

**“RAQAMLI XAVFSIZLIK TAHDIDI SIFATIDA
KIBERTERRORIZM: O`ZBEKISTON TAJRIBASI VA HUQUQIY
MEXANIZMLAR”**

Abdurahmonova Zahroxon Tohir qizi
Axadova Durdona Abdifoil qizi
*SHDPI Filologiya fakulteti Xorijiy til
va adabiyoti yo`nalishi talabalari*

Annotatsiya: *Ushbu maqolada raqamli asr muammolari, raqamli xavfsizlik hamda kiberterrorizmning tahdidilari sababi o`rganildi va O`zbekiston tajribasi bilan bir qatorda huquqiy mexanizmlari tahlil qilindi.*

**Kalit so`zlar:** *Raqamli asr muammolari, kiberterrorizm, O`zbekiston tajribasi, huquqiy mexanizmlar, kiberterrorizmga qarshi choralar.*

**"КИБЕРТЕРРОРИЗМ КАК УГРОЗА ЦИФРОВОЙ БЕЗОПАСНОСТИ:
ОПЫТ УЗБЕКИСТАНА И ПРАВОВЫЕ МЕХАНИЗМЫ"**

Абдурахмонова Захрохон Тохир кызы
Ахадова Дурдона Абдифозил кызы
*Факультет филологии, иностранных языков, ШХДПИ
и студенты-литературоведы*

Аннотация: *В статье рассматриваются проблемы цифровой эпохи, причины нарушения цифровой безопасности и угрозы кибертерроризма, анализируются правовые механизмы, а также опыт Узбекистана.*

Ключевые слова: *Проблемы цифровой эпохи, кибертерроризм, опыт Узбекистана, правовые механизмы, меры противодействия кибертерроризму.*

**CYBERTERRORISM AS A THREAT TO DIGITAL SECURITY:
UZBEKISTAN'S EXPERIENCE AND LEGAL MECHANISMS**

Abdurakhmonova Zahrokhon Tohir qizi
Akhadova Durdona Abdifoil qizi
*Students of the Faculty of Philology,
Foreign Languages and Literature*

Annotation: *This article examines the problems of the digital age, the causes of the threats of digital security and cyberterrorism, and analyzes the legal mechanisms, along with the experience of Uzbekistan.*

Keywords: *Problems of the digital age, cyberterrorism, Uzbekistan's experience, legal mechanisms, measures against cyberterrorism.*

XXI asr – axborot texnologiyalari asridir. Insoniyat taraqqiyoti, ijtimoiy hayot, siyosiy boshqaruv, iqtisodiy faoliyat va madaniy almashinuv internet va raqamli texnologiyalar orqali amalga oshirilmoqda. Shu bilan birga, axborot maydonining kengayishi nafaqat qulayliklar, balki xavf-xatarlarni ham keltirib chiqarmoqda. Bunday tahdidlardan biri – kiberterrorizmdir. Mazkur maqolada kiberterrorizm tushunchasi, uning asosiy ko‘rinishlari, O‘zbekiston hududida mavjud bo‘lgan xavflar, shuningdek, unga qarshi kurashishda amalga oshirilayotgan choralar tahlil qilinadi. 1. Kiberterrorizm tushunchasi va uning mohiyati: Kiberterrorizm — bu axborot texnologiyalaridan foydalangan holda jamiyatda qo‘rquv, vahima, ijtimoiy beqarorlik, iqtisodiy izdan chiqish va davlat boshqaruv tizimiga zarar yetkazish maqsadida amalga oshiriladigan tahdidli harakatlardir. Jahon amaliyotida bu tushuncha quyidagi shakllarda namoyon bo‘ladi: Hukumat veb-saytlarini buzish (deface qilish); Energetika, transport yoki bank tizimlariga zarar yetkazish; Ijtimoiy tarmoqlar orqali terroristik targ‘ibot yuritish; Dasturiy tahdidlar (viruslar, fishing, DDOS hujumlar) orqali infratuzilmalarni ishdan chiqarish. 2. Kiberterrorizmning O‘zbekistondagi tahdid darajasi⁶: O‘zbekiston Respublikasi Prezidenti Sh.M.Mirziyoyev ta’kidlaganidek, “Yangi O‘zbekiston”da xavfsizlik masalasi davlat siyosatining ustuvor yo‘nalishlaridan biridir. So‘nggi yillarda raqamli texnologiyalar keng joriy qilinayotgan bir vaqtda, ularni nazorat qilish, axborot xavfsizligini ta’minlash, kiberjinoatlarning oldini olish dolzarb ahamiyat kasb etmoqda. O‘zbekiston Respublikasi Ichki ishlar vazirligi va Milliy gvardiya axborot xavfsizligini ta’minlashda faoliyat olib bormoqda. Bundan tashqari, 2020-yilda qabul qilingan “Kiberxavfsizlik konsepsiyasi” asosida barcha davlat tashkilotlari axborot resurslarining muhofazasini kuchaytirishga majbur qilindi.

