RAQAMLI MAKONDA JINOYATCHILIK: NAZARIYA VA HUQUQIY TARTIBGA SOLISH MUAMMOLARI

G‘apurova Gulsanam Kamoliddin qizi
Toshkent davlat yuridik universiteti
Xususiy huquq fakulteti 2-kurs talabasi
marketuzum81@gmail.com

Anotatsiya: *Zamonaviy raqamlashtirish sharoitida kiberjinoyatchilik global xavfsizlik uchun jiddiy tahdidga aylandi. Maqolada kiberjinoyatlarning asosiy turlari - phishing, ransomware, DDoS hujumlari, veb-saytni egallab olish va haktivist faoliyati tahlil qilinadi. Ushbu maqolada O‘zbekiston Respublikasida kiberjinoyatlarga qarshi kurashning huquqiy asoslari, milliy qonunchilik bilan xalqaro standartlar o‘rtasidagi muvofiqlik darajasi baholanadi. Huquqiy tartibga solish bo‘yicha yuzaga kelayotgan dolzarb muammolar va milliy qonunchilikdagi bo‘shliqlar aniqlanib, kiberjinoyatlarga qarshi samarali kurash tizimini yaratish bo‘yicha amaliy takliflar, qonunchilikni takomillashtirish yo‘llari va xalqaro hamkorlikni mustahkamlash choralari taklif etiladi.*

Kalit so‘zlar: *kiberjinoyatlar va kiberjinoyatchilik, raqamli xavfsizlik, huquqiy tartibga solish, xalqaro hamkorlik, O‘zbekiston qonunchiligi.*

CRIME IN DIGITAL SPACE: THEORY AND PROBLEMS OF LEGAL REGULATION

G‘apurova Gulsanam Kamoliddin qizi
Tashkent State University of Law
Faculty of Private Law, 2nd-year student
marketuzum81@gmail.com

Abstract: *In the context of modern digitalization, cybercrime has become a serious threat to global security. This article analyzes the main types of cybercrimes – phishing, ransomware, DDoS attacks, website hijacking, and hacktivist activity. The article evaluates the legal foundations of combating cybercrime in the Republic of Uzbekistan and examines the level of conformity between national legislation and international standards. Current legal issues and gaps in national regulations are identified, and practical proposals are made for creating an effective system to combat cybercrime, including ways to improve legislation and strengthen international cooperation.*

Keywords: *cybercrimes and cybercriminal activity, digital security, legal regulation, international cooperation, Uzbekistan legislation.*

ПРЕСТУПНОСТЬ В ЦИФРОВОМ ПРОСТРАНСТВЕ: ТЕОРИЯ И ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ

Гапурова Гулсанам Камолиддин кызы
Ташкентский государственный юридический университет
Факультет частного права, студентка 2 курса
marketuzum81@gmail.com

Аннотация: *В условиях современной цифровизации киберпреступность стала серьёзной угрозой глобальной безопасности. В статье анализируются основные виды киберпреступлений — фишинг, программы-вымогатели, DDoS-атаки, захват веб-сайтов и деятельность хактивистов. Рассматриваются правовые основы борьбы с киберпреступностью в Республике Узбекистан, а также оценивается степень соответствия национального законодательства международным стандартам. Выявляются актуальные правовые проблемы и пробелы в национальном регулировании, предлагаются практические меры по созданию эффективной системы борьбы с киберпреступностью, совершенствованию законодательства и укреплению международного сотрудничества.*

Ключевые слова: *киберпреступления и киберпреступность, цифровая безопасность, правовое регулирование, международное сотрудничество, законодательство Узбекистана.*

Kirish (Introduction)

Zamonaviy raqamli texnologiyalarning jadal rivojlanishi va internet tarmog‘ining keng tarqalishi jamiyat hayotining deyarli barcha sohalarini qamrab olgan bir davrda, kiberjinoyatchilik masalasi global xavfsizlik va huquqiy tartibga jiddiy tahdid sifatida namoyon bo‘lmoqda. Axborot-kommunikatsiya texnologiyalarining imkoniyatlari kengayishi bilan birga, jinoyatchilar ham o‘z faoliyatini raqamli muhitga ko‘chirib, an’anaviy jinoyatchilik turlarini yangi shakllarda amalga oshirish imkoniyatini qo‘lga kiritdilar. Albatta, texnologiyalarning rivojlanib borishi bir tomondan ishni sifatini oshirib, vaqtni tejash uchun yordam berdi, ammo ikkinchi tomondan kiberjinoyatchilikni yanada rivojlanishi uchun yo‘l ochib berdi desak mubolag‘a bo‘lmaydi.

