ZAMONAVIY KIBERMUHITDA XAVFSIZLIKNI TA’MINLASH: QONUNCHILIK, HAMKORLIK VA STRATEGIK ISLOHOTLAR

Muslimov Xusan Nishonboyevich
IIV Malaka oshirish instituti
Jangovar tayyorgarlik sikli o‘qituvchisi, mayor

Annotatsiya: **Mazkur maqolada global kiberxavfsizlik muammolari va ularga qarshi kurashishda milliy hamda xalqaro hamkorlikning ahamiyati tahlil etilgan. Raqamli iqtisodiyot rivoji va axborot texnologiyalarining keng tarqalishi ortidan kiberjinoyatchilikning kuchayishi muammosi dolzarblik kasb etmoqda. O‘zbekistonda qabul qilingan "Kiberxavfsizlik to‘g‘risida"gi Qonun va unga mos qonunosti hujjatlar asosida milliy tizim shakllantirilayotgani qayd etilgan. Shu bilan birga, amalga oshirilayotgan chora-tadbirlarning samaradorligini oshirish uchun xalqaro konvensiyalar, xususan, Budapesht konvensiyasi kabi huquqiy hujjatlarning ahamiyati, kadrlar tayyorlash, profilaktika tadbirlari va infratuzilmani takomillashtirish masalalari muhokama qilingan. Maqolada kiberjinoyatlar va ularni aniqlash, javobgarlikni belgilash, tezkor ma’lumot almashish va institutsional hamkorlikka oid muammolarga yechimlar taklif etilgan.**

Kalit so‘zlar: **Kiberxavfsizlik, kiberjinoyatchilik, axborot texnologiyalari, raqamli iqtisodiyot, milliy qonunchilik, xalqaro hamkorlik, Budapesht konvensiyasi, profilaktika, axborot madaniyati, kibermadaniyat, kiberxavf tahdidlari.**

Аннотация: В данной статье проанализированы глобальные проблемы кибербезопасности и значение национального и международного сотрудничества в борьбе с ними. В условиях развития цифровой экономики и широкого распространения информационных технологий актуализируется проблема усиления кибер преступности. Отмечено, что в Узбекистане

формируется национальная система на основе принятого Закона «О кибербезопасности» и соответствующих подзаконных актов. Также обсуждаются вопросы повышения эффективности предпринимаемых мер, важность международных правовых документов, таких как Будапештская конвенция, подготовки кадров, профилактических мероприятий и совершенствования инфраструктуры. В статье предложены решения по вопросам киберпреступлений, их выявления, установления ответственности, оперативного обмена информацией и институционального сотрудничества.

Ключевые слова: Кибербезопасность, киберпреступность, информационные технологии, цифровая экономика, национальное законодательство, международное сотрудничество, Будапештская конвенция, профилактика, информационная культура, киберкультура, киберугрозы.

Abstract: This article analyzes global cybersecurity issues and highlights the importance of national and international cooperation in combating them. With the growth of the digital economy and the widespread use of information technologies, the issue of rising cybercrime has become increasingly urgent. The article notes that a national system is being developed in Uzbekistan based on the adopted Law "On Cybersecurity" and relevant by-laws. It also discusses the importance of enhancing the effectiveness of current measures, including international legal instruments such as the Budapest Convention, human resource development, preventive strategies, and infrastructure improvement. The article proposes solutions to challenges related to cybercrime detection, accountability, rapid information exchange, and institutional cooperation.

Keywords: Cybersecurity, cybercrime, information technology, digital economy, national legislation, international cooperation, Budapest Convention, prevention, information culture, cyber culture, cyber threats.

Davlatimiz rahbari Mirziyoyev Shavkat Miromonovich kiberxavfsizlik borasida bir qator tashabbuslarni ilgari surganligi bejiz emas. Jumladan:

2023 yil 20 dekabr – Prezident videoselektor yig‘ilishida axborot texnologiyalari sohasini rivojlantirish va davlat boshqaruvini raqamlashtirish bo‘yicha ustuvor vazifalarni belgiladi. Ushbu yig‘ilishda 2023 yilning o‘tgan 11 oyi mobaynida 5,5 mingta kiberjinoyat sodir etilgani, ularning 70 foizi bank kartalari bilan bog‘liq firibgarlik va o‘g‘irlik jinoyatlari ekanligi ta’kidlandi. Shuningdek, mamlakatdagi 50 ga yaqin to‘lov tizimining hammasi ham kiberxavfsizlik talablariga javob bermasligi tanqid qilindi. Prezident mutasaddi vazirlik va idoralarga barcha elektron to‘lov tizimlari uchun yagona kiberxavfsizlik talablarini ishlab chiqish va ijrosini qat’iy nazorat qilish bo‘yicha topshiriq berdi.

