AXBOROT-KOMMUNIKATSIYA TEXNOLOGIYALARI RIVOJI FONIDA KIBERJINOYATLAR KO‘LAMINING KENGAYISHI: KRIMINOLOGIK TAHLIL VA ZAMONAVIY QARSHI KURASHISH STRATEGIYALARI

Maqsudaliyeva Muxlisa Muzaffarjon qizi	O‘zbekiston Respublikasi IIV Akademiyasi 2-o‘quv kursi 204-guruh kursanti gmail: muxlisaxonmaqsudaliyeva@gmail.com
T.E. Masharipov	Ilmiy rahbar: IIV Akademiyasi Tezkor-qidiruv faoliyati kafedrasi katta o‘qituvchisi, mayor gmail: masaripovtohir@gmail.com.

Annotatsiya

Mazkur maqolada axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi fonida kiberjinoyatlar ko‘lamining kengayishi kriminologik jihatdan tahlil qilingan. Kiberjinoyatlarning zamonaviy shakllari, ularning ijtimoiy xavfliligi, jinoyat sodir etish mexanizmlari hamda sabab-sharoitlari o‘rganilgan. Shuningdek, milliy qonunchilik va xalqaro tajriba asosida kiberjinoyatlarga qarshi kurashishning zamonaviy strategiyalari ishlab chiqilgan. Tadqiqot natijasida profilaktik, tashkiliy va texnologik choralarni kuchaytirish zarurligi asoslab berilgan.

Kalit so’zlar kiberjinoyat, kriminologiya, axborot xavfsizligi, raqamli iqtisodiyot, ijtimoiy muhandislik, profilaktika, kiberxavfsizlik strategiyasi.

Аннотация. В статье проводится криминологический анализ расширения масштабов киберпреступности на фоне стремительного развития информационно-коммуникационных технологий. Рассматриваются современные формы киберпреступлений, их общественная опасность, механизмы совершения и детерминирующие факторы. На основе национального законодательства и международного опыта предлагаются современные стратегии противодействия киберпреступности. Обосновывается необходимость усиления профилактических, организационных и технологических мер

Ключевые слова: киберпреступность, криминология, информационная безопасность, цифровая экономика, социальная инженерия, профилактика, стратегия кибербезопасности.

Abstract: This article provides a criminological analysis of the expansion of cybercrime in the context of rapid development of information and communication technologies. The study examines modern forms of cybercrime, their social danger, mechanisms of commission, and determining factors. Based on national legislation and international experience, modern strategies for combating cybercrime are proposed. The research substantiates the need to strengthen preventive, organizational, and technological measures.

Keywords: cybercrime, criminology, information security, digital economy, social engineering, prevention, cybersecurity strategy.

Kirish

Bugun hayotimizning barcha sohalariga kirib kelgan axborot kommunikatsiya texnologiyalari tizimini rivojlantirish, bu sohaga oid xalqaro va mintaqaviy munosabatlarda ishtirok etish hamda mazkur sohani zamonaviy kibertahdidlardan himoya qilishni taqozo etadi. Raqamli texnologiyalar jadal rivojlanayotgan bugungi davrda internet va axborot-kommunikatsiya tizimlari jamiyat hayotining ajralmas qismiga aylandi. Onlayn bank xizmatlari, elektron savdo, masofaviy ta'lim va ijtimoiy tarmoqlar qulaylik yaratishi bilan birga, yangi turdagi jinoyatchilik — kiberjinoyatchilikning kengayishiga ham sabab bo'lmoqda. Kiberjinoyatlar nafaqat alohida fuqarolarga, balki davlat va yirik tashkilotlarga ham katta iqtisodiy zarar yetkazmoqda. Endilikda jinoyatchilik nafaqat an'anaviy makonda, balki virtual muhitda ham keng tus olgan. Tadqiqotlar doirasida kiberjinoyatchilkning determinantlari, uning ijtimoiy xavflilik darajasi, transmilliy xususiyati hamda profilaktik va institutsional mexanizmlar muhokama qilinadi. Kiberjinoyatchilik bugungi kunda milliy xavfsizlik, iqtisodiy barqarorlik va shaxsiy ma'lumotlar daxlsizligiga jiddiy tahdid solmoqda. Shu bois mazkur muammoni kriminologik jihatdan tahlil qilish va samarali qarshi kurashish strategiyalarini ishlab chiqish dolzarb masalalardan biridir. Kriminologik jihatdan, kiberjinoyatchi ko'pincha yuqori darajali bilimga ega, lekin ijtimoiy mas'uliyat darajasi past shaxs sifatida tavsiflanadi.

