh, Germaniya va Singapur tajribasi bilan taqqoslandi. Tizimli-tahliliy metod orqali kiberjinoyatchilikka qarshi kurashishning konstitutsiyaviy, jinoyat-huquqiy va xalqaro-huquqiy mexanizmlari yagona tizim sifatida o'rganildi.

XXI asrda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi jamiyatning barcha sohalarini raqamlashtirishga xizmat qilmoqda. Shu bilan birga, raqamli muhitdan noqonuniy maqsadlarda foydalanish holatlari ham ortib bormoqda. Natijada kiberjinoyatchilik zamonaviy dunyoning eng xavfli transmilliy tahdidlaridan biriga aylandi. Ilmiy adabiyotlarda kiberjinoyatchilik tushunchasiga turlicha yondashuvlar mavjud. Keng ma'noda kiberjinoyatchilik deganda kompyuter tizimlari, axborot tarmoqlari va elektron ma'lumotlardan foydalanish orqali sodir etiladigan yoki ularga qarshi qaratilgan barcha huquqbuzarliklar tushuniladi. Mazkur tushuncha kompyuter tizimlarining o'zi jinoyat obyekti bo'lgan holatlarni ham, kompyuter texnologiyalari jinoyat sodir etish vositasi sifatida foydalanilgan holatlarni ham qamrab oladi. Kiberjinoyatchilikning xalqaro-huquqiy asoslarini belgilovchi muhim hujjatlardan biri 2001-yilda qabul qilingan Budapesht konvensiyasi hisoblanadi. Mazkur Konvensiyada kompyuter tizimlariga noqonuniy kirish, ma'lumotlarni noqonuniy egallash, tizimlar faoliyatiga noqonuniy aralashish, kompyuter firibgarligi va boshqa qator qilmishlar kiberjinoyatlar sifatida e'tirof etilgan.

O'zbekiston Respublikasida ham kiberxavfsizlikni ta'minlash davlat siyosatining ustuvor yo'nalishlaridan biri hisoblanadi. Xususan, "Kiberxavfsizlik to'g'risida"gi Qonun axborot makonida xavfsizlikni ta'minlashning huquqiy asoslarini mustahkamlaydi. Shuningdek, O'zbekiston Respublikasi Jinoyat kodeksida kompyuter axborotidan noqonuniy foydalanish, axborot tizimlariga noqonuniy kirish va boshqa kiberjinoyatlar uchun javobgarlik nazarda tutilgan.

Kiberjinoyatchilikning eng muhim jihatlaridan biri uning transmilliy xarakterga egaligidir. An'anaviy jinoyatlardan farqli ravishda kiberjinoyatlar muayyan hudud bilan chegaralanmaydi. Jinoyatchi bir davlat hududida bo'lib, boshqa davlat fuqarolari yoki tashkilotlariga qarshi hujum uyushtirishi mumkin. Transmilliylikning asosiy sababi internet tarmog'ining global xususiyatidir. Kiberjinoyatni sodir etishda foydalanilgan serverlar bir necha davlatlarda joylashgan bo'lishi, jinoyatchi boshqa davlatda faoliyat yuritishi, jabrlanuvchi esa uchinchi davlat hududida bo'lishi mumkin. Bu esa jinoyatni aniqlash, tergov qilish va aybdorlarni javobgarlikka tortish jarayonini murakkablashtiradi. Shu sababli xalqaro hamkorlik kiberjinoyatchilikka qarshi kurashning asosiy vositalaridan biri hisoblanadi.

Davlatlar o'rtasida axborot almashinuvi, ekstraditsiya, o'zaro huquqiy yordam va qo'shma tergov mexanizmlarining samarali ishlashi kiberjinoyatlarga qarshi kurash samaradorligini oshiradi. Bu borada Interpol, Yevropol hamda Birlashgan Millatlar Tashkiloti muhim rol o'ynamoqda. Bundan tashqari, kiberjinoyatchilikning transmilliy tabiati davlat suvereniteti, yurisdiksiya va xalqaro javobgarlik masalalariga ham yangi yondashuvlarni talab qilmoqda. Shu bois ko'plab davlatlar milliy qonunchilikni xalqaro standartlarga moslashtirish va xalqaro hamkorlik mexanizmlarini kuchaytirishga intilmoqda. Natijada kiberjinoyatchilik nafaqat alohida shaxslar yoki tashkilotlar, balki butun davlatlar xavfsizligiga tahdid soluvchi global muammo sifatida namoyon bo'lmoqda. Shu sababli unga qarshi kurashishda milliy huquqiy mexanizmlar bilan bir qatorda xalqaro-huquqiy hamkorlik ham hal qiluvchi ahamiyat kasb etadi. Oxirgi statistik ma'lumotlarga nazar tashlaydigan bo'lsak, fuqarolarni kartalaridan ommaviy ravishda pul yechib olinishlari va hakerlar tomonidan ijtimoiy tarmoq profillari vzlom qilinishi bilan bog'liq jinoyatlar O'zbekiston Respublikasi hududi emas balki boshqa davlatlardan turib amalga oshirilmoqda. Bu esa o'z navbatidan davlatning imperativ tushdagi qonunlariga roiya qilmaganlikni anglatib javobgarlikka asos bo'ladi va qator tashkilotlar tomonidan vaziyat atroflicha o'rganilib zarur himoya choralari qo'llanilishiga asos bo'ladi.