Kiberjinoyatchilikdan keladigan butunjahon zarari kelgusi to‘rt yil davomida sezilarli o‘sish ko‘rsatishi prognoz qilinmoqda: 2024 yildagi 9,22 trillion dollardan 2028 yilga borib 13,82 trillion dollargacha yetishi kutilmoqda[5]. Kiberxujumlar nafaqat moliyaviy zararni keltirib chiqarmoqda, balki davlatlar xavfsizligi, shaxsiy ma’lumotlar himoyasi, tijorat sirlari va muhim infratuzilma ob’ektlariga ham jiddiy xavf tug‘dirmoqda. Ushbu holatda kiberjinoyatchilikka qarshi samarali kurashish zamonaviy davlatlarning eng muhim vazifalaridan biriga aylandi.

[5] https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

Kiberjinoyatchilikka qarshi kurashishda qonunchilik bazasining mukammalligi hal qiluvchi ahamiyatga ega. Biroq, raqamli jinoyatlarning transchegaraviy xarakteri, texnologik yangiliklar va qonunchilik tizimining nisbatan sekin moslashuvchanlik xususiyatlari orasidagi tafovut jiddiy muammolar tug‘dirmoqda. Xalqaro hamkorlik va milliy qonunchilik tizimlarining uyg‘unlashtirilishi zarurati tobora kuchayib bormoqda. Hozirgi kunda kiberjinoyatchilik sohasida xalqaro hamkorlikni tartibga soluvchi bir qancha muhim hujjatlar mavjud bo‘lib, ular orasida Budapesht konventsiyasi, Shanhay hamkorlik tashkilotiga a’zo davlatlar o‘rtasida “Xalqaro axborat xavfsizligini ta’minlash sohasidagi hamkorlik to‘g‘risida”gi bitim, BMT tomonidan qabul qilingan rezolyutsiyalar va hududiy tashkilotlarning nizolari alohida o‘rin tutadi. Biroq, bu hujjatlarning amaliy samaradorligi va milliy qonunchilik bilan uyg‘unligi masalalari hali ham to‘liq hal etilmagan. Ushbu tadqiqot ishining dolzarbligi kiberjinoyatchilikka qarshi kurashish sohasida xalqaro va milliy qonunchilik tizimlarining hozirgi holatini tahlil qilish, mavjud kamchilik va bo‘shliqlarni aniqlash hamda ularni bartaraf etish bo‘yicha takliflar ishlab chiqish zarurati bilan belgilanadi.

Adabiyotlar tahlili va metodlar

Ushbu maqolada kiberjinoyatlar va uning turlari, huquqiy holatini o‘rganish uchun qiyosiy-huquqiy metod va umumiy-huquqiy tahliliy metodlardan foydalanimiz. Kiberjinoyatchilikka qarshi kurashish to‘g‘risida to‘xtalishdan avval, kiberjinoyat atamasiga ta’rif beradigan bo‘lsak, mubolag‘a bo‘lmasdi bunda O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonunining 3-moddasida belgilangan, “axborotni egallash, uni o‘zgartirish, yo‘q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta’minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyat” [6]ni tushunamiz, mazkur ta’rifdagi kibermakon so‘zi esa axborot texnologiyalari yordamida yaratiladigan muhit ma’nosini anglatadi. Yana shuni ham ta’kidlab o‘tishimiz joizki, “kiberjinoyat tushunchasi, bugungi kunda ommaviy ravishda qo‘llaniladigan axborottexnologiyalari sohasidagi jinoyatlar va kompyuter jinoyatlariga nisbatan kengroq bo‘lib, axborotlashtirish sohasidagi barcha jinoyatlarni qamrab oladi.”[7] V.A.Nomokonov va T.L.Tropinaning yuqoridagi fikrlariga to‘liq qo‘shilgan holda shuni ayta olamizki, kiberjinoyat faqatgina kompyuterlar orqali emas, balki jahon axborot tarmog‘iga ulana oladigan vositalar, masalan mobil telefon apparati orqali ham sodir etilishi mumkin. Shuningdek, kiberjinoyat tushunchasiga rus olimlaridan bo‘lgan I.V.Ramanov – Internet tarmog‘iga kirishi mumkin bo‘lgan har qanday vosita orqali davlatga yoki jismoniy va yuridik shaxslarga iqtisodiy, siyosiy, ma’naviy, madaniy va boshqa shaklda zarar yetkazish maqsadidagi ijtimoiy xavfli harakat yoki harakatsizlik deb ta’rif bergan.[8]

[6] https://lex.uz/uz/docs/-5960604 O’zbekiston Respublikasining “Kiberxavfsizlik to’g’risida”gi O’zbekiston Respublikasining Qonuni 3-modda, 15.04.2022 yildagi O‘RQ-764-son

[7] Номоконов В.А, Тропина Т.Л. Киберпреступность как новая криминалная угроза. // Криминология: вчера, сегодня, завтра. – 2012 г. – 1(24). – С47

[8] Романов И.В. Понятие киберпреступлений и его значение для расследование. // Сибирские уголовно-процессуальние и криминалистические чтение. 2016. – С.106

