

KIBERXAVFSIZLIK JINOYATLARINING OLDINI OLISH – DAVR TALABI

**Maxmudov Dilmurod Ro'zmatovich**

O'zbekiston Respublikasi IIV Akademiyasining "Kriminologiya"
kafedrası professori v.b., yuridik fanlar doktori, dotsent

Annotatsiya. Ushbu maqolada raqamli jamiyatda kiberjinoatlarning kuchayib borayotgani, ularning davlat xavfsizligi, iqtisodiy barqarorlik va shaxsiy erkinliklarga salbiy ta'siri haqida so'z yuritiladi. Muallif tomonidan kiberjinoatlarning oldini olishda mavjud qonunchilikdagi bo'shliqlar, kadrlar yetishmovchiligi, madaniyat yetishmasligi va xalqaro hamkorlikdagi muammolar tahlil qilinadi. Shuningdek, muammo yechimlari sifatida qonunchilikni takomillashtirish, malakali mutaxassislar tayyorlash, kiberxavfsizlik madaniyatini shakllantirish va xalqaro hamkorlikni kuchaytirish bo'yicha takliflar ilgari suriladi.

Kalit so'zlar: kiberxavfsizlik, kiberjinoatlar, raqamli xavfsizlik, qonunchilik, xalqaro hamkorlik, elektron dalillar, profilaktika

ПРЕДОТВРАЩЕНИЕ КИБЕРПРЕСТУПЛЕНИЙ – ТРЕБОВАНИЕ НАСТОЯЩЕГО ВРЕМЕНИ

Аннотация. В статье рассматриваются проблемы киберпреступности в условиях цифрового общества и её влияние на национальную безопасность, экономическую стабильность и личные свободы. Автор анализирует пробелы в законодательстве, нехватку квалифицированных кадров, низкий уровень киберкультуры в обществе, а также недостаточность международного сотрудничества. Предлагаются стратегические меры по совершенствованию законодательства, подготовке специалистов, формированию кибербезопасного мышления и укреплению международного взаимодействия.

Ключевые слова: кибербезопасность, киберпреступность, цифровая безопасность, законодательство, международное сотрудничество, электронные доказательства, профилактика

CYBERCRIMES PREVENTION - DEMAND OF THE PRESENT TIME

Abstract. This article discusses the increasing threat of cybercrime in the digital age and its negative implications for national security, economic stability, and personal freedoms. The author analyzes gaps in legislation, the shortage of specialized professionals, low levels of cyber culture among the population, and insufficient international cooperation. The article concludes with strategic proposals for legal reform, professional training, public awareness campaigns, and the enhancement of cross-border collaboration.

Keywords: cybersecurity, cybercrime, digital safety, legislation, international cooperation, electronic evidence, prevention

Bugungi kunda raqamli axborot texnologiyalari inson hayotining barcha jabhalariga jadal sur'atlarda kirib kelmoqda. Elektron hukumat, raqamli iqtisodiyot, onlayn ta'lim va tibbiyot, bank tizimlari va hatto huquqni muhofaza qilish organlari ham axborot tizimlariga bog'liq holga kelgan. Ammo ushbu jarayonlar bilan bir

qatorda kiberjinoatchilik ham shiddat bilan o'sib bormoqda, bu esa milliy xavfsizlik, shaxsiy erkinliklar va iqtisodiy barqarorlikka tahdid solayotgan muhim omillardan biriga aylandi. Xususan, 2022-yil 15-aprelda O'zbekistonda kiberxavfsizlik munosabatlarini tartibga solish maqsadida "Kiberxavfsizlik to'g'risida"gi qonun qabul qilingani hech kimga sir emas [1].

Darhaqiqat, bugungi kunda kiberxavfsizlik jinoyatlari nafaqat moliyaviy yoki axborot yo'qotishlariga, balki davlatning siyosiy va iqtisodiy ustuvorliklariga qarshi qaratilgan tahdidlar sifatida ham namoyon bo'lmoqda. Mazkur jinoyatlarning jahon miqyosida transmilliy xarakteri, anonimlik va tezkor amalga oshirilishi ularni aniqlash va tergov qilishni ancha murakkablashtirmoqda. O'zbekistonda ham so'nggi yillarda kiberhujumlar, shaxsiy ma'lumotlarni o'g'irlash, onlayn firibgarlik holatlari ko'payib borayotgani bunga yaqqol misoldir [2].