NATIJALAR

Kiberjinoyatchilikka qarshi kurashning konstitutsiyaviy-huquqiy asoslarini tahlil qilishda, avvalo, axborot olish va undan foydalanish huquqining konstitutsiyaviy mazmunini yoritish zarur. Chunki raqamli jamiyat sharoitida insonning ko'plab huquq va erkinliklari aynan axborot-kommunikatsiya texnologiyalari orqali amalga oshiriladi. Shu bois kiberxavfsizlikni ta'minlash fuqarolarning axborot sohasidagi konstitutsiyaviy huquqlarini himoya qilish bilan chambarchas bog'liqdir. O'zbekiston Respublikasi Konstitutsiyasida avvalo inson manfaatlari ustuvor hisoblanib uning har bir moddasidan tortib boshqa qonunchiliklar ham inson va uning barcha huquqlari taminlashiga xizmat qiladi. O'zbekiston Respublikasi Konstitutsiyasining 33-moddasiga muvofiq, har kim fikrlash, so'z va e'tiqod erkinligi huquqiga ega. Ushbu norma shaxsning axborot bilan erkin munosabatda bo'lishi, o'z fikrini shakllantirishi va uni erkin ifoda etishining konstitutsiyaviy asosini tashkil etadi. Axborot texnologiyalarining rivojlanishi natijasida mazkur huquq internet tarmoqlari, ijtimoiy media platformalari, elektron ommaviy axborot vositalari va boshqa raqamli resurslar orqali amalga oshirilmoqda. Shuningdek har kim axborotni izlash, olish va tarqatish huquqiga egaligi mustahkamlangan. Mazkur norma demokratik jamiyatning asosiy tamoyillaridan biri bo'lib, fuqarolarning davlat va jamiyat hayotidagi faol ishtirokini ta'minlaydi. Shu bilan birga, mazkur huquqdan foydalanish boshqa shaxslarning huquqlari, davlat xavfsizligi, jamoat tartibi hamda qonun bilan qo'riqlanadigan manfaatlarga zarar yetkazmasligi lozim. Kiberjinoyatlar, xususan, kompyuter tizimlariga noqonuniy kirish, axborot resurslarini bloklash, ma'lumotlarni yo'q qilish yoki o'zgartirish

kabi harakatlar fuqarolarning Konstitutsiyada kafolatlangan axborot olish huquqiga bevosita tajovuz qiladi. Shu sababli davlat tomonidan amalga oshiriladigan kiberxavfsizlik choralari nafaqat axborot tizimlarini, balki fuqarolarning konstitutsiyaviy huquqlarini ham himoya qilishga qaratilgan. Mazkur masala xalqaro huquqiy hujjatlarda ham o'z aksini topgan. Jumladan, Inson huquqlari umumjahon deklaratsiyasining 19-moddasi hamda Fuqarolik va siyosiy huquqlar to'g'risidagi xalqaro paktning 19-moddasi har bir insonning axborotni izlash, olish va tarqatish huquqini e'tirof etadi. O'zbekiston ushbu xalqaro standartlarni tan olgan holda ularni milliy qonunchilikka implementatsiya qilgan.

Shaxsiy hayot daxlsizligi va shaxsga doir ma'lumotlarni himoya qilish davlatning asosiy konstitutsiyaviy majburiyati hisoblanadi. Davlat har bir fuqaroning shaxsiy ma'lumotlarini xavfsizligini taminlashi va tashqi xavf va bosimlardan himoya qilishi shart hisoblanadi. Afsuski hozirgi kunda ko'plab fuqarolarni shaxsga doir ma'lumotlari kiberhujumlar tomonidan buzilishi yohud tarqatib yuborilishi mamlakatimizda ko'p kuzatilmoqda. Ayniqsa fuqarolarning rasmlari va passport ma'lumotlaridan foydalanib kiber jinoyatchilar turli xil maqsadlarda foydalanishi hatto rasmlarni fotoshop orqali ming tusga kirgazib tarqarishlari insonning eng ulug' va muborak hisoblangan shani va qadr qimmatiga putur yetkazilish holatlari kuzatilmoqda.

Kiberjinoyatchilikning eng xavfli ko'rinishlaridan biri shaxsga doir ma'lumotlarga noqonuniy tajovuz qilish bilan bog'liqdir. Zamonaviy raqamli texnologiyalar sharoitida fuqarolarning shaxsiy ma'lumotlari elektron bazalarda saqlanadi va qayta ishlanadi. Bu esa mazkur ma'lumotlarning noqonuniy egallanishi, tarqatilishi yoki ulardan g'arazli maqsadlarda foydalanilishi xavfini kuchaytiradi. O'zbekiston Respublikasi Konstitutsiyasining 31-moddasiga ko'ra, har bir shaxsning shaxsiy hayoti daxlsizligi, shaxsiy va oilaviy siri himoya qilinadi. Mazkur norma insonning shaxsiy hayotiga noqonuniy aralashuvdan himoyalaniş huquqining konstitutsiyaviy kafolati hisoblanadi. Bundan tashqari, Konstitutsiyada yozishmalar, telefon orqali so'zlashuvlar, pochta jo'natmalari, elektron xabarlar va boshqa muloqot vositalarining sir saqlanishi kafolatlangan. Ushbu norma zamonaviy axborot texnologiyalari rivojlangan sharoitda alohida ahamiyat kasb etadi. Chunki bugungi kunda shaxsiy muloqotlarning katta qismi elektron pochta, messenjerlar va ijtimoiy tarmoqlar orqali amalga oshirilmoqda. Kiberjinoyatchilar tomonidan elektron pochta hisoblarini buzish, bank kartalari ma'lumotlarini o'g'irlash, shaxsiy fotosurat va hujjatlarni noqonuniy qo'lga kiritish yoki internet tarmoqlarida tarqatish Konstitutsiyaning 31 va boshqa moddalarida nazarda tutilgan huquqlarning buzilishiga olib keladi. Shu bois shaxsiy hayot daxlsizligini ta'minlash kiberxavfsizlik siyosatining ustuvor yo'nalishlaridan biri hisoblanadi. Mazkur huquqlar "Shaxsga doir ma'lumotlar to'g'risida"gi Qonun orqali yanada rivojlantirilgan. Ushbu qonun shaxsga doir ma'lumotlarni yig'ish, saqlash, qayta ishlash va ulardan foydalanishning huquqiy asoslarini belgilaydi hamda ma'lumotlar subyektlarining huquqlarini himoya qilishga