Shu o‘rinda ta’kidlab o‘tishimiz kerakki, global tarmoq jinoyatchiligi tushunchasi unga qadar mavjud bo‘lgan “kompyuter jinoyatchiligi”, tushunchasi bilan to‘la mos kelmaydi va shunga ko‘ra mazkur jinoyatchilik turi bugungi kunda “kiberjinoyatchilik” tushunchasi bilan atalib kelinmoqda. Xalqaro ilmiy va huquqiy amaliyotda dastlab “kompyuter jinoyatchiligi” tushunchasi, keyinchalik “kompyuter bilan bog‘liq jinoyat”, “kompyuter orqali jinoyat sodir etish”, “elektron jinoyatchilik” va “yuqori texnologiyalar jinoyatchiligi”, “virtual jinoyatchilik” tushunchalari ishlatilib, bugunga kunga kelib esa “kiberjinoyatchilik” yoki “global tarmoq jinoyatchiligi” atamasi qo‘llanilmoqda. Ushbu tushunchalar yaratilishidan asosiy maqsad ayni paytda Internet global tarmog‘i orqali sodir etilgan jinoyatchilik chegarasini aniq belgilash va unga qarshi kurashda xos yondashuv zarur ekanligini tushuntirish bo‘lgan deb olim I.To‘raxodjaeva “kiberjinoyatchilikning kompyuter jinoyatchiligidan kengroq tushuncha hisoblanishini” ta’kidlab o‘tadi[9]. Kiberjinoyatlar tushunchasining vaqtga nisbatan o‘zaro bog‘liqligini yana 1979- yilda Dallas advokatlar assosasiyasining konferentsiyasi tomonidan dastlab kompyuter jinoyatlarining asosiy belgilari o‘sha paytdagi mavjud axborot kommunikasiya texnologiyalarining texnik imkoniyatlari yuzasidan belgilanganligi orqali ta’kidlashimiz mumkin[10]. Kiberjinoyatlar yig‘indisi kiberjinoyatchilikni tashkil qiladi va bu L.Bo‘ranovning fikriga ko‘ra, “kiberjinoyatchilik axborot kommunikasiya texnologiyalari sohasidagi ko‘plab turdagi jinoyatlarni o‘zida birlashtirgan jinoyatlar majmuidir”[11] deb o‘z aksini topgan. L.Kochkina kiberjinoyatchilikni “kompyuter ma’lumotlari sohasidagi jinoyatlar”, “axborot jinoyatlari”, “kompyuter uskunalari bilan bog‘liq jinoyatlar”, “yuqori texnologiyalar kompyuterlaridagi jinoyatlar”, “axborot sohasidagi jinoyatlar” deb, tarif berib o‘tadi[12], T.Borodkina ushbu jinoyatlarni axborot sohasidagi jinoyat deb atagandi[13]. Kiberjinoyatlarni tasniflash va ma'lum bir guruhlarga ajratib o‘rganish maqsadga muvofiq. Biroq, kiberjinoyatlarni har kim turlicha tasniflaydi, xususan, Kasperskiy kompaniyasi “ularni elektron pochta va Internet firibgarligi, shaxsiy ma’lumotlarning firibgarligi (shaxsiy ma'lumotlarning o‘g‘irlanishi va noto‘g‘ri ishlatilishi), moliyaviy ma’lumot yoki bank kartasi ma’lumotlarini o‘g‘irlash, korporativ ma’lumotlarni o‘g‘irlash va sotish, kibertovlamachilik, kriptodjeking, kiberjosuslik kabi turlarga ega ekanligini inobatga olib ularni ikkita guruhga kompyuterlarning o‘ziga qaratilgan kiberjinoyatlar va kompyuterdan foydalanilgan holda amalga oshiriladigan kiberjinoyatlarga ajratadi”[14]. Zamonaviy texnologiyalar rivojlanib borgan sari kiberjinoyatlar va kompyuter orqali amalga oshiriladigan jinoyatlar soni ortib bormoqda. O‘z navbatida boshqa olimlar

[9] Toraxodjaeva I. O'zbekistonda Internet tarmog'iorqali sodir etiladigan jinoyatchilikka qarshi kurash muammolari // – T.: Yuridik fanlar axborotnomasi / Vestnik yuridicheskix nauk / Review of law sciences. – ilmiy-amaliy jurnali. 2019 (03)-son. – B.128-132.

[10] Широков В.А., Беспалова Е.В. Киберпреступность: история уголовно-правового противодействия. – М.: “Информационное право”, 2006. № 4. http://center-bereg.ru/h1846.html.

[11] Бўранов Л. Кибержиноятчиликка қарши курашишда интернет-маданиятнинг аҳамияти. 2018 й., https://ictnews.uz/uz/15/05/2018/cybercrime/.

[12] Kochkina L. Definition of the concept “cybercrime”. Selected types of cybercrime // Сибирские уголовнопроцессуальные и криминалистические чтения. 2017. № 3 (17). – С. 2.