3. Kiberterrorizmga qarshi kurashishning huquqiy asoslari; O‘zbekistonda kiberterrorizmga qarshi kurash quyidagi normativ-huquqiy hujjatlar asosida olib borilmoqda: O‘zbekiston Respublikasi Jinoyat kodeksi – 155-modda (terrorchilik), 278-modda (ommaviy tartibsizliklar), 244-modda (ekstremistik materiallarni tarqatish) orqali kiberterrorizm bilan bog‘liq jinoyatlar uchun jinoiy javobgarlik belgilangan. “Axborotlashtirish to‘g‘risida”gi Qonun – axborot resurslari xavfsizligini

⁶ O‘zbekiston Respublikasi Prezidentining 2020-yil 6-oktabrdagi PQ-4851-sonli Qarori – “Kiberxavfsizlikni ta’minlash chora-tadbirlari to‘g‘risida”

ta'minlash choralari belgilangan. "Elektron hukumat" to'g'risidagi Qonun – davlat idoralarining raqamli tizimlaridan foydalanish va ularni himoya qilish mexanizmlarini belgilaydi⁷. Adabiyot manbalarida (masalan, O'zbekiston Respublikasi Fanlar akademiyasi nashrlari, Bosh prokuratura akademiyasi ilmiy to'plamlari) keltirilishicha, O'zbekistonda aynan diniy ekstremistik guruhlar tomonidan ijtimoiy tarmoqlar orqali yollash va targ'ibot yuritish holatlari qayd etilgan. 4. O'zbekistonda kiberxavfsizlik tizimini takomillashtirish yo'llari: Kiberterrorizmga qarshi samarali kurashish uchun quyidagi yo'nalishlarda ish olib borish muhimdir:

1. Raqamli savodxonlikni oshirish – aholining, ayniqsa yoshlarning internetdan ongli foydalanishini ta'minlash.

2. Texnik himoya vositalarini takomillashtirish – Dasturiy va apparat himoya vositalari (antivirus, kriptografiya, sun'iy intellekt asosidagi himoya).

3. Huquqiy baza va xalqaro hamkorlikni kengaytirish – MDH va boshqa xalqaro tashkilotlar bilan axborot almashinuvini yo'lga qo'yish.

4. Maxsus kadrlar tayyorlash – Axborot xavfsizligi, kiberxavfsizlik sohalarida malakali mutaxassislar yetishtirish (masalan, TATU, AKT universitetlari huzurida). Shu o'rinda yurtimizda kiberterrorizmni oldini olish bo'yicha ma'lum bir chora-tadbirlar olib borilmoqda:

1. O'zbekiston Respublikasidagi huquqiy-me'yoriy manbalar asosida: "Axborotlashtirish to'g'risida"gi Qonun (2003-yil) – bu qonun axborot tizimlari va resurslarini shakllantirish, foydalanish va himoya qilish asoslarini belgilaydi. Kiberxavfsizlikni ta'minlash shu qonun doirasida muhim o'rin egallaydi. "Axborot xavfsizligi konsepsiyasi" (2018-yil) – bu hujjatda axborot makonida vujudga kelayotgan tahdidlar, xususan, kiberterrorizm, kiberjinoyat, axborot urushi kabi tushunchalarga aniqlik beriladi. Unga ko'ra, axborot xavfsizligi milliy xavfsizlikning tarkibiy qismidir. "Kiberxavfsizlikni ta'minlash konsepsiyasi" (2020-yil, Prezident qarori bilan) – bu konsepsiya O'zbekistonda axborot va kommunikatsiya texnologiyalarining rivojlanishi bilan bog'li xatarlarni minimallashtirish, kiberxavfsizlik sohasida samarali choralarni ishlab chiqishni nazarda tutadi. Cyber Security Center (Raqamli texnologiyalar vazirligi qoshida) – O'zbekistonning kiberxavfsizlik infratuzilmasini boshqaruvchi markaziy organ bo'lib, hukumat tizimlarini himoya qilish, xavf tahlilini yuritish, profilaktik choralar ko'rish bilan shug'ullanadi. Kiberterrorizm va yoshlar: ijtimoiy-psixologik xavflar to'g'risida so'z yuritamiz: Zamonaviy dunyoda yoshlar internet tarmog'ida eng faol qatlam hisoblanadi. Bu esa kiberterroristik guruhlar uchun maqsadli auditoriyani tashkil etadi. Ayrim guruhlar yoshlarni quyidagi usullar orqali radikal