qaratilgan. Xalqaro huquq nuqtayi nazaridan ham shaxsiy hayot daxlsizligi fundamental inson huquqlaridan biri hisoblanadi. Xususan, Inson huquqlari umumjahon deklaratsiyasining 12-moddasi va Fuqarolik va siyosiy huquqlar to'g'risidagi xalqaro paktning 17-moddasi hech kimning shaxsiy va oilaviy hayotiga o'zboshimchalik bilan aralashishga yo'l qo'yilmasligini belgilaydi.

Kiberjinoyatchilikka qarshi kurash davlatning inson huquqlari va xavfsizlikni ta'minlash borasidagi konstitutsiyaviy vazifalaridan kelib chiqadi. Raqamli texnologiyalar jamiyat hayotining barcha sohalariga kirib borgan hozirgi davrda davlatning axborot makonini himoya qilish bo'yicha faoliyati alohida ahamiyat kasb etmoqda. O'zbekiston Respublikasi Konstitutsiyasining 31-moddasida har kimning shaxsiy hayoti daxlsizligi, shaxsiy va oilaviy siri himoya qilinishi, yozishmalar, telefon so'zlashuvlari, pochta, elektron va boshqa xabarlar sir saqlanishi kafolatlangan. Shuningdek, ushbu moddada shaxsga doir ma'lumotlarni himoya qilish huquqi ham mustahkamlangan. Mazkur norma davlat zimmasiga fuqarolarning shaxsiy ma'lumotlarini noqonuniy foydalanish, tarqatish va kiberhujumlardan himoya qilish majburiyatini yuklaydi. Shuningdek, Konstitutsiyaning 33-moddasiga ko'ra, har kim axborotni izlash, olish va tarqatish huquqiga ega. Mazkur modda davlat tomonidan Internet jahon axborot tarmog'idan foydalanish uchun shart-sharoitlar yaratib berilishini ham nazarda tutadi. Shu bois davlat axborot infratuzilmasining barqaror va xavfsiz faoliyatini ta'minlash, axborot resurslarini kiberxurujlardan himoya qilish hamda fuqarolarning axborotdan erkin foydalanish huquqini kafolatlash choralari ko'rishi lozim. Bundan tashqari, Konstitutsiyaning 34-moddasida davlat organlari va tashkilotlarining fuqarolarga ularning huquq va manfaatlariga daxldor bo'lgan hujjatlar, qarorlar va boshqa materiallar bilan tanishish imkoniyatini yaratishi belgilangan. Mazkur norma davlat axborot tizimlarining ishonchliligi va himoyalanganligini ta'minlash zaruratini yuzaga keltiradi. Konstitutsiyaning 81-moddasida ommaviy axborot vositalarining erkinligi, axborotni izlash, olish, undan foydalanish va tarqatish huquqlari kafolatlangan. Raqamli davrda ommaviy axborot vositalarining asosiy faoliyati internet va elektron platformalar orqali amalga oshirilayotganligi sababli davlat ushbu axborot resurslarining kiberxavfsizligini ta'minlash bo'yicha tegishli choralarni ko'rishi zarur. Davlatning mazkur konstitutsiyaviy majburiyatlari "Kiberxavfsizlik to'g'risida"gi Qonun, "Axborotlashtirish to'g'risida"gi Qonun, "Shaxsga doir ma'lumotlar to'g'risida"gi Qonun hamda O'zbekiston Respublikasi Jinoyat kodeksining axborot texnologiyalari sohasidagi jinoyatlarga oid normalarida yanada rivojlantirilgan. Shu bilan birga, davlatning kiberxavfsizlikni ta'minlash bo'yicha faoliyati inson huquqlarini cheklash vositasiga aylanmasligi kerak. Kiberjinoyatchilikka qarshi kurashish choralari Konstitutsiyada belgilangan shaxsiy hayot daxlsizligi, axborot olish erkinligi va boshqa fundamental huquqlar bilan muvozanatda amalga oshirilishi lozim. Aynan ana shunday yondashuv demokratik huquqiy davlatning asosiy mezonlaridan biri hisoblanadi.

