KIBERJINOYATLAR VA ULARNING OLDINI OLISHNING HUQUQIY ASOSLARI

Termiz Davlat Universiteti Yuridik fakulteti
2-bosqich talabasi ***Rayxona Raxmonova Nabijon qizi***

Annotatsiya : Ushbu ilmiy maqola kiberjinoyatlarning zamonaviy jamiyat uchun tahdid sifatidagi dolzarbligini tahlil qiladi va ularning oldini olish hamda ularga qarshi kurashishning huquqiy asoslarini O'zbekiston Respublikasi kontekstida atroflicha ko'rib chiqadi. Maqolada kiberjinoyatlarning mohiyati, turlari va global miqyosdagi ta'siri baholanib, ularning iqtisodiy zarari va ijtimoiy xavfi yoritiladi. Shuningdek, xalqaro huquqiy tartibga solish mexanizmlari, jumladan, global hamkorlikning ahamiyati ta'kidlanadi. O'zbekistonda kiberjinoyatlarga qarshi kurash bo'yicha qabul qilingan qonun hujjatlari va normativ-huquqiy bazalar tizimli tahlil qilinib, mavjud kamchiliklar va takomillashtirish yo'nalishlari aniqlanadi. Elektron dalillarni tergov qilish, sudga oshirish va ulardan foydalanishning huquqiy jihatlari ham muhokama qilinadi. Maqola kiberjinoyatlar profilaktikasining huquqiy mexanizmlarini mustahkamlash, milliy strategiyani ishlab chiqish va xalqaro tajribani tatbiq etish bo'yicha takliflar bilan yakunlanadi.

Kalit so‘zlar: Kiberjinoyat, kiberxavfsizlik, huquqiy asoslar, O'zbekiston, elektron dalillar, profilaktika, xalqaro hamkorlik

Abstract: This scientific article analyzes the urgency of cybercrimes as a threat to modern society and thoroughly examines the legal frameworks for their prevention and combat in the context of the Republic of Uzbekistan. The article evaluates the nature, types, and global impact of cybercrimes, highlighting their economic damage and social danger. It also emphasizes international legal regulation mechanisms, including the importance of global cooperation. Legal acts and normative-legal bases adopted in Uzbekistan for combating cybercrimes are systematically analyzed, identifying existing shortcomings and directions for improvement. Legal aspects of investigating, prosecuting, and using electronic evidence are also discussed. The article concludes with proposals for strengthening legal mechanisms for cybercrime prevention, developing a national strategy, and implementing international experience.

Keywords: Cybercrime, cybersecurity, legal frameworks, Uzbekistan, electronic evidence, prevention, international cooperation

Аннотация: Данная научная статья анализирует актуальность киберпреступлений как угрозы для современного общества и всесторонне рассматривает правовые основы их предотвращения и борьбы с ними в контексте Республики Узбекистан. В статье оцениваются сущность, виды и глобальное воздействие киберпреступлений, освещаются их экономический ущерб и

социальная опасность. Также подчеркивается значение механизмов международного правового регулирования, включая глобальное сотрудничество. Систематически анализируются принятые в Узбекистане законодательные акты и нормативно-правовые основы по борьбе с киберпреступлениями, выявляются существующие недостатки и направления для совершенствования. Обсуждаются также правовые аспекты расследования, судебного преследования и использования электронных доказательств. Статья завершается предложениями по укреплению правовых механизмов профилактики киберпреступлений, разработке национальной стратегии и применению международного опыта.

Ключевые слова: Киберпреступность, кибербезопасность, правовые основы, Узбекистан, электронные доказательства, профилактика, международное сотрудничество

Raqamli texnologiyalarning jadal rivojlanishi zamonaviy jamiyat hayotining barcha jabhalariga sezilarli ta'sir ko'rsatmoqda. Internet va axborot-kommunikatsiya texnologiyalari iqtisodiyotni, boshqaruvni va ijtimoiy aloqalarni tubdan o'zgartirib, keng imkoniyatlar ochmoqda. Biroq, bu rivojlanish bilan birga, yangi turdagi tahdidlar ham paydo bo'ldi, ulardan eng xavflisi kiberjinoyatchilikdir. Kiberjinoyatlar deganda, kompyuterlar va tarmoqlar qurol sifatida ishlatiladigan yoki ularga qaratilgan, xavfsizlik va moliyaga zarar yetkazishga qaratilgan har qanday jinoiy faoliyat tushuniladi. Ular josuslik, moliyaviy o'g'irlik va boshqa transchegaraviy huquqbuzarliklarni qamrab oladi, ayrim transmilliy hodisalar hatto kiberurush deb ataladi. Uorren Baffetning so'zlariga ko'ra, bu "insoniyatning birinchi raqamli muammosi" bo'lib, "haqiqiy tahdid" tug'diradi.