Ilmiy jihatdan qaraydigan bo'lsak, jinoyat huquqi va kriminologiya sohalarida kiberjinoyatchilik hali yetarli darajada o'rganilmagan muammolardan biri sanaladi. Axborot tizimlaridan foydalanib sodir etiladigan jinoyatlar tarkibini aniq belgilash, ularga javobgarlik choralari individuallashtirish va eng muhimi – ularning oldini olishga qaratilgan kompleks profilaktik mexanizmlarni ishlab chiqish davr talabiga aylanmoqda. Xususan, kiberxavfsizlik sohasidagi jinoyatlarning oldini olish masalasi nafaqat amaliy, balki strategik va ilmiy ahamiyatga ega dolzarb muammo hisoblanadi. Bularga:

a) *kiberxavfsizlik sohasidagi jinoyatlarning oldini olish strategiyasida yuzaga keladigan muammo* – mazkur muammo davlatning siyosiy va iqtisodiy barqarorligiga jiddiy ta'sir ko'rsatadi. Shuningdek, maxsus xizmatlar, bank tizimi, sog'liqni saqlash, energetika va aloqa kabi muhim infratuzilmalarga qilingan kiberhujumlar nafaqat iqtisodiy zarar, balki davlat xavfsizligiga ham tahdid soladi;

b) *kiberxavfsizlik sohasidagi jinoyatlarni oldini olishning ilmiy ahamiyati bilan bog'liq muammo* – mazkur muammo mamlakatda nafaqat *jinoyat huquqi* doirasini, balki axborot huquqi, raqamli kriminologiya, elektron dalillar tahlili va kiberprofilaktika kabi sohalarni ham o'z ichiga qamrab oladi. Masalan, huquqshunos olim A.R.Mamatqulov to'g'ri ta'kidlaganidek, bugungi kunda “elektron dalillarning sud amaliyotidagi maqomi, ularni to'plash va huquqiy asosda rasmiylashtirish borasida ilmiy-amaliy bo'shliq hali hamon mavjud” [3].

Shuningdek, mazkur muammolarni yuzaga kelishiga esa o'z navbatida normativ-huquqiy hujjatlar bazasini takomillashtirish [4], kiberxavfsizlik sohasiga ixtisoslashgan iqtidorli kadrlarni tayyorlash, jamiyatda kiberxavfsizlik madaniyatini shakllantirish hamda xalqaro hamkorlikni mustahkamlash kabi yo'nalishlardagi vazifalar ijorosini ta'minlash bilan bog'liq sustkashliklar ham sabab bo'lmoqda desak hech mubolag'a bo'lmaydi. Bularga:

birinchidan, normativ-huquqiy hujjatlar bazasini yetarlicha rivojlanmaganligi – bugungi kunda, R.Mamatqulov to'g'ri ta'kidlaganidek, kiberxavfsizlik sohasidagi jinoyatlarni huquqiy jihatdan to'liq tartibga solish uchun mavjud qonun hujjatlari yetarli darajada takomillashtirilmagan [3]. Xususan, Jinoyat kodeksida axborot jinoyatlarining aniq va mukammal klassifikatsiyasi, javobgarlik mezonlari va elektron dalillarni huquqiy jihatdan baholash mexanizmi hali ham aniq belgilanmagan;

ikkinchidan, ixtisoslashgan kadrlar tayyorlashdagi muammolar – kiberxavfsizlik sohasida faoliyat yuritish uchun huquqiy va texnik bilimlarni sintez qilgan, mukammal bilimga ega mutaxassislar yetishmaydi. Amaldagi OTMlarda ushbu yo'nalishda mutaxassis tayyorlashning o'quv dasturlari yetarlicha zamonaviy emas, ilmiy tadqiqotlarga asoslangan emas. Shu o'rinda, xalqaro aloqalar, jahon siyosati va siyosiy fanlar bo'yicha xalqaro ekspert A.U. Nematullayev o'zining “O'zbekiston Respublikasining kiberxavfsizligini ta'minlash muammolari” nomli maqolasida axborot texnologiyalarining rivojlaniishi bilan bog'liq ravishda kiberxavfsizlik sohasidagi mutaxassislarni tayyorlashdagi muammolarni tahlil qiladi [5]. U, xususan, “*Digital Uzbekistan–2030*” strategiyasini amalga oshirish jarayonida kadrlar yetishmasligi va mavjud infratuzilmaning yetarli emasligini ta'kidlaydi;

uchinchidan, kiberxavfsizlik madaniyatining yetishmasligi – jamiyatda aholining keng qatlamlari, ayniqsa, yoshlar o'rtasida shaxsiy ma'lumotlar bilan ishlash madaniyati, xavfsiz internetdan foydalanish ko'nikmalari, onlayn tahdidlarga nisbatan hushyorlik darajasi past ekanligidir;

to'rtinchidan, xalqaro hamkorlikning yetarlicha faol emasligi — kiberjinoyatlar ko'pincha transmilliy xususiyatga ega bo'lib, ularni faqat milliy qonunlar doirasida hal etish murakkabdir. O'zbekiston hozircha Budapesht konvensiyasiga¹ qo'shilmagan, bu esa elektron dalillarni transchegaraviy almashishda huquqiy to'siqlar yaratadi.