O'zbekiston Respublikasida kiberjinoyatchilikka qarshi kurashishning milliy huquqiy mexanizmlari jinoyat huquqi normalari, maxsus kiberxavfsizlik sohasidagi qonunchilik hamda huquqni muhofaza qiluvchi organlarning institutsional faoliyati orqali amalga oshiriladi. Ushbu mexanizmlar raqamli muhitda axborot xavfsizligini ta'minlash, fuqarolarning huquq va erkinliklarini himoya qilish hamda davlatning axborot infratuzilmasini himoyalashga xizmat qiladi. Bugungi kunda axborot texnologiyalarining jadal rivojlanishi jamiyat hayotini tubdan o'zgartirdi. Bank tizimlari, davlat xizmatlari, savdo platformalari va hatto shaxsiy muloqotlar ham raqamli muhitga ko'chdi. Biroq ushbu taraqqiyot bilan bir qatorda yangi xavf — kiberjinoyatchilik ham keskin ortib bormoqda. O'zbekiston Respublikasi Jinoyat kodeksining XX¹-bobi aynan shu munosabatlarni huquqiy tartibga solishga qaratilgan bo'lib, u axborot texnologiyalari sohasida sodir etiladigan jinoyatlar uchun javobgarlikning tizimli asosini yaratadi. Axborot tizimlarining xavfsizligini ta'minlash va qoidalarni buzish (278¹-modda) Axborot tizimlari va ma'lumotlar bazalari bugungi raqamli jamiyatning asosiy infratuzilmasi hisoblanadi. Ularning yaratish, joriy etish va foydalanish jarayonida belgilangan xavfsizlik talablariga amal qilmaslik jiddiy oqibatlariga olib kelishi mumkin. Qonunchilikda bunday holatlar natijasida fuqarolar, davlat yoki jamoat manfaatlariga zarar yetkazilsa, bu jinoyat sifatida baholanadi. Bu norma asosan tizimlarni noto'g'ri tashkil etish, texnik himoya choralariغا beparvolik yoki axborot xavfsizligi standartlariga rioya qilmaslik holatlariga qarshi qaratilgan. Kompyuter axborotiga ruxsatsiz kirish va undan foydalanish (278²-modda).

Kiberjinoyatchilikning eng ko'p uchraydigan shakllaridan biri — bu kompyuter tizimlariga noqonuniy kirishdir. Bunda shaxsiy ma'lumotlar o'g'irlanishi, o'zgartirilishi yoki yo'q qilinishi mumkin. Shuningdek, bu turdagi harakatlar bank tizimlari, davlat portallari yoki yirik korporativ tarmoqlarning ish faoliyatiga ham jiddiy zarar yetkazishi ehtimoli mavjud. Ayniqsa, bunday jinoyatlar bir guruh shaxslar tomonidan yoki xizmat mavqeidan foydalanib sodir etilganda, ularning ijtimoiy xavflilik darajasi yanada ortadi. Kiberjinoyat vositalarini yaratish va tarqatish (278³-modda) Kiberjinoyatlarning oldini olishda muhim jihatlardan biri — ularni amalga oshirish uchun ishlatiladigan vositalarni cheklashdir. Maxsus dasturlar, zararli kodlar yoki ruxsatsiz kirish vositalarini yaratish va tarqatish kiberjinoyatchilikni kengaytiruvchi asosiy omillardan biridir.

Shu sababli qonunchilik faqat jinoyatning o'zini emas, balki uni amalga oshirishga xizmat qiluvchi texnik vositalarni tayyorlash va tarqatishni ham jinoyat sifatida belgilaydi. Axborotni o'zgartirish va kompyuter sabotaji (278⁴–278⁵-moddalar) Axborot tizimlaridagi ma'lumotlarning buzilishi yoki o'zgartirilishi nafaqat texnik muammo, balki huquqiy jihatdan ham og'ir oqibatlariga ega harakat hisoblanadi. Chunki bugungi kunda axborotning aniqligi va ishonchliligi ko'plab qarorlar uchun asos bo'lib xizmat qiladi. Kompyuter sabotaji esa yanada og'irroq jinoyat bo'lib, u tizimlar yoki texnik uskunalarni qasddan ishdan chiqarishga qaratilgan. Bunday harakatlar ko'pincha yirik infratuzilma obyektlariga zarar yetkazishga

yo'naltirilgan bo'ladi. Zararli dasturlar bilan bog'liq jinoyatlar (278⁶-modda) Viruslar va boshqa zararli dasturlar zamonaviy kiberxavfsizlik uchun eng katta tahdidlardan biri hisoblanadi. Ular orqali axborot tizimlariga kirish, ma'lumotlarni yo'q qilish yoki ularni boshqarish imkoniyati paydo bo'ladi. Shu sababli bunday dasturlarni yaratish, ulardan foydalanish yoki tarqatish jinoyat sifatida baholanadi va og'ir javobgarlikni keltirib chiqaradi. Telekommunikatsiya tarmoqlaridan noqonuniy foydalanish (278⁷-modda) Telekommunikatsiya tarmoqlari global axborot almashinuvining asosiy vositasi bo'lib, ulardan noqonuniy foydalanish transmilliy jinoyatlarni keltirib chiqarishi mumkin. Himoya tizimlarini chetlab o'tish, xalqaro trafikni noqonuniy yo'naltirish yoki maxsus vositalarni saqlash kabi harakatlar kiberxavfsizlikka bevosita tahdid soladi. Kripto-aktivlar sohasidagi huquqbuzarliklar (278⁸-modda) Raqamli iqtisodiyotning rivojlanishi kripto-aktivlar sohasini ham huquqiy tartibga solishni talab qildi. Litsenziyasiz faoliyat yuritish, anonim operatsiyalarni amalga oshirish yoki noqonuniy kripto-almashinuvlar moliyaviy tizim xavfsizligiga jiddiy xavf tug'diradi. Shu sababli ushbu sohadagi qonunbuzarliklar ham jinoyat sifatida belgilangan. Firibgarlik va o'g'rilikda axborot texnologiyalarining roli (168–169-moddalar) So'nggi yillarda firibgarlik va o'g'rilik jinoyatlari ham raqamli shaklga o'tdi. Elektron to'lov tizimlari, bank kartalari va internet platformalari orqali sodir etilayotgan jinoyatlar JKning 168 va 169-moddalari doirasida kiberjinoyat sifatida baholanadi. Bu holatlar fuqarolarning mol-mulkiga bevosita zarar yetkazishi bilan birga, raqamli iqtisodiyotga bo'lgan ishonchni ham pasaytiradi.