[13] Бородкина Т.Н., Павлюк А.В. Киберпреступления: понятие, содержание и меры противодействия. Социально-политические науки. № 1. 2018. – С. 135-137

[14] https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime

zamonaviy kiberjinoyatning boshqa turlari ham mavjud ekanligi to‘g‘risida fikr yuritishmoqda. Quyidalar eng keng tarqalgan kiberjinoyat turlari hisoblanadi:

2.1.Ma’lumotlarni o‘g‘irlash va shaxsiy ma'lumotlarni suiiste’mol qilish

- Phishing hujumlari (Email phishing-soxta elektron pochta xabarlari orqali foydalanuvchilardan shaxsiy ma'lumotlarni talab qilish, SMS phishing - qisqa matnli xabarlar orqali amalga oshiriluvchi hujumlar, Voice phishing- telefon qo‘ng‘iroqlari orqali ma’lumot o‘g‘irlash, Website spoofing- taniqli veb-saytlarning soxta nusxalarini yaratish).[15]
- Identifikatsiyani o‘g‘irlash
- Ma’lumotlar bazasiga ruxsatsiz kirish

2.2. Moliyaviy kiberjinoyatlar

- Bank kartalaridan noqonuniy foydalanish
- Cryptocurrency orqali pul yuvish
- Online to‘lov tizimlariga hujumlar

2.3. Dasturiy ta'minot orqali hujumlar

- Ransomware (tovon dasturlari)
- Trojan dasturlar (Banking trojans -bank ma’lumotlarini o‘g‘irlash, RAT (Remote Access Trojans) - masofaviy boshqaruv, Infostealer – ma’lumot o‘g‘irlash, Dropper - boshqa zararli dasturlarni yuklash).
- Botnet tarmoqlari

2.4. Tizimga zarar yetkazuvchi hujumlar

- DDoS hujumlari (Volume-based attacks- trafik hajmini oshirish, Protocol attacks - tarmoq protokollarini suiiste'mol qilish, Application layer attacks-dastur qatlamiga hujum)
- Veb-saytlarni buzish
- Ma’lumotlarni yo‘q qilish (Logic bombs- belgilangan vaqtda ishlaydigan zararli kod, Wiper malware- ma'lumotlarni butunlay o‘chiradigan dastur, Manual deletion- qo‘lda o‘chirish)[16]. Zamonaviy texnologiyalar rivojlangan sari kiberjinoyatning turlari ko‘payaveradi. Kiberjinoyatlar rivojlanib borgan sari nafaqat individual foydalanuvchilarga, balki biznes va davlat muassasalariga ham katta zarar yetkazadi. Ular iqtisodiy yo‘q otishlar, shaxsiy ma’lumotlarning oshkor bo‘lishi, jamoat xavfsizligiga tahdid solishi mumkin. Ushbu jinoyatlar turli darajalarda jamiyatga salbiy ta’sir ko‘rsatadi:

Iqtisodiy yo‘qotishlar – kompaniyalar va davlat muassasalari kiberjinoyatlar tufayli katta moliyaviy zarar ko‘rishi mumkin. Firibgarlik, tovlamachilik va ma’lumotlar o‘g‘irlanishi natijasida yirik korporatsiyalar milliardlab dollar yo‘qotadi.

Shaxsiy ma’lumotlarning oshkor bo‘lishi – kiberjinoyatlar natijasida foydalanuvchilarning shaxsiy va moliyaviy ma’lumotlari firibgarlar qo‘liga tushishi mumkin, bu esa kredit firibgarligi va shaxsiy hayotga tahdid tug‘diradi.

[15] APWG Phishing Activity Trends Report, Q1 2025
[16] https://uz.wikipedia.org/wiki/Kiberjinoyat

Ijtimoiy ishonchsizlikning ortishi – internetdagi firibgarlik va soxta ma'lumotlarning ko'payishi jamiyatda ishonchsizlikni oshiradi, bu esa odamlarning onlayn xizmatlarga nisbatan shubha bilan qarashiga sabab bo'ladi.

Kiberurush xavfi – davlatlar o'rtasida kiberjosuslik va kiberhujumlar tobora kuchayib bormoqda. Bu esa milliy xavfsizlikka jiddiy tahdid solishi va xalqaro munosabatlarga salbiy ta'sir ko'rsatishi mumkin.

Ishonchli tizimlarning izdan chiqishi – bank tizimlari, davlat xizmatlari va yirik korporativ tarmoqlarga qilingan hujumlar butun jamiyat faoliyatini izdan chiqarishi mumkin.

Ish o'rinlarining yo'qolishi – kiberjinoyatlar tufayli kompaniyalar katta zarar ko'rib, ishchilarni qisqartirishga majbur bo'lishi mumkin.