Xususan, kiberjinoyatlarning transmilliy tabiati sababli, ularni samarali tergov qilish va sudga tortish uchun davlatlar o'rtasidagi hamkorlik muhim ahamiyatga ega. Konvensiyaga qo'shilmagan davlatlar uchun bunday hamkorlikni amalga oshirishda huquqiy to'siqlar yuzaga keladi.

Ma'lumot uchun: 2015-yilda Amerika Qo'shma Shtatlari va Xitoy Xalq Respublikasi o'rtasida kiberxavfsizlik bo'yicha ijroiyl kelishuv qabul qilingan. Ushbu kelishuv kiberxavfsizlik siyosatiga oid bir qator sohalarni qamrab oladi, jumladan, axborot almashinuvi mexanizmlari hamda har ikki davlat kiber vositalar orqali zehniy mulkni o'g'irlashni qo'llab-quvvatlamaslik to'g'risidagi kelishuvni ham o'z ichiga oladi. Kelishuv AQSH Prezidenti Barak Obama va Xitoy Bosh kotibi Si Szinpin ishtirokida Oq uyda bo'lib o'tgan qo'shma matbuot anjumanida e'lon qilingan [6].

Bugungi kunda O'zbekistonda kiberxavfsizlik bilan bog'liq jinoyatlarning oldini olish shuningdek, mavjud muammolarni bartaraf etish maqsadida quyidagi strategik yo'nalishlarda tizimli ishlar olib borish tavsiya etiladi. Bularga:

birinchidan, Jinoyat kodeksiga axborot xavfsizligi bo'yicha alohida moddalarni kiritish, jumladan *elektron dalillarning* maqomini aniq belgilash;

ikkinchidan, barcha oliy ta'lim muassasalarida *"Kiberhuquq"* va *"Axborot xavfsizligi huquqi"* fanlarini majburiy tartibda joriy etish;

uchinchidan, huquqni muhofaza qilish organlari va IT markazlari o'rtasida o'zaro hamkorlikda kadrlar malakasini oshirish dasturlarini yo'lga qo'yish;

to'rtinchidan, O'zbekistonda axborot madaniyatini shakllantirish maqsadida aholi o'rtasida tizimli va maqsadli ravishda ma'rifiy-targ'ibot ishlarini tashkil etish, axborot xavfsizligiga oid bilim va ko'nikmalarni ommalashtirish, turli yosh toifalari uchun moslashtirilgan o'quv-amaliy loyihalarni amalga oshirish;

beshinchidan, O'zbekistonning Budapesht konvensiyasiga qo'shilishini ta'minlash va xalqaro elektron dalillar ayirboshlashning huquqiy mexanizmlarini yaratish.

Foydalanilgan manbalar

1. O'zbekiston Respublikasi Qonunchilik ma'lumotlari milliy bazasi / <https://lex.uz/pdf/5960604>.
2. O'zbekiston Respublikasi Markaziy bankining ma'lumoti / https://cbu.uz/oz/press_center/news/1897716.
3. *Mamatqulov A.R.* Elektron dalillarning huquqiy maqomi // *Yurist axborotnomasi*, 2023. — 4-son.
4. Bugungi kunda O'zbekistonda aynan kiberxavfsizlik munosabatlari "Kiberxavfsizlik to'g'risida"gi, "Muvofiqlikni baholash to'g'risida"gi, "Elektron raqamli imzo to'g'risida"gi, "Elektron hujjat aylanishi to'g'risida"gi, "Aloqa to'g'risida"gi, "Davlat sirlarini saqlash to'g'risida"gi, "Elektron hisoblash mashinalari uchun yaratilgan dasturlar va ma'lumotlar bazalarining huquqiy himoyasi to'g'risida"gi qonunlar va boshqa qonunosti hujjatlari bilan tartibga solinmoqda // <https://csec.uz/uz/docs/uzbekistan-laws>.
5. *Nematullayev A.U.* O'zbekiston Respublikasining kiberxavfsizligini ta'minlash muammolari // https://parl.uz/articles/society/intervyu_s_chlenom_molodezhnogo_parlamenta_pri_oliy_mazhlise_respubliki_uzbekistan.
6. https://en.wikipedia.org/wiki/2015_United_States%E2%80%93China_Cybersecurity_Agreement.

¹ Budapesht konvensiyasi — kiberhuquqbuzarliklarga qarshi kurashish bo'yicha birinchi xalqaro shartnoma bo'lib, uning maqsadi milliy qonunlarni muvofiqlashtirish, tergov usullarini takomillashtirish va davlatlar o'rtasida hamkorlikni kuchaytirishdir. Konvensiya 2001-yil 23-noyabrda imzolangan va 2004-yil 1-iyulda kuchga kirgan. 2025-yil yanvar holatiga ko'ra, 78 davlat ushbu konvensiyani ratifikatsiya qilgan.