Kiberjinoyatlar tushunchasi va turlari: Insonning har bir qilgan jinoyati uchun jazo muqarrardir. Shuningdek, hozirda kiberjinoyat qilgan insonlar soni tobora ortib bormoqda. Kiberjinoyatchilar uchun ushbu turdagi jinoyatlarni oldini olish uchun ko'plab chora tadbirlar ko'rilmoqda. 1994-yil 22-sentabrda qabul qilingan Jinoyat kodeksi ham javobgarlik masalasi alohida belgilab qo'yilgan. "Axborotlashtirish to'g'risida"gi qonun va 2001-yilda qabul qilingan Budapest Conventation on Cybecrime kiberjinoyatlarga qarshi xalqaro huquqiy asoslardan biri sifatida e'tirof etsak mubolag'a bo'lmayd. Bundan tashqari, O'zbekiston Respublikasining 2022-yil 15-aprel kuni qabul qilingan O'RQ-764-sonli "Kiberxavfsizligi to'g'risida"gi qonuni bilan tartibga solingan. Ushbu qonunga asosan biz birinchi navbatda kiberjinoyatlar va kiberhimoya tushunchasiga to'xtalib o'tishimiz lozim. Kiberjinoyatlardan qay tarzda himoyalanishimizni bilib qo'yishimiz darkor.

Kiberjinoyatlar — bu axborot texnologiyalari, kompyuter tizimlari yoki internet tarmoqlari orqali sodir etiladigan noqonuniy harakatlardir va shu o'rinda aytib o'tishimiz mumkinki, axborotni egallash, uni o'zgartirish, yo'q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta'minot va texnik vositalardan foydalanilib amalga oshirilmoqda.

Kiberhimoya — kiberxavfsizlik hodisalarining oldini olishga, kiberhujumlarning oqibatlarini bartaraf etishga, telekommukiatsiya tarmoqlari, axborot tizimlari hamda resurslari faoliyatining barqarorligini va ishonchliligini tiklashga qaratilgan huquqiy, tashkiliy, moliyaviy-iqtisodiy, muhandislik-texnik chora-tadbirlar,shuningdek ma'lumotlarni kriptografik va texnik jihatdan himoya qilish chora-tadbirlar majmuidir. Telekommukatsiya tarmoqlari va aloqa kanallaridagi

tezkor-qidiruv tadbirlari tizimining kiberxavfsizligini ta’minlash alohida qonunchilik hujjatlarida belgilangan tartibda amalga oshiriladi.

Kiberjinoyatlar soni juda ko’p bo’lganligi sababli ularni tasniflash va ma’lum bir guruhlarga ajratib o’rganish maqsadga muvofiq hisoblanadi. Hozirgi zamonda uning quyidagi turlari keng tarqalgan:

– Phishing[1] (soxta xabarlar orqali aldash) – taxminan 35–40 %
– Ransomware[2] (ma’lumotni bloklab, pul talab qilish) – 20–30 %
– Bank kartalari va onlayn to‘lov firibgarligi – 15–20 %
– Shaxsiy ma’lumotlarni o‘g‘irlash (data breach) – 10–15 %
– DDoS hujumlar- 5%
– Boshqa turdagi zararli dasturlar va xakerlik hujumlari – 10 % atrofida.

Hozirda bulardan tashqari, kiberterrorizm va ekstremizm turi ham keng tarqalib bormoqda. Ijtimoiy tarmoqlarda (Instagam, telegram, facebook) insonlarning qarindoshi, qo’shnisi, tanishi degan yolg’on so’zlar bilan aldab, ishonchiga kirib olib noqonuniy ravishda telefonlariga silka orqali ulanib olib pullarini yechib, o’zlashtirib olishayotgan odamlarni ham uchratyapmiz.

Bugungi kunda kiberjinoyatlar nafaqat alohida shaxslarga, balki davlat idoralari, bank tizimlari va yirik kompaniyalarga ham jiddiy zarar yetkazmoqda. Asosan bularga fuqarolarning huquqiy bilimlari yetishmasligi sabab kelib chiqmoqda. Fuqarolar kundan kunga kiberjinoyatlarning qurboniga aylanib borishmoqda. Kiberjinoyatchilik shaxs, texnologik muhit va motivatsion omillar o’zaro ta’sirining mahsuli sifatida qaraladi. Kiberjinoyatchilar ko’pincha texnik sohada yetarli bilim va ko’nikmaga ega, yosh va anonimlik imkoniyatlardan foydalanishga moyil shaxslar hisoblanadi. Jinoyatchilar virtual muhitda jinoyat sodir etayotgani sababli ham o’zlarini erkin tutadi, javobgarlik sezgisi pasayadi va jinoyat sodir etish ehtimoli ortadi.