Psixologik va huquqiy oqibatlar – kiberjinoyat qurbonlari depressiya, stress va boshqa psixologik muammolarga duch kelishadi. Bundan tashqari, huquqiy jarayonlarning murakkabligi jinoyatchilarga qarshi kurashda qo'shimcha qiyinchiliklar tug'diradi . Kiberjinoyatlar tufayli xalqaro darajadagi muammolar ham yuzaga kelmoqda, masalan, kiberurush va transchegaraviy hujumlar. Shu sababli, bu muammolarga qarshi global hamkorlik va ilg'or texnologik himoya choralari talab etiladi[17]. Kiberjinoyatlar tufayli xalqaro darajadagi muammolar ham yuzaga kelmoqda, masalan, kiberurush va transchegaraviy hujumlar. Shu sababli, bu muammolarga qarshi global hamkorlik va ilg'or texnologik himoya choralari talab etiladi.

Natija

Kiberjinoyatlarning ortishi milliy qonunchilik tizimida va xalqaro huquq tizimida yangi qonunlarni yaratishni talab qilmoqda. Amaldagi qonunchiligimizga ko'ra, kiberxavfsizlik va axborot texnologiyalari bilan bog'liq jinoyat turlari sifatida O'zbekiston Respublikasi Jinoyat kodeksining 103-modda 2- qismi "g" bandi, 103^1 -modda 2-qismi "v" bandi, 139-modda 2-qismi, 140-modda 2-qismi, 141^1 -modda, 141^2-modda, 158-modda 3-qismi, 159-modda 1-qismi, 160-modda, 162-modda,165-modda, 167-modda 3-qismi "g" bandi, 168-modda 2-qismi "v" bandi, 169-modda 3-qismi "b" bandi, 177-modda, 188^1 -modda, 189-modda, 191-modda, 192-modda, 194-modda, 215-modda, 216-modda, 216^1 -modda, 216^2 -modda, 217-modda, 228-modda, 229^2 -modda, 230^1- modda, 230^2 -modda, 237-modda, 239-moddam 244^1 -modda 3-qismi "g" bandi, 244^5-modda, 278-modda 3-qismi hamda ushbu kodeksga 2007-yilda kiritilgan XX1-bob ya'ni axborot texnologiyalari sohasidagi jinoyatlarni o'z ichiga oluvchi 278^1-278^7moddalarni nazarda tutiladi. N.S.Salayev va R.N.Ro'ziyevlar o'z monografiyalarida Jinoyat kodeksidagi kompyuter texnologiyasidan foydalanib sodir etiladigan jinoyatlarni obyektiga nisbatan shartli ravishda 11 turga bo'lib o'rganishni nazarda tutishgan.

Axborot texnologiyalari sohasidagi jinoyatlarning ijtimoiy xavflilik darajasi yuqori bo'lganligi tufayli, ularning oldini olish va unga qarshi kurashish uchun butun davlatimiz siyosati darajasida e'tibor berilib, axborotni muhofaza qilish va uni kiberhujumlardan saqlash maqsadida o'nlab normativ-huquqiy hujjatlar, shu jumladan, O'zbekiston Respublikasining

[17] https://www.uzmarkaz.uz/en/news/kibermakondagi-jinoyatlar-va-ularning-oldini-olish-choralari