2023 yil 8 iyun – Prezidentning “O‘zbekiston Respublikasining muhim axborot infratuzilmasi ob’ektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi qaroriga asosan Davlat xavfsizlik xizmatiga yangi vakolatlar berildi. Qarorga ko‘ra, DXX muhim axborot infratuzilmasi ob’ektlarida kiberhujumlarni aniqlash, ularning oldini olish, tezkor chora ko‘rish va oqibatlarini bartaraf etish hamda kiberxavfsizlikni ta’minlash bo‘yicha faoliyatni muvofiqlashtiradi.

2025 yil 20 yanvar – Prezidentning “Cyber university” davlat universitetini tashkil etish to‘g‘risidagi qarori qabul qilindi. Ushbu universitet axborotni himoyalash, axborot va kiberxavfsizlik, raqamli texnologiyalar va raqamli iqtisodiyot, sun’iy intellektka asoslangan avtomatlashtirilgan axborot-tahliliy tizimlarni yaratish, robototexnika va boshqa turdosh sohalar bo‘yicha kadrlar tayyorlashni o‘z oldiga maqsad qilib qo‘ydi.

Bugungi kunda global axborot maydonida kibermakon bilan bog‘liq yangidan-yangi tahdidlar yuzaga kelmoqda. Shu bois virtual olamdagi hujumlardan himoyalanish masalasi dunyo hamjamiyatini jiddiy tashvishga solmoqda. Raqamli iqtisodiyotning rivojlanishi va axborot texnologiyalarining keng ommalashuvi natijasida kiberjinoyatchilik zamonaviy jamiyat uchun jiddiy tahdidlardan biriga aylandi. Ushbu global muammo faqat milliy darajada emas, balki xalqaro hamkorlik asosida samarali hal qilinadi. Shu sababli, xalqaro kelishuvlar va konvensiyalar

kiberjinoyatlarga qarshi kurashda muhim huquqiy asoslarga ega. Shu munosabat bilan O‘zbekiston Respublikasida mutasaddi tashkilotlar tomonidan kiberjinoyatchilikka qarshi kurashishda samaradorlikka erishishi uchun xalqaro kelishuvlarga qo‘shilishi, ularning milliy qonunchilikka moslashtirilishi va amaliyotga tatbiq etilishi jarayonlari tashkil etilishi lozim [1].

O‘zbekiston Respublikasida kiberxavfsizlik sohasidagi munosabatlar va kiberjinoyatlarga qarshi kurashish O‘zbekiston Respublikasining 2022-yil 15-apreldagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonuni hamda boshqa qonunosti hujjatlari orqali tartibga solinadi. Mazkur qonunda “**kiberjinoyatchilikka** – axborotni egallash, uni o‘zlashtirish, yo‘q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta’minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig‘indisi” [2] deya ta’rif berilgan.

Zamonaviy raqamli davrda kibertahdidlarga qarshi kurash faqat texnologik choralarga tayanib qolmaydi. Bu masala har tomonlama, ya’ni huquqiy, institutsional, texnologik va ijtimoiy jihatdan ham keng ko‘lamli yondashuvni talab etadi. Bugungi kunda internet, kompyuter va mobil aloqa hayotimizning asosi bo‘lib, yangi imkoniyatlar bilan birga yangi xavflarni ham olib kelmoqda. Shu sababli, bu tahdidlarga qarshi samarali kurash uchun milliy darajadagi sa’y-harakatlar bilan birgalikda xalqaro tajriba va hamkorlikka ham tayanish zarur. Avvalo, axborot-kommunikatsiya sohasiga xos tahdidlar bilan ishlashga qodir bo‘lgan mutaxassislarni tayyorlash muhimdir. Buning uchun nafaqat texnik, balki huquqiy munosabatda ham yetuk kadrlar kerak. Yoshlar orasida axborot xavfsizligi ongini oshirish, xabardorlik darajasini ko‘tarish maqsadida o‘quv dasturlari, seminar-treninglar tashkil etilishi zarur. Shu bilan birga, maktab va oliy ta’lim muassasalarida kibermadaniyatni shakllantirish, axborot etikasini o‘rgatish bo‘yicha maxsus yo‘nalishlar kiritilishi lozim. Bunday yondashuv nafaqat profilaktika sifatida, balki kelajakda ehtiyoj bo‘ladigan malakali mutaxassislarni tayyorlash imkonini beradi.

Axborot xavfsizligini ta’minlashda o‘zaro integratsiyalashgan tizim yaratilishi zarur. Buning uchun texnik platformalar, monitoring tizimlari, real vaqt rejimida

tahdidlarni aniqlash imkonini beruvchi dasturiy yechimlar keng joriy etilishi muhim. Bu tizimlar faqat texnik, balki huquqiy va institutsional nuqtai nazardan ham qo‘llab-quvvatlanishi kerak. Ichki ishlar vazirligi, Davlat xavfsizlik xizmati, prokuratura, sud hokimiyati kabi muassasalar o‘rtasida axborot almashinuvi, tezkor muvofiqlashtirish va real vaqtli harakatni ta’minlaydigan mexanizmlar yaratilishi lozim.