Kiberjinoyatlar ko‘lamining kengayish sabablari: Bugungi kunda O‘zbekiston Respublikasi Konstitutsiyasida mustahkamlangan internet jahon axborot tarmoqlaridan cheklanmagan tarzda foydalanishga fuqorolarimizga sharoitlar yaratib berilishi natijasida bundan kiberjinoyatchilar o‘zlarining jinoiy rejalarini amalga oshirmoqda va bu jinoyatlar insonlar iqtisodiy ahvollariga ko‘rinmas zarba bergan holda oilaviy shart-sharoitlarini yomonlashtirib qo‘ymoqda.

Kriminologik tadqiqotlar shuni ko‘rsatadiki, kiberjinoyatchilar ko‘pincha yuqori texnik savodxonlikka ega bo‘lib, ularning asosiy motivatsiyasi moliyaviy manfaatdorlik hisoblanadi. AKT rivojlanishi bilan birga kiberjinoyatlar soni ham tobora oshib bormoqda. Bunga quyidagi omillar sabab bo‘lmoqda:

– Raqamlashtirish jarayoni tobora tezlashib borayotganligi davlat xizmatlari, bank operatsiyalari va savdo jarayonlari onlayn shaklga o‘tmoqda;

– Aholining raqamli savodxonligi yetarli emasligi – ko‘plab foydalanuvchilar internet xavfsizligi qoidalarini bilmasligi;

– Anonimlik imkoniyati – internet orqali jinoyatchilar o‘z shaxsini yashirish imkoniga ega;

[1] phishing — bu internet orqali “yem tashlab”, foydalanuvchini tuzoqqa tushirish jarayonidir.
[2] ransomware — bu ma’lumotlarni “garovga olib”, evaziga pul so‘raydigan kiberjinoyat vositasidir.

– Yoshlar orasida texnologiyalar va ijtimoiy tamoqlarga qiziqishi, lekin huquqiy bilimlarning yetarli emasligi.

Xalqaro tashkilotlar, jumladan Interpol va United Nations Office on Drugs and Crime ma’lumotlariga ko‘ra, so‘nggi yillarda kiberjinoyatlar global miqyosda eng tez o‘sayotgan jinoyat turlaridan biriga aylangan.

Kriminologik tahlil: Kriminologik nuqtai nazardan qaraydigan bo’lsak bugungi kunda (kiberjinoyatchilikning statistikasi)[3] (2021-2025):

– Oxirgi besh yilda O‘zbekistonda **kiberjinoyatlar soni 10–11 barobar oshdi**.

nuqtai nazar 2021-yilda jami **4 865 ta**, 2025-yilda esa **62 440 ta** kiberjinoyat qayd etildi.

– Shu davrda fuqarolarga yetkazilgan zarar jami **3.7 trillion**[4] **so‘mga** etdi.

– Joriy 11 oy ichida O‘zbekistonliklar kiberjinoyatlar tufayli **1.89 trillion so‘m zarar ko‘rdi**.

Kriminologik dan kiberjinoyatchilikning o‘ziga xos jihatlari mavjud:

– Jinoyatchilarning yoshi ko‘pincha yoshlar orasida bo‘lishi;

– Yuqori texnik bilim va dasturlash ko‘nikmalarining mavjudligi;

– Jinoyatni masofadan turib amalga oshirish imkoniyati;

– Zarar ko‘lami keng va tez tarqaluvchi xususiyatga ega;

Kiberjinoyatlar ko‘pincha iqtisodiy manfaat olish maqsadida sodir etiladi, biroq siyosiy, mafkuraviy yoki shaxsiy adovat sababli ham amalga oshirilishi mumkin. Bundan tashqari, 2022-yilda toshkentliklar kiberjinoyatlardan 45,2 mlrd so‘m zarar ko‘rdi. Toshkentda fuqarolarning bank kartalaridagi pullarini aldov yo‘llari bilan o‘zlashtirish holatlari keskin oshdi. 2022-yilda bunday kiberjinoyatlar oqibatida toshkentliklar kamida 45,2 mlrd so‘m zarar ko‘rgan. Bu pullarning bor-yo‘g‘i 9,2 mlrd so‘mga yaqini undirib berilgan.[5]