Kiberjinoyatchilikning iqtisodiy ta'siri nihoyatda katta. McAfee kompaniyasining 2014 yilgi hisobotida global miqyosda yillik zarar 445 milliard dollarga baholangan edi. Cybersecurity Ventures agentligi esa global yo'qotishlar 2021 yilga kelib 6 trillion dollarga, 2025 yilga kelib esa 10,5 trillion dollarga yetishini prognoz qilgan. 2018 yilda CSIS va McAfee hamkorligida o'tkazilgan tadqiqotga ko'ra, global yalpi ichki mahsulotning qariyb 1 foizi, ya'ni taxminan 600 milliard dollar har yili kiberjinoyatchilik tufayli yo'qotiladi. Kiberjinoyatlar moliyaviy firibgarlik (masalan, ma'lumotlarni ruxsatsiz o'zgartirish, shaxsiyatni o'g'irlash), kiberterrorizm (siyosiy yoki ijtimoiy majburlash maqsadida hujumlardan foydalanish) va kiber tovlamachilik (hujumchilardan buzuvchi hujumlarni, masalan, xizmat ko'rsatishni rad etish yoki ransomware hujumlarini to'xtatish uchun to'lov talab qilish) kabi turlarni o'z ichiga oladi. Jahon Iqtisodiy Forumining 2020 yilgi hisobotida uyushgan kiberjinoyatchilikning o'sishi qayd etilib, AQShda uni aniqlash va jinoiy javobgarlikka tortish darajasi 1 foizdan past ekanligi ta'kidlangan.

O'zbekiston ham kiberxavfsizlik borasida jiddiy zaifliklarga duch kelmoqda va xalqaro baholashlarda doimiy ravishda past o'rinlarni egallab keladi. Comparitech tadqiqotiga ko'ra, O'zbekiston kripto-konchilar tomonidan eng ko'p nishonga olinadigan mamlakat sifatida aniqlangan bo'lib, 60 davlat orasida 56-o'rinni egallagan. Kiberxavfsizlikka ta'sir qilish indeksi (CEI) ham O'zbekistonni 108 mamlakat orasida 70-o'rinda baholagan. 2020 yildagi monitoring natijalariga ko'ra, milliy internet segmentida 27 milliondan ortiq zararli tarmoq hodisasi qayd etilgan, davlat va iqtisodiy boshqaruv saytlariga hujumlar 144 foizga oshgan. Garchi O'zbekistonning Global kiberxavfsizlik indeksi (GCI) reytingi 2017 yildagi 93-o'rindan 2021 yilda 70-o'ringa ko'tarilgan bo'lsada, qonunchilik va tayyorgarlik jihatlarida hali ham orqada qolmoqda. Mutaxassislar ushbu muammolarni keng qamrovli davlat kiberxavfsizlik siyosati, milliy strategiya, doimiy monitoringning yo'qligi hamda rejalashtirilgan huquqiy asoslarni shakllantirishdagi kechikishlar bilan izohlamoqdalar. Shu nuqtai nazardan, ushbu maqola kiberjinoyatlarga qarshi kurashning huquqiy asoslarini tizimli tahlil qilish, mavjud muammolarni aniqlash va ularni hal etish bo'yicha takliflar ishlab chiqishni maqsad qilgan. Shuningdek, kiberjinoyatlarning huquqiy asoslari bo'yicha ilmiy tadqiqotlar jahon miqyosida faol olib borilmoqda. Ko'plab xalqaro tashkilotlar, jumladan, Birlashgan Millatlar Tashkiloti, Yevropa Kengashi, Interpol va Yevropol kiberjinoyatchilikka qarshi kurash bo'yicha qator dasturlar va konvensiyalarni ishlab chiqqan. Jumladan, Budapesht konvensiyasi (Kiberjinoyatlar bo'yicha konvensiya) xalqaro huquqiy hamkorlikning asosiy instrumentlaridan biri hisoblanadi. Ushbu hujjatlar kiberjinoyatlarning turlarini aniqlash, ularga qarshi kurashishda davlatlararo hamkorlikni kuchaytirish va tergov jarayonlarini unifikatsiya qilishga qaratilgan. Xalqaro miqyosdagi adabiyotlarda kiberjinoyatlarning iqtisodiy, ijtimoiy va siyosiy oqibatlari, ularning turlari va paydo bo'lish sabablari atroflicha o'rganilgan. Ayniqsa, kiberterrorizm, ma'lumotlar o'g'irlanishi va infratuzilmalarga qilingan hujumlarning tahdidi alohida e'tiborga molik.