“Axborotlashtirish to‘g‘risida”gi Qonuni (2003), “Elektron hujjat aylanishi to‘g‘risida”gi Qonuni (2004), “Kiberxavfsizlik to‘g‘risida”gi Qonuni (2022), “Davlat sirlarini saqlash to‘g‘risida”gi Qonuni (1993), O‘zbekiston Respublikasi Prezidentining “Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirishga oid qo‘shimcha chora-tadbirlar to‘g‘risida”gi PQ-4452-sonli qarori (2019), O‘zbekiston Respublikasi Prezidentining “Raqamli O‘zbekiston – 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish to‘g‘risida”gi PF-6079-sonli farmoni (2020) kabi yana o‘nga yaqin qonun hujjatlari qabul qilindi. Yuqorida keltirilgan normativ-huquqiy hujjatlar ichida sohani tartibga solishga qaratilgan maxsus qonun hujjati bu 2022-yil 15-aprelda qabul qilingan hamda mazkur yilning 17-iyulida kuchga kirgan “Kiberxavfsizlik to‘g‘risida”gi O‘zbekiston Respublikasining O‘RQ 764-sonli Qonunidir. Kiberjinoyatchilikka qarshi kurashda va oldini olishda bitta davlatda qabul qilingan qonun va harakatlar orqali iijobiy natijaga erishi bulmaydi balki umummiliy xalqaro miqyosda xamkorlik, davlatlararo ushbu sohaga tegishli yagona huquqiy tizimni ishlab chiqish, xalqaro standartlardan keng foydalanish va tergov jarayonlarida tatbiq etishdan iborat bo‘ladi. Kiberjinoyatlar xalqaro maydonda ham sodir etilayotgani turli davlatlarni hamkorlikka chaqirmoqda. Shujumladan, O‘zbekiston ham a’zolardan biri bo‘lgan Shanxay Hamkorlik Tashkiloti (SHHT) hamda Mustaqil Davlatlar Hamdo‘stligi (MDH) davlatlari bilan hamkorlikni o‘rnatgani va muhim normativ-hujjatlarni qabul qilgani muhim ahamiyatga ega desak mubolag‘a bo‘lmaydi. Shanxay Hamkorlik Tashkilotining 2009-yil 16-iyundagi (2021-yil 5 yanvarda kuchga kirgan) “Xalqaro axborot (kiber) xavfsizligini ta’minlash sohasida hamkorlik to‘g‘risidagi kelishuvi” AKT munosabatlarini tartibga solishda samarali mexanizm sifatida tan olindi va hamkorlik o‘rnatildi (Rossiya, Yekaterinburg). Mazkur SHHTning kelishuvda, xususan, quyidagi asosiy masalalar asosiy tushunchalar, xalqaro axborot xavfsizligini ta’minlash sohasidagi asosiy tahdidlar, hamkorlikning asosiy yo‘nalishlari, hamkorlikning umumiy prinsiplari, hamkorlikning asosiy shakllari va mexanizmlari, axborotning himoyasi, moliyalashtirish, xalqaro shartnomalarga munosabatda nizolarni hal qilish, ishlash tili, depozitariy va yakuniy qoidalar nazarda tutilgan bo‘lsa hamkorlikning asosiy yo‘nalishlari sifatida quyidagilar belgilandi: 1) xalqaro axborot xavfsizligini ta’minlash sohasida zarur qo‘shma chora tadbirlarni belgilash, muvofiqlashtirish va amalga oshirish; 2) ushbu sohada yuzaga keladigan tahdidlarga monitoring va birgalikda javob berish tizimini yaratish; 3) mudofaa qobiliyatiga, milliy va jamoat xavfsizligiga tahdid soluvchi axborot qurollarining tarqalishi va qo‘llanilishini cheklash sohasida xalqaro huquq normalarini ishlab chiqish bo‘yicha qo‘shma chora-tadbirlarni ishlab chiqish; 4) axborot-kommunikatsiya texnologiyalaridan terroristik maqsadlarda foydalanish tahdidlariga qarshi kurashish; 5) axborot jinoyatlariga qarshi kurashish; 6) ushbu Bitim maqsadlari uchun zarur bo‘lgan axborot xavfsizligi sohasida ekspertiza, tadqiqotlar va baholashni o‘tkazish; 7) global internet tarmog‘ining xavfsiz, barqaror ishlashi va boshqaruvini xalqarolashtirishga ko‘maklashish; 8) tomonlar davlatlarining o‘ta muhim tuzilmalarining axborot xavfsizligini

ta’minlash va boshqalar[18]. Mustaqil davlatlar hamdo‘stligi davlatlari-ishtirokchilari tomonidan 2018 yil 28 sentyabr kuni “Mustaqil Davlatlar Hamdo‘stligiga (MDH) a’zo davlatlar o‘rtasida axborot texnologiyalari sohasidagi jinoyatlarga qarshi kurashish bo‘yicha hamkorlik to‘g‘risida kelishuv” imzolandi (Tojikiston, Dushanbe). Ushbu uchrashuvda axborotni yo‘q qilish, bloklash, o‘zgartirish yoki nusxalash, qonun bilan himoyalangan kompyuter ma’lumotlariga ruxsatsiz kirish orqali axborot (kompyuter) tizimini buzish, zararli dasturlarni yaratish, ulardan foydalanish yoki tarqatish, kompyuter tizimiga kirish huquqiga ega bo‘lgan shaxs tomonidan kompyuter tizimidan foydalanish qoidalarini buzish, natijada qonun bilan qo‘riqlanadigan kompyuter ma’lumotlarining yo‘q qilinishi, bloklanishi yoki o‘zgartirilishi, agar bu harakat jiddiy zarar yoki og‘ir oqibatlarga olib kelgan bo‘lsa, kompyuter tizimida qayta ishlangan, mashina tashuvchilarida saqlanadigan yoki ma’lumotlar uzatish tarmoqlari orqali uzatiladigan ma’lumotlarni o‘zgartirish yoki kompyuter tizimiga noto‘g‘ri ma’lumotlarni kiritish yoki qonun bilan himoyalangan kompyuter ma’lumotlariga ruxsatsiz kirish bilan bog‘liq bo‘lgan mulkni o‘g‘irlash, “Internet” axborot-telekommunikatsiya tarmog‘i yoki boshqa elektr aloqa kanallari orqali voyaga yetmagan shaxs tasviri bilan pornografik materiallar yoki pornografik xususiyatdagi narsalarni tarqatish, mualliflik huquqi ob’ektlari bo‘lgan kompyuter tizimlari va ma’lumotlar bazalari uchun dasturlardan noqonuniy foydalanish, shuningdek, agar bu qilmish katta zarar yetkazgan bo‘lsa, mualliflik huquqini o‘zlashtirib olish, “Internet” axborot-telekommunikatsiya tarmog‘i yoki boshqa elektr aloqa kanallaridan foydalangan holda, belgilangan tartibda ekstremistik deb e’tirof etilgan yoki terrorchilik faoliyatini amalga oshirishga yoki terrorizmni oqlashga chaqiriqlarni o‘z ichiga olgan materiallarni tarqatish kabi harakatlar axborot texnologiyalari sohasidagi jinoiy qilmishlar deb tan olinadi. Bunday uchrashuvlar qatoriga, jumladan, 2015-yilning 20, 21-may kunlari Yevropada Xavfsizlik va Hamkorlik Tashkilotining ko‘magida mamlakatimiz poytaxti Toshkentda “Kiberolam va axborot-kommunikatsiya texnologiyalari (AKT) sohasida xavfsizlik” mavzusida tashkil etilgan va o‘tkazilgan seminarni, 2021-yilning 29-iyun kuni Toshkent shahrida O‘zbekiston Prezidenti huzuridagi Strategik va mintaqalararo tadqiqotlar instituti tomonidan Axborot texnologiyalari va kommunikasiyalarini rivojlantirish vazirligi hamda MDH Ijroiya qo‘mitasi ko‘magida tashkil etilgan va o‘tkazilgan Axborot xavfsizligi bo‘yicha MDH xalqaro ekspert forumini va boshqa xalqaro uchrashuvlarni kiritish mumkin.