Zamonaviy qarshi kurash strategiyalari: O’zbekiston kiberjinoyatchilikka qarshi kurashish uchun huquqiy va tashkiliy chora-tadbirlarni faol ravishda amalga oshirib kelmoqda. Xususan, 2025-yil 30-aprel kuni qabul qilingan Prezident farmoni (PF-153-son) kiberjinoyatchilikka qarshi kurashishni mustahkamlashga qaratilgan bo’lib, bu sohada ichki ishlar vazirligi asosiy vakolatli organ qilib belgilangan. Farmonga muvofiq, banklar, to’lov tizimlari operatorlari va to’lov tashkilotlari mijozlarining moliyaviy xavfsizligini ta’minlashga majburdir. Shu bilan birga, kiberjinoyatlarni amalga oshirish uchun o’z nomidagi bank kartasi, hisob raqami yoki SIM-kartadan foydalanishga yo’l qo’ygan shaxslarga ma’muriy va jinoiy javobgarlik joriy qilingan. Markaziy bank “moliyaviy piramida” firibgarlik sxemalarini aniqlash va oldini olish uchun maxsus tizimni joriy qilmoqda, bu esa fishing hujumlarining ko’payishiga qarshi muhim qadamlardan biri hisoblanadi. Kiberxavfsizlik markazi va Ichki ishlar vazirligining Kiberjinoyatchilikka qarshi kurashish bo;limi ham kiberhujumlarni monitoring qilish, ularning manbalarini aniqlash va tezkor javob berish bilan shug’ullanmoqda. Masalan, 2024-yilda ushbu tashkilotlar 500dan ortiq

[3] https://kun.uz/63123328?utm_source=chatgpt.com

[4] https://uz.kursiv.media/uz/2025-12-24/ozbekistonliklar-bir-yilda-kiberjinoyatlar-tufayli-qanchaga-chuv-tushdi/?utm_source=chatgpt.com

[5] http://imrconf.com/index.php/CGRP/article/view/436/379

fishing saytlarini aniqlab,ularni bloklagan[6], bu esa mamlakatdagi kiberxavfsizlikni mustahkamlash yo'lida muhim qadam bo'lgan. Shu bilan birga, ushbu chora-tadbirlarga qaramay kiberxavfsizlik infratuzilmasidagi muammolar, xususan, malakali mutaxassislarning yetishmasligi va texnik resurslarning cheklanganligi muammoni yanada murakkablashtirib bormoqda. Kiberjinoyatchilikka qarshi kurashish bo'yicha dunyo mamlakatlari tomonidan huquqiy, texnik va profilaktik yo'nalishlarda bir qator chora tadbirlar amalga oshirilmoqda. Kiberjinoyatchilikning oldini olish uchun turli texnik himoya choralarini kuchaytirishimiz lozim. Misol uchun, oddiy telefonimizda autentifikatsiya tizimini yoqishimiz, ma'lumotlarni shifrlashimiz, kiberxavfsizlik monitoring tizimlari va sun'iy intellekt asosida tahdidlarni aniqlash lozim.

Bundan tashqari, kiberxavfsizlikka qarshi kurashhish xodimlari aholi o'rtasida axborot xavfsizligi bo'yicha targ'ibot ishlari olib borishi jinoyatchilikni oldini olishda katta rol o'ynaydi. Davlat tomonidan ta'lim muassalarida kiberxavfsizlik fanlarini joriy etish hamda ushbu soha asosida ishlovchi yuqori malakali mutaxassislarni tayyorlash lozim. Bulardan tashqari, kiberjinoyatga oid milliy qonunchilikni takomillashtirish, jazo tizimini kuchaytirish, elektron dalillar bilan ishlash tartibini aniqlashtirish, xalqaro standartlarga mos normativ bazani shakllantirish, xalqaro hamkorlikni rivojlantirish, tezkor axborot almashinuvini yo'lga qo'yish juda muhim sanaladi. Kiberjinoyatlarga qarshi kurashish uchun kompleks yondashuv zarur. Quyidagi strategiyalar muhim hisoblanadi:

1. Huquqiy bazani takomillashtirish – axborot xavfsizligiga oid qonunchilikni kuchaytirish;
2. Kiberxavfsizlik tizimlarini rivojlantirish – davlat va xususiy sektor hamkorligini yo‘lga qo‘yish;
3. Raqamli savodxonlikni oshirish – aholiga internetdan xavfsiz foydalanish qoidalarini o‘rgatish;
4. Xalqaro hamkorlikni kengaytirish – transmilliy jinoyatlarga qarshi birgalikda kurashish;

Texnologik himoya vositalaridan foydalanish – kuchli parollar, ikki bosqichli autentifikatsiya, antivirus dasturlar;

Xulosa

Xulosa qilib aytganda, har qanday ijobiy taraqqiyot bilan birga uning soyasida zarar yetkazuvchi illatlar ham ildiz otib boradi. O‘zbekistonda raqamli sohaning kengayishi, internetdan cheklanmagan tarzda foydalanish imkoniyatlarining berilishi ham ayrim jinoyatchilar tomonidan suiiste'mol qilinib, fuqarolarning moliyaviy va shaxsiy xavfsizligiga tahdid tug‘dirib kelmoqda. Bugungi kunda kibermakon jinoyatlarining o‘sishi bank kartalaridan noqonuniy pul yechish, yolg‘on bank xodimi sifatida qo‘ng‘iroq qilish, zararli APK-fayllar tarqatish kabi usullar orqali amalga oshirilmoqda. AKT rivoji taraqqiyoti uchun katta imkoniyatlar yaratmoqda. Biroq bu jarayon bilan birga kiberjinoyatchilik ham murakkablashib bormoqda. Kiberjinoyatchilik zamonaviy jamiyatning eng murakkab va tez o'zgaruvchan xavf omillaridan biridir. Axborot-kommunikatsiya texnologiyalarining jadal rivoji insoniyat hayotini yengillashtirgan bo‘lsa-da, kiberjinoyatlar xavfini ham keskin oshirdi.

[6] https://phoenixpublication.net/index.php/TTVAL/article/view/6597

Kiberjinoyatlar o’zining transmilliyligi, anonimligi, yuqori latentligi va texnologik murakabligi bilan an’anaviy jinoyatlardan keskin faqr qiladi. Ular ko’plab insonlarga zarar yetkazmoqda. Ayniqsa,phishing, ransomware, ma’lumotlar sizib chiqishi va sun’iy intellekt yordamida amalga oshirilayotgan ijtimoiy muhandislik hujumlari zamonaviy kiberjinoyatcholikning eng xavfli ko’rinishlariga aylanmoqda. Ularning oldini olish uchun nafaqat huquqni muhofaza qiluvchi organlar, balki har bir foydalanuvchi ham mas’uliyatli bo‘lishi zarur. Raqamli xavfsizlik madaniyatini shakllantirish — zamonaviy jamiyatning ustuvor vazifalaridan biridir.

Foydalanilgan adabiyotlar:

1. O’zbekiston Respublikasining 2022-yil 15-aprel kuni qabul qilingan O’RQ-764-sonli “Kiberxavfsizligi to’g’risida”gi qonuni. – Toshkent, 2022.

2 United Nations. Cybersecurity and Cybercrime Reports. – New York, 2020–2024.

3. Interpol. Global Cybercrime Strategy Documents. – Lyon, France.

4.O‘zbekiston Respublikasi Axborot xavfsizligi to‘g‘risidagi normativ-huquqiy hujjatlar to‘plami. – T., 2021–2024.

5.O‘zbekiston Respublikasi Jinoyat kodeksi. – Tashkent, 2022.

6.O‘zbekiston Respublikasi Axborotlashtirish va kiberxavfsizlik bo‘yicha normativ-huquqiy hujjatlar. – Tashkent, 2021–2025.

7.O‘zbekiston Respublikasi “Axborotlashtirish to‘g‘risida”gi qonuni. – Toshkent, 2020.

8. Budapest Convention on Cybercrime. – Council of Europe, 2001

9. O‘zbekiston Respublikasi Prezidentining raqamli iqtisodiyotni rivojlantirish bo‘yicha farmonlari. – Toshkent, 2021–2025.

10. https://lex. uz/uz/docs/-5960604

11. https://iiv. uz/news/kiberjinoyatchilikka-qarshi-kiberxavfsizlik

12. https://qalampir.uz/uz/news/iiv-ogo%D2%B3lantiradi-internetda-14.firibgarlikning-noodatiyturi-kengayyapti-11673

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