Mamlakatimizda kiberxavfsizlik choralari ko'rish va sohani rivojlantirish maqsadida 2022-yil 25-fevralda "Kiberxavfsizlik" to'g'risida qonun qabul qilingan. Ushbu qonunning mohiyatini tahlil qiladigan bo'lsak, mazkur Qonunning eng muhim jihati shundaki, u kiberxavfsizlikni faqat texnik masala sifatida emas, balki davlat siyosatining strategik yo'nalishi sifatida belgilaydi. Ya'ni kiberxavfsizlik endilikda alohida tashkilotlarning emas, balki butun davlat tizimining uzviy vazifasi sifatida qaraladi. Qonun axborot tizimlari va axborot resurslarining himoyasini ta'minlash, ularga noqonuniy kirishlarning oldini olish, shuningdek ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini saqlash kabi asosiy prinsiplarni mustahkamlaydi. Bu esa zamonaviy raqamli infratuzilmaning barqaror ishlashi uchun huquqiy kafolat yaratadi. Shuningdek, ushbu Qonun kiberxavfsizlik sohasida davlat organlarining vakolatlarini aniq belgilab beradi. Davlat tomonidan kiberxavfsizlik siyosatini ishlab chiqish, muvofiqlashtirish va nazorat qilish mexanizmlari joriy etiladi. Bu esa turli darajadagi axborot tizimlarida yagona yondashuvni ta'minlashga xizmat qiladi. Qonunning yana bir muhim jihati shundaki, u nafaqat davlat axborot tizimlarini, balki xususiy sektor va fuqarolarning axborot resurslarini ham himoya qilishni ko'zda tutadi.

KIBERJINOYATCHILIKKA QARSHI KURASHISHNING XALQARO-HUQUQIY ASOSLARI

Kiberjinoyatchilik global miqyosda tez sur'atlarda rivojlanib borayotgan zamonaviy xavfsizlik tahdidlaridan biri hisoblanadi. Axborot texnologiyalarining chegarasiz tabiati sababli bunday jinoyatlar bir davlat hududi bilan cheklanib qolmay, bir vaqtning o'zida bir nechta davlat manfaatlariga ta'sir ko'rsatishi mumkin. Shu bois kiberjinoyatchilikka qarshi kurashish faqat milliy darajada emas, balki xalqaro-huquqiy hamkorlik asosida amalga oshiriladi. Xalqaro huquqda kiberjinoyatchilikka qarshi kurash masalalari Xalqaro huquq tizimida kiberjinoyatchilikka qarshi kurashish masalasi axborot xavfsizligini ta'minlash, transmilliy jinoyatchilikni oldini olish hamda davlatlarning raqamli suverenitetini himoya qilish bilan bevosita bog'liqdir.

Kiberjinoyatchilik sohasidagi eng muhim xalqaro hujjatlardan biri bu 2001-yilda qabul qilingan Budapesht konvensiyasi (Kiberjinoyatchilik to'g'risidagi konvensiya) hisoblanadi. Ushbu konvensiya Yevropa Kengashi tomonidan ishlab chiqilgan bo'lib, u kiberjinoyatchilikka qarshi kurashishning huquqiy asoslarini belgilaydi. Konvensiyaning asosiy maqsadi — kompyuter tizimlari orqali sodir etiladigan jinoyatlarni aniqlash, tergov qilish va ularga qarshi samarali huquqiy mexanizmlarni yaratishdir. U quyidagi asosiy yo'nalishlarni qamrab oladi: Birinchidan, kompyuter tizimlariga noqonuniy kirish, ma'lumotlarni o'zgartirish yoki yo'q qilish kabi jinoyatlarni kriminalizatsiya qilish talablarini belgilaydi. Ikkinchidan, dalillarni raqamli shaklda saqlash va ulardan foydalanish bo'yicha protsessual qoidalarni ishlab chiqadi. Bu kiberjinoyatlar bo'yicha tergov jarayonini standartlashtirishga xizmat qiladi. Uchinchidan, xalqaro hamkorlikni kuchaytirish, ya'ni davlatlar o'rtasida tezkor ma'lumot almashish va huquqiy yordam ko'rsatish mexanizmlarini belgilaydi. Budapesht konvensiyasi kiberjinoyatchilikka qarshi kurashishda eng muhim universal hujjatlardan biri bo'lib, ko'plab davlatlar uchun namunaviy huquqiy asos sifatida xizmat qilmoqda.