Muhokama

Tadqiqot natijalari shuni ko‘rsatadiki, kiberjinoyatchilik bugungi kunda nafaqat texnik, balki jiddiy huquqiy va ijtimoiy muammodir. Kiberjinoyat tushunchasining an’anaviy kompyuter jinoyatlaridan ko‘ra kengroq talqin qilinishi, uning global tarmoqqa ulangan barcha qurilmalarni qamrab olishi bilan izohlanadi.

Huquqiy muvofiqlik va blanket normalar

O‘zbekiston Respublikasi Jinoyat kodeksida kiberjinoyatlarga oid moddalarning mavjudligi ijobiy holat bo‘lsa-da, ularning aksariyati blanket normalar hisoblanadi. Bu esa

[18] **Shakurov R. R., Vohidov M. M.** *Kiber huquq – huquq sohasi sifatida.* – Toshkent, 2022. – 15 bet.

huquqni muhofaza qiluvchi organ xodimlaridan nafaqat yuridik, balki yuqori darajadagi axborot-texnologik bilimlarni ham talab etadi. Masalan, kiberjinoyat tarkibini aniqlash uchun “Kiberxavfsizlik to‘g‘risida”gi qonun va boshqa texnik reglamentlarga murojaat qilish zarurati yuzaga kelmoqda.

Transchegaraviy xususiyat va xalqaro hamkorlik

Kiberjinoyatchilikning chegarasiz ekanligi (transchegaraviyligi) bir davlat doirasida qabul qilingan choralar bilan unga qarshi samarali kurashib bo‘lmasligini ko‘rsatadi. O‘zbekistonning SHHT va MDH doirasidagi kelishuvlarga a’zo bo‘lishi bu boradagi muhim qadamdir. Ayniqsa, axborot-kommunikatsiya texnologiyalaridan terroristik va ekstremistik maqsadlarda foydalanishga qarshi birgalikda kurashish masalasi mintaqaviy xavfsizlik uchun strategik ahamiyatga ega.

Ijtimoiy-iqtisodiy oqibatlar

Kiberhujumlarning iqtisodiy zarari yildan-yilga ortib borayotgani (2028-yilga kelib 13,82 trillion dollar) ushbu sohada profilaktika choralarini kuchaytirishni taqozo etadi. Moliyaviy yo‘qotishlardan tashqari, kiberjinoyatlar jamiyatda raqamli xizmatlarga nisbatan ishonchsizlikni keltirib chiqarishi va shaxsning psixologik holatiga salbiy ta’sir ko‘rsatishi aniqlandi.

Takliflar

Tahlillar asosida quyidagi xulosalarga kelish mumkin:

Qonunchilikni takomillashtirish: Jinoyat kodeksidagi kiberjinoyatlarga oid normalarni texnologik taraqqiyotga mos ravishda yanada aniqlashtirish va yangi turdagi kiberhujumlar (masalan, kriptodjeking) uchun javobgarlikni belgilash lozim.

Raqamli savodxonlik: Kiberjinoyat qurboniga aylanmaslik uchun fuqarolarning kiber-ogohligini oshirish va shaxsiy ma’lumotlarni himoya qilish bo‘yicha ta’lim dasturlarini kengaytirish zarur.