O'zbekistonda esa kiberjinoyatchilik va uning huquqiy tartibga solinishi bo'yicha ilmiy adabiyotlar, xususan, tizimli tadqiqotlar nisbatan kamroq. Garchi "Kiber jinoyatchilik va kiber qonunlar" kabi ayrim raqamli hujjatlar mavjud bo'lsada, ularning ilmiy qimmati va ekspertlar tomonidan baholanishi cheklangan. Ushbu turdagi materiallar ko'pincha ilmiy hamjamiyat tomonidan tan olingan ekspertizadan o'tmaydi va ularning foydalilik darajasi nol foiz bo'lib qoladi. Bu esa mamlakatda kiberjinoyatchilikka qarshi kurashning nazariy va huquqiy asoslarini chuqur o'rganishga bo'lgan ehtiyojni yanada kuchaytiradi. Mavjud adabiyotlar asosan normativ-huquqiy hujjatlarning tavsifiy tahlili bilan cheklanib, huquqni qo'llash amaliyoti, elektron dalillarni yig'ish va baholashning murakkabliklari, shuningdek, kiberprofilaktikaning samarali mexanizmlari bo'yicha chuqur ilmiy asoslangan

tavsiyalarni kam o'z ichiga oladi. Shu bois, ushbu tadqiqot kiberjinoyatlarga qarshi kurashishning huquqiy asoslarini O'zbekiston sharoitida tizimli ravishda tahlil qilish, xalqaro tajribani hisobga olgan holda milliy qonunchilikni takomillashtirish yo'nalishlarini aniqlashga qaratilgan bo'lib, mavjud bo'shliqni qisman to'ldirishga intiladi.

Ushbu tadqiqotda kiberjinoyatlar va ularning oldini olishning huquqiy asoslarini tahlil qilish uchun kompleks yondashuv qo'llanildi. Tadqiqotning metodologik asosi sifatida quyidagi usullar tanlandi: tizimli tahlil, qiyosiy-huquqiy tahlil, mantiqiy-deduktiv va induktiv usullar, shuningdek, statistik ma'lumotlarni tahlil qilish.

Tizimli tahlil kiberjinoyatlarga qarshi kurashishning huquqiy tizimini yaxlit va o'zaro bog'liq elementlar majmui sifatida o'rganish imkonini beradi. Bu metod orqali mavjud normativ-huquqiy hujjatlar, ularning o'zaro aloqasi va amaliyotdagi samaradorligi baholanadi.

Qiyosiy-huquqiy tahlil xalqaro kiberxavfsizlik qonunchiligi va amaliyoti (masalan, Yevropa Kengashining Budapesht konvensiyasi) bilan O'zbekiston Respublikasi qonunchiligini solishtirish orqali eng yaxshi amaliyotlarni aniqlash va milliy tizimni takomillashtirish yo'nalishlarini belgilashga xizmat qiladi.

Mantiqiy-deduktiv va induktiv usullar kiberjinoyatchilikning umumiy tendensiyalaridan xususiy holatlarga o'tish va aksincha, ma'lumotlardan umumlashgan xulosalar chiqarish uchun ishlatiladi. Bu kiberjinoyatlar turlari, ularning sabablari va oqibatlarini chuqur tushunishga yordam beradi.

Statistik ma'lumotlarni tahlil qilish, xususan, O'zbekistonning kiberxavfsizlik bo'yicha xalqaro reytinglardagi o'rni, kiberhujumlar soni va ularning turlari to'g'risidagi ma'lumotlar mavzuning dolzarbligini asoslash va mavjud tahdidlarning miqyosini aniqlashda muhim rol o'ynaydi. Bu usullar orqali mamlakatda kiberxavfsizlikni ta'minlash sohasida qanday ishlar qilinganligi va qanday muammolar mavjudligi to'g'risida ob'ektiv xulosa chiqariladi. Tadqiqotda O'zbekiston Respublikasining "Kiberxavfsizlik markazi" tomonidan e'lon qilingan qonun hujjatlari to'plamlari, jumladan, 1992 yildan boshlab qabul qilingan va 2022 yilgi yangilanishlarni o'z ichiga olgan o'n oltita qonun hujjatining tahlili ham asosiy manbalardan biri sifatida xizmat qildi. Tadqiqotning amaliy ahamiyati, kiberjinoyatchilikka qarshi kurashishda samarali huquqiy mexanizmlarni yaratish bo'yicha ilmiy asoslangan takliflar ishlab chiqishdan iboratdir.