Xalqaro hamkorlik va davlatlararo huquqiy yordam mexanizmlari Kiberjinoyatchilikning transmilliy tabiati davlatlar o'rtasida yaqin hamkorlikni talab etadi. Xalqaro huquqiy yordam mexanizmlari jinoyatchilarni aniqlash, dalillarni yig'ish va ularni javobgarlikka tortishda muhim ahamiyatga ega. Bunday hamkorlik doirasida davlatlar o'zaro huquqiy yordam so'rovlari (MLA – Mutual Legal Assistance) orqali ma'lumot almashadi, jinoyatchilarni ekstraditsiya qiladi hamda tergov harakatlarini muvofiqlashtiradi. Bundan tashqari, Interpol va boshqa xalqaro tashkilotlar orqali tezkor axborot almashinuvi yo'lga qo'yilgan. Shuningdek, kiberjinoyatchilikka qarshi kurashishda milliy CERT (Computer Emergency Response Team) markazlari ham muhim rol o'ynaydi. Ular kiberhujumlarni aniqlash, tahlil qilish va ularni bartaraf etish bo'yicha xalqaro tarmoqlar bilan hamkorlik qiladi. Xulosa qilib aytganda, kiberjinoyatchilikka qarshi kurashishning xalqaro-huquqiy asoslari davlatlar o'rtasidagi

hamkorlik, Budapesht konvensiyasi va boshqa xalqaro mexanizmlar orqali shakllanib, global axborot xavfsizligini ta'minlashga xizmat qiladi. Bu esa zamonaviy raqamli jamiyatda barqarorlik va xavfsizlikni saqlashning muhim sharti hisoblanadi.

MUHOKAMA

Kiberjinoyatchilikka qarshi kurashish bugungi kunda nafaqat milliy huquq tizimining, balki xalqaro huquqning ham dolzarb yo'nalishlaridan biri hisoblanadi. O'zbekiston Respublikasida ushbu sohada shakllangan normativ-huquqiy baza, xususan Jinoyat kodeksining normalari hamda "Kiberxavfsizlik to'g'risida"gi Qonun kiberjinoyatlarga qarshi kurashishning asosiy huquqiy poydevorini tashkil etadi. Mazkur normalar orqali axborot tizimlariga noqonuniy kirish, zararli dasturlar tarqatish, kompyuter sabotaji va kriptο-aktivlar bilan bog'liq noqonuniy harakatlar uchun javobgarlik belgilangan.

Shu bilan birga, amaliyot tahlili kiberjinoyatchilikka qarshi kurashishda ayrim muammolar mavjudligini ko'rsatadi. Eng asosiy muammolardan biri — kiberjinoyatlarning tezkor o'zgaruvchan xususiyatga ega ekanligidir. Ya'ni jinoyatchilar yangi texnologiyalar va yashirish usullaridan foydalangan holda an'anaviy huquqiy mexanizmlardan tezroq moslashib ketmoqda. Bu esa qonunchilikning doimiy ravishda takomillashtirib borilishini talab etadi.

Ikkinchi muhim masala — raqamli dalillarni to'plash va ularni protsessual jihatdan rasmiylashtirish jarayonidir. Kiberjinoyatlarda asosiy dalillar elektron shaklda bo'lgani uchun ularni yo'qotmasdan saqlash, tahlil qilish va sudga taqdim etish alohida texnik bilim va zamonaviy ekspertiza imkoniyatlarini talab qiladi. Ayrim hollarda esa ushbu texnik imkoniyatlarning yetarli darajada emasligi tergov jarayonini murakkablashtiradi.

Shuningdek, xalqaro tajriba shuni ko'rsatadiki, kiberjinoyatchilik transmilliy xarakterga ega bo'lgani sababli davlatlar o'rtasidagi hamkorlik hal qiluvchi ahamiyatga ega. Budapesht konvensiyasi kiberjinoyatlarga qarshi kurashishning xalqaro standartini belgilab bergan bo'lsa-da, amaliyotda huquqiy yordam so'rovlari va ma'lumot almashish jarayonlarida ba'zan kechikishlar kuzatiladi. Bu esa jinoyatlarni tezkor fosh etishga salbiy ta'sir ko'rsatadi.

Bundan tashqari, jamiyatda kiberxavfsizlik bo'yicha huquqiy ong va madaniyat darajasi ham yetarli emasligi dolzarb muammo bo'lib qolmoqda. Fuqarolarning shaxsiy ma'lumotlarini himoya qilish, firibgarlik sxemalaridan saqlanish va internetdan xavfsiz foydalanish bo'yicha bilimlari yetarli darajada shakllanmaganligi kiberjinoyatlar sonining oshishiga olib kelmoqda. Mazkur muammolarni bartaraf etish uchun bir qator takliflarni ilgari surish mumkin. Jumladan, kiberjinoyatlar bo'yicha maxsuslashtirilgan ekspert-kriminalistika markazlarini rivojlantirish, raqamli tergov (digital forensics) imkoniyatlarini kengaytirish hamda huquqni muhofaza qiluvchi organlarning texnik bazasini modernizatsiya qilish zarur. Shuningdek, xalqaro hamkorlikni yanada tezkor va samarali qilish, ayniqsa transchegaraviy ma'lumot almashinuvi mexanizmlarini soddalashtirish muhim hisoblanadi.

Eng asosiy jihatlariga yana e'tibor qaratsak pul inson uchun eng zarur resurs hisoblanadi fuqarolardan noqonuniy tarzda plastik yoki kredit kartalardan pul yechib olinishi bu eng katta fuqarolarga zarar hisoblanadi. Afsuski fuqarolar bu holatda hech nima qila olishmaydi. Hozirgi asosiy taklif shundan iboratki fuqarolarga kompensatsiya masalasidir. Bank tizimi xavfsizlik jihatdan kuchki bo'lish kerak hakkerlar tomonidan yechib olinga har bir so'm bank tomonidan qaysidir qismi qoplanishi yoki to'liq qoplanishi kerak shunda bank va mijoz o'rtasidagi munosabatga putur yetmaydi.