Texnik va huquqiy uyg‘unlik: Yuristlar va kiberxavfsizlik mutaxassislari o‘rtasida doimiy muloqot platformasini yaratish, texnik harakatlarni yuridik tilga to‘g‘ri o‘girish (kvalifikatsiya qilish) sifatini oshiradi.

Xulosa

Internet va raqamli texnologiyalarning rivojlanib borgan sari kiberjinoyatlar nafaqat jismoniy shaxslar, balki yirik kompaniyalar, davlatlar va butun jamiyatlar uchun ham katta xavf tug‘dirmoqda. Kiberjinoyatlar turli shakllarda namoyon bo‘lib, ular internetdagi individual ma’lumotlarni o‘g‘irlashdan tortib, global miqyosdagi kiberhujumlarga qadar kengaymoqda. Bu o‘z navbatida, kiberxavfsizlik va himoya choralarini kuchaytirishni talab qiladi. Kiberjinoyatlar nafaqat individual shaxslar, balki kompaniyalar va davlatlar uchun jiddiy xavf tug‘dirmoqda. Ularning oldini olish va samarali kurashish uchun ilg‘or texnologiyalarni qo‘llash, foydalanuvchilarga foydalanish bo‘yicha ta’lim berish, xalqaro hamkorlikni kuchaytirish va xavfsizlik protokollarini takomillashtirish va kiberjinoyatlarning iqtisodiy va ijtimoiy ta’siri juda katta bo‘lganligi sababli, ularning oldini olish bo‘yicha ko‘plab ilmiy va amaliy tadqiqotlar olib borish zarur. Biroq, kiberxavfsizlik sohasida hali

ko‘plab yutuqlarga erishish kerak. Fikrimizcha, avvalo bu kabi jinoyatlarning qurboniga aylanib qolmaslik uchun, har bir fuqarolardan ogohlik talab etiladi. Zero, agar shaxs kompyuterida saqlanayotgan axborotlar xavfsligini ta’minlash choralarini ko‘rishi va shaxsiy ma’lumotlarini ishonchli tarzda saqlash imkoniyatiga egadir. Xulosa qilib aytganda, kompyuter tizimlariga qarshi jinoyatlar o’ta dinamik xususiyatga ega bo‘lib jinoyatchilar doimo qonundan bir qadam oldinda yurishga harakat qilishadi. O‘zbekiston jinoyat kodeksining ushbu sohaga oid normalar blanket normalar hisoblanadi ya’ni ushbu jinoyatlarning to’liq tarkibini tushunish uchun “kiberxavfsizlik to‘g‘risidagi qonunga va boshqa texnik reglamentlarga murojaat qilish talab etiladi. Yuristlar uchun asosiy vazifa - texnik harakatni to‘g‘ri yuridik tilga o‘girish va tegishli kvalifikatsiya qilishdir.

Foydalanilgan adabiyotlar

1 https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

2 https://lex.uz/uz/docs/-5960604 O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi O‘zbekiston Respublikasining Qonuni 3-modda, 15.04.2022 yildagi O‘RQ-764-son

3 Номоконов В.А, Тропина Т.Л. Киберпреступность как новая криминалная угроза. // Криминология: вчера,
сегодня, завтра. – 2012 г. – 1(24). – С47

4 Романов И.В. Понятие киберпреступлений и его значение для расследование. // Сибирские уголовно-
процессуальние и криминалистические чтение. 2016. – С.106

5 Toraxodjaeva I. O‘zbekistonda Internet tarmog‘iorqali sodir etiladigan jinoyatchilikka qarshi kurash muammolari // – T.: Yuridik fanlar axborotnomasi / Vestnik yuridicheskix nauk / Review of law sciences. – ilmiy-amaliy jurnali. 2019 (03)-son. – B.128-132.

6 Широков В.А., Беспалова Е.В. Киберпреступность: история уголовно-правового противодействия. – М.: “Информационное право”, 2006. № 4. http://center-bereg.ru/h1846.html.

7 Бўранов Л. Кибержиноятчиликка қарши курашишда интернет-маданиятнинг аҳамияти. 2018 й., https://ictnews.uz/uz/15/05/2018/cybercrime/.

8 Kochkina L. Definition of the concept “cybercrime”. Selected types of cybercrime // Сибирские уголовнопроцессуальные и криминалистические чтения. 2017. № 3 (17). – С. 2.

9 Бородкина Т.Н., Павлюк А.В. Киберпреступления: понятие, содержание и меры противодействия. Социально-политические науки. № 1. 2018. – С. 135-137

10 https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime

11 APWG Phishing Activity Trends Report, Q1 2025

12 https://uz.wikipedia.org/wiki/Kiberjinoyat

13 https://www.uzmarkaz.uz/en/news/kibermakondagi-jinoyatlar-va-ularning-oldini-olish-choralari

14 **Shakurov R. R., Vohidov M. M.** Kiber huquq – huquq sohasi sifatida. – Toshkent, 2022. – 15 bet.