⁷ Karimov, B. (2020). Terrorizm va ekstremizm: zamonaviy tahdidlar va ularga qarshi kurash. Toshkent: Yuridik adabiyotlar nashriyoti.

qarashlarga og‘dirishga urinadi: Soxta diniy, mafkuraviy materiallar orqali ongini zaharlash; “Adolat”, “ozodlik”, “qahramonlik” singari tushunchalarni buzib talqin qilish; Virtual guruhlar orqali o‘z fikrlarini singdirish (masalan, Telegram, Dark Web forumlari orqali). O‘zbekiston milliy xavfsizlik tizimida kiberxavfsizlikning o‘rni oxirgi vaqtlarda ortib bormoqda. Milliy xavfsizlikni ta’minlashda raqamli muhitni himoya qilish – asosiy yo‘nalishlardan biri sifatida qaralmoqda. 2022-yil 1-noyabrda Prezident Sh.M. Mirziyoyev raisligida o‘tkazilgan yig‘ilishda quyidagilar ta’kidlangan: “Axborot makonida mafkuraviy kurash kuchaymoqda. Raqamli himoya – bu shunchaki texnologiya emas, bu milliy barqarorlikning asosi.” Shu munosabat bilan quyidagi tashabbuslar yo‘lga qo‘yilgan:⁸ Milliy kibermakon monitoringi – davlat organlari va muhim infratuzilmalar tarmoqlarining doimiy nazorati; Kiber xavfsizlikka oid milliy malaka oshirish kurslari – IIV, DXX, Raqamli texnologiyalar vazirligi tomonidan tashkil etiladi. Xulosa o‘rnida ta’kidlash joizki: Kiberterrorizm bugungi raqamli davrning eng xavfli tahdidlaridan biri bo‘lib, unga qarshi kurashda davlat siyosatining uzviy qismi sifatida kompleks chora-tadbirlar zarur. O‘zbekistonda bu borada muayyan huquqiy, institutsional va texnik asoslar yaratilgan bo‘lsa-da, xavf doimiy ravishda yangilanib borayotganligi bois, doimiy monitoring, ta’lim, profilaktika va xalqaro hamkorlik zarur. Yurtimizda raqamli xavfsizlikni ta’minlash orqali davlatimiz barqarorligiga xizmat qiladigan asosiy tayanch mustahkamlanadi.

FOYDALANILGAN ADABIYOTLAR

1. Qodirov, S. (2021). Axborot xavfsizligi va kiberxavfsizlik muammolari. Toshkent: Innovatsion rivojlanish nashriyoti.
2. Karimov, B. (2020). Terrorizm va ekstremizm: zamonaviy tahdidlar va ularga qarshi kurash. Toshkent: Yuridik adabiyotlar nashriyoti.
3. O‘zbekiston Respublikasi Prezidentining 2020-yil 6-oktabrdagi PQ-4851-sonli Qarori – “Kiberxavfsizlikni ta’minlash chora-tadbirlari to‘g‘risida”.
4. Hasanov, M., & Nuriddinov, A. (2019). Axborot texnologiyalari va jamiyat xavfsizligi. Toshkent: Fan va texnologiya nashriyoti.
5. Xudayberganov, U. (2022). “Kiberjinoyatchilik va unga qarshi kurashning huquqiy asoslari”. Ijtimoiy fanlar jurnali, 3(1), 44–52.
6. Turg‘unov, Sh. (2021). “Zamonaviy tahdidlar: kiberterrorizm va axborot urushi”. Milliy xavfsizlik muammolari jurnali, 5(2), 60–68.
7. O‘zbekiston Respublikasi Jinoyat kodeksi (amaldagi tahrirda), 27-bob: Axborot xavfsizligiga qarshi jinoyatlar.
8. Rasulov, J. (2020). Globallashuv va axborot tahdidlari. Samarqand: Iqtisodiyot va fan.

⁸ Turg‘unov, Sh. (2021). “Zamonaviy tahdidlar: kiberterrorizm va axborot urushi”. Milliy xavfsizlik muammolari jurnali, 5(2), 60–68.