Kiberjinoyatlar to'g'risidagi konvensiya milliy qonunlarni uyg'unlashtirish, tergov usullarini takomillashtirish va davlatlar o'rtasidagi hamkorlikni oshirish orqali Internet va kompyuter jinoyatlarini kiber jinoyatlar hal qilishga qaratilgan birinchi xalqaro shartnomadir. U Fransiyaning Strasburg shahrida Yevropa Kengashi tomonidan Yevropa Kengashining kuzatuvchi bir qancha davlatlari Kanada, Yaponiya, Filippin, Janubiy Afrika va AQShning faol ishtirokida ishlab chiqilgan. Konvensiya va uning tayyorlangan hisoboti Yevropa Kengashi Vazirlar Qo'mitasi tomonidan 2001-yil 8-noyabrdagi 109-sessiyasida qabul qilingan. 2001-yil 23-noyabrda Vengriya poytaxti Budapeshtda imzolash uchun chaqirilgan va 2004-yil 1-iyuldan boshlab kuchga kirgan. 2020-yil dekabr holatiga ko'ra, 65 davlat konvensiyani ratifikatsiya qilgan, yana to'rtta davlat konvensiyani imzolagan, ammo uni ratifikatsiya qilmagan. Bu kiberjinoyatchilikni tartibga soluvchi birinchi ko'p tomonlama qonuniy majburiy vositadir. 2018-yildan beri Hindiston kiberjinoyatlar avj olganidan keyin Konvensiyaga nisbatan o'z pozitsiyasini qayta ko'rib chiqmoqda. Ammo xorijiy agentliklar bilan ma'lumot almashish bo'yicha xavotirlar saqlanib qolmoqda. 2006-yil 1-martda Kiberjinoyat to'g'risidagi konvensiyaga qo'shimcha protokol kuchga kirdi. Qo'shimcha protokolni ratifikatsiya qilgan davlatlar kompyuter tizimlari orqali irqchilik va ksenofobik materiallarni, shuningdek, irqchilik yoki ksenofobiya asosidagi tahdid va haqoratlarni tarqatish uchun jinoiy javobgarlikka tortilishi kerak.

Konvensiya Internet va boshqa kompyuter tarmoqlari orqali sodir etilgan jinoyatlar to'g'risidagi birinchi xalqaro shartnoma bo'lib, ayniqsa mualliflik huquqining buzilishi, kompyuter bilan bog'liq firibgarlik, bolalar pornografiyasi, nafrat jinoyatlari va tarmoq xavfsizligini buzish bilan bog'liq. Shuningdek, u kompyuter tarmoqlarini qidirish, topish, qo'lga kiritish va qonuniy ravishda jazolash kabi bir qator vakolatlar va tartiblarni o'z ichiga oladi. Uning muqaddimada bayon etilgan asosiy maqsadi jamiyatni kiberjinoyatlardan himoya qilishga qaratilgan umumiy jinoiy siyosatni olib borish, ayniqsa tegishli qonun hujjatlarini qabul qilish va xalqaro hamkorlikni rivojlantirishdan iborat.

Konvensiyada quyidagi jinoyatlar belgilangan: noqonuniy kirish, noqonuniy qo'lga olish, ma'lumotlarga aralashuv, tizimga aralashuv, qurilmalardan noto'g'ri foydalanish, kompyuter bilan bog'liq qalbakilashtirish, kompyuter bilan bog'liq firibgarlik, bolalar pornografiyasi bilan bog'liq huquqbuzarliklar, mualliflik huquqi va qo'shni huquqlar bilan bog'liq

huquqbuzarliklar. Shuningdek, u saqlangan ma'lumotlarni tezkor saqlash, trafik ma'lumotlarini tezkor saqlash va qisman oshkor qilish, ishlab chiqarish tartibi, kompyuter ma'lumotlarini qidirish va olib qo'yish, trafik ma'lumotlarini real vaqt rejimida yig'ish va kontent ma'lumotlarini qo'lga kiritish kabi protsessual huquqiy masalalarni belgilaydi. Bundan tashqari, Konvensiyada saqlanadigan kompyuter ma'lumotlariga o'zaro yordamni talab qilmaydigan transchegaraviy kirishning ma'lum bir turi to'g'risidagi qoida mavjud (rozilik bilan yoki hamma uchun mavjud bo'lganda) va tezkorlikni ta'minlash uchun 24/7 tarmoqni o'rnatishni nazarda tutadi. Bundan tashqari, shartlar va kafolatlar sifatida Konvensiya inson huquqlari va erkinliklarini, shu jumladan Inson huquqlari to'g'risidagi Yevropa konvensiyasi, Fuqarolik va siyosiy huquqlar to'g'risidagi xalqaro pakt va boshqa amaldagi inson huquqlari bo'yicha xalqaro hujjatlardan kelib chiqadigan majburiyatlardan kelib chiqadigan huquqlarni munosib himoya qilishni ta'minlashni talab qiladi va mutanosiblik tamoyilini o'z ichiga oladi. Konvensiya Yevropa va xalqaro ekspertlarning to'rt yillik mehnati mahsulidir. U kompyuter tarmoqlari orqali irqchilik va ksenofobiya tashviqotining har qanday nashrini jinoiy tuhmat to'g'risidagi qonunlarga o'xshash jinoiy javobgarlikka tortuvchi qo'shimcha protokol bilan to'ldirildi. Hozirda konvensiya doirasida kiberterrorizm ham o'rganilmoqda. Xulosa qilib aytganda, kiberjinoiyatchilikka qarshi kurashish tizimi kompleks yondashuvni talab etadi. Bu jarayonda nafaqat huquqiy baza, balki texnik infratuzilma, xalqaro hamkorlik va fuqarolarning huquqiy savodxonligi ham muhim rol o'ynaydi. Shu jihatdan, mavjud tizimni yanada takomillashtirish zamonaviy raqamli jamiyat barqarorligini ta'minlashning asosiy shartlaridan biri hisoblanadi.