Ammo bu texnik va institutsional chora-tadbirlarning samarali ishlashi faqat ularni birlashtiruvchi va tartibga soluvchi qonunchilik mavjud bo‘lsa mumkin. Ayniqsa, axborot-kommunikatsiya infratuzilmasini himoya qiluvchi qonun hujjatlari doimiy ravishda qayta ko‘rib chiqilishi va kibermakondagi tez o‘zgarishlarga xos bo‘lgan yondoshuvlar bilan mos ravishda yangilanishi zarur. Misol uchun, O‘zbekiston Respublikasining 2022-yil 15- apreldagi “Kiberxavfsizlik to‘g‘risida”gi Qonuni asosan mutasaddi tashkilotlarning vakolatlarini kengaytirishga yo‘naltirilgan, ammo xalqaro hamkorlik, transchegaraviy jinoyatlarni tergov qilish va dalillarni zamonaviy standartlar asosida almashishning aniq mexanizmlari hozircha joriy etilmagan [3]. Bu esa, jinoyatga oid dalillarni tez va tartibli ravishda kelib tushgan boshqa davlatlarga yetkazish yoki ularning dalillarini olishda muammolarni yuzaga keltirmoqda. Shu bilan birga, jinoyatni aniqlash va tergovda vaqt talab qilmaydigan real vaqtli monitoring vositalarini joriy etishda ham qonunchilikdagi bo‘shliqlar kuzatilmoqda.

Kiberjinoyatlar tushunchasi Qonunda aniq belgilangan bo‘lsa ham, “blokirovka qilish” (ya’ni xakerlar tomonidan sayt yoki tizimni ishlashdan to‘xtatish), “DDoS hujumlar” yoki botnetlar orqali boshqariladigan tarqatilgan hujumlar kabi o‘ziga xos holatlar bo‘yicha penalizatsiya va jazolash mexanizmlari to‘liq ifodalanmagan [4]. Bu esa sud amaliyotida u yoki bu holatda jinoyat sodir bo‘lganmi yoki sodir bo‘lmaganmi, qanchalik og‘irligi qanday aniqlanishi borasida savollarni keltirib chiqaradi. Global miqyosda esa, nodavlat aktorlar va kiberqurilmalar tomonidan amalga oshirilayotgan hujumlar ham mavjud bo‘lib, bu turlar bo‘yicha amaliy jihatdan aniq yo‘riqnomalar va profilaktika choralarini belgilaydigan qonunchilik zarurdir.

Kiberxavfsizlikka oid xalqaro konventsiyalar — jumladan, Budapesht Konvensiyasi va boshqa huquqiy oqimlar ham bo‘shliqlarni to‘ldirishda muhim manba hisoblanadi. Shu sababli, O‘zbekistonda ratifikatsiya qilinmagan Budapesht Konvensiyasining tegishli moddalarini milliy qonunchilikka tatbiq etish zarur. Bu, transchegaraviy tergovlar yoki boshqa davlatlar bilan dalillarni tez almashish hokazo holatlarda muhim rol oynaydi. Masalan, jinoyat ijtimoiy tarmoqlarda sodir etilgan bo‘lsa, tegishli davlatdan ma’lumotlar arizasi kelishini kutish vaqt talab qilishi mumkin — lekin agar qonun hamda xalqaro mexanizmlar to‘liq yo‘lga qo‘yilgan bo‘lsa, bu muddat sezilarli darajada qisqaradi.

Bundan tashqari, MDH kabi hamkor tashkiotlar bilan tuzilgan bitimlar asosida darhol aloqa va texnik yordam olish mumkin. Biroq bu doiralar cheklangan bo‘lishi mumkin; global platformalarda — masalan, Interpol, Europol yoki OSCE kabi tashkilotlar bilan hamkorlik joriy etilishi kiberjinoyatlarga qarshi samarali kurashni yanada kuchaytiradi [5]. Amaliyotda, masalan, kiberhujumlar aniqlanganda, bir necha daqiqa ichida dalilni olish va qayta ishlash, tegishli serverlarni bloklash, xakerlar tomonidan yaratilgan tarmoqlarni aniqlash kabi chora-tadbirlar amalga oshiriladi. Biroq buni amalga oshirish uchun laboratoriya va texnik infratuzilma bilan bir qatorda, xalqaro standartlarga mos keluvchi protokollar zarur.