Xulosa qilib aytganda, Kiberjinoyatlar XXI asrning eng jiddiy tahdidlaridan biri bo'lib, uning global miqyosdagi iqtisodiy zarari va ijtimoiy xavfi doimiy ravishda o'sib bormoqda. O'zbekiston Respublikasi bu borada qator huquqiy asoslarni yaratgan bo'lsada, jumladan, 1992 yildan boshlab o'n oltidan ortiq qonun hujjatlari qabul

qilinganligi, 2022 yilda ham yangi qonunlar bilan normativ-huquqiy baza mustahkamlanganligi shunga guvohlik beradi, ammo tizimli kamchiliklar saqlanib qolmoqda. Xalqaro reytinglardagi past ko'rsatkichlar, davlat va iqtisodiy boshqaruv saytlariga qilingan hujumlarning keskin o'sishi va milliy internet segmentida qayd etilgan millionlab zararli hodisalar kiberjinoyatchilikka qarshi kurashish mexanizmlarini jiddiy takomillashtirish zarurligini ko'rsatadi.Keng qamrovli milliy kiberxavfsizlik strategiyasini ishlab chiqish va amalga oshirish: Ushbu strategiya kiberxavfsizlikni ta'minlash bo'yicha uzoq muddatli maqsadlar, vazifalar va ustuvor yo'nalishlarni aniq belgilashi lozim. Unda davlat organlari, xususiy sektor va fuqarolik jamiyati institutlarining o'zaro hamkorlik mexanizmlari belgilanishi kerak.

Normativ-huquqiy bazani takomillashtirish: Kiberjinoyatlarning barcha turlarini qamrab oluvchi, elektron dalillarni yig'ish, saqlash va ulardan foydalanish bo'yicha xalqaro standartlarga mos keladigan qonun hujjatlarini qabul qilish va mavjudlarini yangilash zarur. Xususan, Budapesht konvensiyasiga qo'shilish va uning normalarini milliy qonunchilikka implementatsiya qilish masalasini ko'rib chiqish lozim.Kiberjinoyatlarni tergov qilish va sudga oshirish salohiyatini oshirish: Huquqni muhofaza qiluvchi organlar xodimlarining raqamli forenzika va kibertergov sohasidagi bilim va ko'nikmalarini oshirish uchun muntazam treninglar va malaka oshirish kurslarini tashkil etish, zamonaviy texnik vositalar bilan ta'minlash zarur.Kiberprofilaktika mexanizmlarini kuchaytirish: Aholi va biznes sub'ektlari orasida kiberxavfsizlik madaniyatini shakllantirish, raqamli gigiyena qoidalarini targ'ib qilish bo'yicha keng ko'lamli kampaniyalar o'tkazish, ta'lim tizimida kiberxavfsizlik bo'yicha dasturlarni joriy etish lozim. Xalqaro hamkorlikni faollashtirish: Kiberxavfsizlik bo'yicha xalqaro tashkilotlar va xorijiy davlatlarning tajribasini o'rganish, ma'lumot almashish va transchegaraviy kiberjinoyatlarni tergov qilishda o'zaro yordamni kuchaytirish muhim ahamiyatga ega. Bu borada ikki tomonlama va ko'p tomonlama kelishuvlar doirasidagi ishlarni faollashtirish kerak.

Ushbu chora-tadbirlarning kompleks tarzda amalga oshirilishi O'zbekistonning kiberxavfsizlik sohasidagi mavqeini mustahkamlashga, kiberjinoyatlar sonini kamaytirishga va mamlakatning raqamli transformatsiyasini xavfsiz muhitda amalga oshirishga xizmat qiladi.

Foydalanilgan adabiyotlar

1. Young, A. Kiberjinoyat: Huquq va Global Boshqaruv. Oxford: Oxford University Press, 2023.
2. Walden, I. Kompyuter jinoyatlari va Raqamli tergovlar. Oxford: Oxford University Press, 2016.

3. Grabowski, M. P. Xalqaro Kiberjinoyat: Huquq va Amaliyot Bo'yicha Qo'llanma. Cheltenham: Edward Elgar Publishing, 2021.
4. Ducheine, P. N., & van der Sloot, B. J. M. "Budapesht kiberjinoyatchilik konvensiyasi: Dastlabki o'n yillik sharhi." Xalqaro Huquq, Kompyuterlar va Texnologiyalar Sharhi, vol. 28, no. 1, 2014, pp. 106-121.
5. Alimi, A. A., & Adegbola, S. O. "Kiberjinoyat Huquqi va Raqamli Davrning Qiyinchiliklari: Nigeriya Kontekstida Tadqiqot." Kiberxavfsizlik Jurnali, jild 4, son 2, 2018, bet. 119-129.