XULOSA

Kiberjinoiyatchilik zamonaviy axborot jamiyatining eng dolzarb va murakkab muammolaridan biri bo'lib, u davlat, jamiyat va shaxs manfaatlariga bevosita tahdid soladi. Axborot texnologiyalarining jadal rivojlanishi bilan bir qatorda kiberjinoiyatlar ham yangi ko'rinish va usullar orqali namoyon bo'lmoqda. Bu esa ularni aniqlash, oldini olish, tergov qilish va huquqiy baholash jarayonlarini yanada murakkablashtirmoqda.

Tahlillar shuni ko'rsatadiki, O'zbekiston Respublikasida kiberjinoiyatchilikka qarshi kurashishning huquqiy asoslari izchil shakllanmoqda. Xususan, O'zbekiston Respublikasi Jinoyat kodeksining tegishli normalari hamda "Kiberxavfsizlik to'g'risida"gi Qonun ushbu sohadagi asosiy normativ-huquqiy bazani tashkil etadi. Mazkur hujjatlar axborot tizimlariga noqonuniy kirish, kompyuter sabotaji, zararli dasturlarni yaratish va tarqatish, shuningdek, kripto-aktivlar bilan bog'liq huquqbuzarliklar uchun javobgarlikni belgilab beradi. Shu bilan birga, kiberjinoiyatlarning transmilliy xarakteri, raqamli dalillar bilan ishlashdagi texnik murakkabliklar hamda xalqaro huquqiy yordam mexanizmlarining ba'zan yetarli darajada tezkor ishlamasligi ushbu yo'nalishda hal etilishi lozim bo'lgan muhim muammolar sifatida

namoyon bo‘lmoqda. Bu esa kiberjinoyatchilikka qarshi kurashish tizimini doimiy ravishda takomillashtirish zarurligini ko‘rsatadi.

Hozirgi globallashuv va raqamli transformatsiya sharoitida jamiyat hayotining deyarli barcha sohaları axborot-kommunikatsiya texnologiyalari bilan uzviy bog‘lanib bormoqda. Davlat xizmatlari, bank-moliya tizimi, ta’lim, sog‘liqni saqlash, elektron tijorat va shaxsiy muloqot vositalarining raqamli platformalarga ko‘chishi fuqarolar uchun qulayliklar yaratish bilan birga, yangi turdagi kiberxavflarni ham yuzaga keltirmoqda. Ayniqsa, bank kartalaridan noqonuniy pul yechib olish, shaxsiy ma’lumotlardan foydalangan holda kredit rasmiylashtirish, ijtimoiy tarmoq profililarini egallab olish, phishing havolalar orqali maxfiy ma’lumotlarni qo‘lga kiritish kabi holatlar fuqarolarning mulkiy manfaatlari va shaxsiy hayoti daxlsizligiga jiddiy zarar yetkazmoqda.

Umuman olganda, kiberjinoyatchilikka qarshi kurashish faqat huquqni muhofaza qiluvchi organlarning vazifasi emas, balki davlat, jamiyat, xususiy sektor va har bir fuqaroning umumiy mas’uliyati hisoblanadi. Mazkur sohada samaradorlikka erishish uchun normativ-huquqiy bazani doimiy takomillashtirish, huquqni muhofaza qiluvchi organlarning texnik va ekspertlik salohiyatini oshirish, bank-moliya tizimlarida kiberxavfsizlik talablarini kuchaytirish, fuqarolarning raqamli savodxonligini yuksaltirish hamda kiberxavfsizlik madaniyatini shakllantirish muhim ahamiyatga ega. Shu jihatdan, kiberjinoyatchilikka qarshi kurashish O‘zbekiston Respublikasida axborot xavfsizligini ta’minlash, fuqarolarning konstitutsiyaviy huquqlarini himoya qilish va raqamli iqtisodiyot barqarorligini mustahkamlashning muhim sharti sifatida baholanishi lozim.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Kiber huquq – huquq sohasi sifatida: risola / tuzuvchilar R.R.Shakurov, M.M.Vohidov. – Toshkent: O‘zbekiston Respublikasi Adliya vazirligi qoshidagi Yuristlar malakasini oshirish markazi, 2022. – 3-10 b.
2. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni.
3. O‘zbekiston Respublikasi Jinoyat kodeksi.
4. United Nations Office on Drugs and Crime (UNODC) – Comprehensive Study on Cybercrime.
5. “Convention on Cybercrime, Budapest, 23 November 2001”.
6. Budapesht konvensiyasi (Convention on Cybercrime), 2001-yil, Yevropa Kengashi.
7. O‘zbekiston Respublikasining “Axborotlashtirish to‘g‘risida”gi Qonuni.
8. O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni.
9. ITU (International Telecommunication Union). Global Cybersecurity Index (GCI) Reports.
10. O‘zbekiston Respublikasi Konsitutsiyasi 2023
11. www.gazeta.uz/oz/tag/iivkiberxavfsizlikmarkazi/