Shuningdek, barcha jarayonlarni qo‘llab-quvvatlovchi monitoring va profilaktika tizimlari rivojlantirilishi lozim. Bu yerda texnik vositalar bilan bir qatorda, ijtimoiy-iqtisodiy omillar ham hisobga olinishi zarur. Masalan, kibertahdidlarga qarshi kurash faqat jinoyatchilikni aniqlash bilan cheklanmaydi — balki bu sohani tashkil etuvchi omillar: buxgalterlar yoki yuridik mutaxassislar ham kiberxavfsizlik asoslari bo‘yicha o‘qitilishi, kichik va o‘rta biznesda ham xavfsizlik siyosati shakllantirilishi talab etiladi. Shu bilan birga, aholining internetdagi bexatar masofadan muomala qilish, shaxsiy ma’lumotlar bilan ehtiyotkor muomala qilish, firibgarlikdan ogohlantirish tavsiyalari, kibermadaniyat haqida aksiyalarning kengaytirilishi ham zarur. Bu orqali profilaktika safarbarligi kuchayadi.

Natijada, zamonaviy kibertahdidlarga qarshi kurash mutaxassislar tayyorlash, texnik va monitoring infratuzilma yaratish, qonunchilikni xalqaro standartlarga moslashtirish va ijtimoiy profilaktika hamjamiyatida axborot xavfsizligi ongini shakllantirish kabi kompleks choralarni talab qiladi. Shu yo‘l bilan O‘zbekiston Respublikasi xalqaro hamkorlikni mustahkamlab, milliy qonunchilikni bu sohada sifatni oshiruvchi tarzda yangilashi mumkin. Bu esa nafaqat zamonaviy tahdidlarga qarshi chora-tadbirlarni kuchaytiradi, balki milliy va global axborot makonida barqaror va xavfsiz muhit yaratishda muhim qadam bo‘ladi.

Xulosa qilib aytganda, kibermakonda yuzaga kelayotgan tahdidlar va jinoyatlar nafaqat texnologik taraqqiyotning salbiy oqibati, balki insoniyatning axborot bilan ishlashdagi madaniy va huquqiy yetuklik darajasining ham sinovidir. O‘zbekiston Respublikasi so‘nggi yillarda kiberxavfsizlikni ta’minlash, axborot makonini himoyalash va zamonaviy tahdidlarning oldini olish bo‘yicha muhim huquqiy asoslarni yaratdi. Biroq mavjud qonunchilikning ayrim jihatlari – xususan, xalqaro hamkorlikning sustligi, zamonaviy kiberjinoyat turlarini penalizatsiya qilishdagi noaniqliklar va texnik resurslarning cheklanganligi – bu sohada yanada tizimli islohotlarni talab etmoqda.

Kiberxavfsizlikning samaradorligi faqat texnologik yechimlar bilan emas, balki malakali mutaxassislar, moslashtirilgan qonunchilik, xalqaro tajriba almashuvi va axborot madaniyatining shakllanishi orqali ta’minlanadi. Bu yo‘lda nafaqat davlat tashkilotlari, balki jamiyatning har bir a’zosi, ta’lim muassasalari, ommaviy axborot vositalari va xususiy sektor ham faol ishtirok etishi zarur. Faqat ana shundagina O‘zbekiston axborot makonida xavfsizlik, barqarorlik va ishonch muhitini qaror toptira oladi. Shu bilan birga, mamlakatimizning global raqamli maydondagi ishtiroki kuchayib, xalqaro axborot xavfsizligi tizimida munosib o‘ringa ega bo‘ladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. O‘zbekiston Respublikasining 2022-yil 15-apreldagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonuni 3-moddasi;

2. Cyber Law: Safeguarding Digital Spaces in Uzbekistan / Maqola / Elektron resurs / Rejim kirish: https://irshadjournals.com/index.php/ijcl/article/view (murojaat qilingan sana 13.06.2025);

3. “Evidence and attribution of responsibility in international cyber-attacks: The adequacy of the international legal framework?” Tilburg Institute for Law, Technology, Market and Society, January 2020, p. 19 / Elektron resurs / Rejim kirish: https://arno.uvt.nl/show.cgi?fid=150329 (murojaat qilingan sana 13.06.2025);

4. OSCE workshop in Uzbekistan supports development of national competency framework and training strategy on cybercrime and electronic evidence / Elektron resurs / Rejim kirish: https://www.osce.org/secretariat/592076 (murojaat qilingan sana 13.06.2025).

5. L.Z.Komilov “Kiberjinoyatlarga qarshi xalqaro kelishuvlar va ularning milliy qonunchilikka implementatsiyasi” / Maqola / Kiberjinoyatchilikka qarshi kurashishning huquqiy, tashkiliy, moliyaviy-iqtisodiy, muhandislik-texnik muammolari va yechimlari nomli Respublika ilmiy-amaliy konferensiya materiallari to‘plami, 166-bet, IIV Malaka oshirish instituti, 2024;