KIBERJINOYATLAR: TUSHUNCHASI, ASOSIY XUSUSIYATLARI, OMILLARI, QARSHI KURASH VA OLDINI OLISHNING MUHIM CHORALARI

Muzaffar Ziyodullayevich ZIYODULLAYEV
professor
yuridik fanlar doktori (DSc)
Toshkent xalqaro universiteti
Toshkent, O‘zbekiston
e-mail: muzzziyo@gmail.com

Annotatsiya

Maqolada zamonaviy raqamli transformatsiya sharoitida “kiberjinoyatlar” fenomenining huquqiy tabiati, o‘ziga xos xususiyatlari tizimli tahlil etilgan. Tadqiqot davomida kibermakondagi jinoyatlarni yuzaga keltiruvchi psixologik, viktimologik, texnologik, iqtisodiy va huquqiy omillar tasniflanib, sohani huquqiy tartibga solish hamda preventiv mexanizmlarni takomillashtirishga doir konseptual takliflar ilgari surilgan.

Tayanch so‘zlar: kiberjinoyat, kiberxavfsizlik, kiberfiribgarlik, kiberqurbon, kibermakon, kibersavodxonlik, transchegaraviylik, anonimlik, sun’iy intellekt, kiberjinoyatlarga qarshi kurash, kiberjinoyatlarning oldini olish.

КИБЕРПРЕСТУПЛЕНИЯ: ПОНЯТИЕ, ОСНОВНЫЕ ХАРАКТЕРИСТИКИ, ФАКТОРЫ, ВАЖНЫЕ МЕРЫ БОРЬБЫ И ПРЕДУПРЕЖДЕНИЯ

Музаффар Зиёдуллаевич ЗИЁДУЛЛАЕВ
профессор
доктор юридических наук (DSc)
Ташкентский международный университет
Тошкент, Узбекистан
e-mail: muzzziyo@gmail.com

Аннотация

В статье проводится системный анализ правовой природы феномена «киберпреступлений» и его специфических особенностей в условиях современной цифровой трансформации. В ходе исследования классифицируются психологические, виктимологические, технологические, экономические и правовые факторы, способствующие возникновению преступлений в киберпространстве, а также выдвигаются концептуальные предложения по совершенствованию правового регулирования данной сферы и превентивных механизмов.

Ключевые слова: киберпреступление, кибербезопасность, кибермошенничество, кибержертва, киберпространство, киберграмотность, трансграничность, анонимность, искусственный интеллект, борьба с киберпреступлениями, предупреждения киберпреступлений.

Bugungi kunda jamiyat taraqqiyotining yangi bosqichi – axborotlashgan va kiberrivojlangan davrga o’tishi insoniyat hayotining barcha sohalariga raqamli texnologiyalarning kirib kelishiga sabab bo’ldi. Biroq, bu jarayon nafaqat qulayliklar, balki kiberjinoyatlar ko’rinishidagi jiddiy xavf-xatarlarni ham keltirib chiqarmoqda. Kiberjinoyatlarga qarshi kurashish muammosi nafaqat har bir mamlakatda milliy darajada, qolaversa global miqyosda yetakchi o’rinlarga chiqmoqda. S.A. Styajkina to‘g‘ri ta’kidlaganidek, ushbu muammoning o’ziga xosligi uning ko’p qirraliligi va turli omillar bilan bog‘liqliligidadir. Unga qarshi samarali kurash olib borish uchun esa huquqiy, texnik, psixologik va ijtimoiy soha vakillarining say-harakatlarini birlashtirish talab etiladi. Binobarin, statistik ma’lumotlarga ko’ra, bugungi kunda kiberjinoyatlar umumiy jinoyatchilik tarkibida sezilarli ulushni egallamoqda. Masalan, Rossiyada kiberjinoyatlar barcha jinoyatlarning to’rtdan bir qismidan ko’prog’ini (26,6%) tashkil etadi [1]. H.A. Akkaevaning kriminologik tahlillariga ko’ra, kiberjinoyatchilik 1970-yillardagi oddiy “frisking” (telekommunikatsiya tizimlariga ruxsatsiz kirish)dan bugungi kunda milliardlab dollar zarar keltiruvchi yuqori daromadli “yashirin iqtisodiyot” sohasiga aylandi. Kiberxavfsizlik sohasidagi dunyodagi yetakchi tadqiqot kompaniyalaridan biri “Cybersecurity Ventures” prognozlariga ko’ra, 2025-yilga kelib kiberjinoyatchilikdan ko’riladigan yillik zarar dunyo miqyosida 10,5 trillion AQSh dollariga yetadi [2].

O‘zbekistonda ham kiberjinoyatlar kundan-kunga ko‘payib, uning turlari 18 tadan 62 taga chiqdi. Ayniqsa, shaxsiy ma’lumotlarni o‘g‘irlash, sun’iy intellekt orqali ovoz va yuz qiyofasini o‘xshatish, zararli fayllarni tarqatish avj olyapti. O‘zlashtirilgan mablag‘lar kriptovalyuta shaklida chetga chiqarilmoqda. Sintetik narkotiklarning 95 foizi internet orqali tarqatilib, to‘lov kriptovalyutada bo‘layotgani ayniqsa achinarlidir [3].

Xo‘sh, “kiberjinoyatlar” o‘zi nima, uning asosiy xususiyatlari nimada namoyon bo‘ladi? Qanday omillar kiberjinoyatlarni keltirib chiqarmoqda va oziqlantirmoqda? Kiberjinoyatlarga qarshi kurash va ularning oldini olish uchun qanday chora-tadbirlarni amalga oshirish lozim?

Yevropa Kengashining 2001-yil 23-noyabrdagi “Kiberjinoyatchilik to‘g‘risida”gi 185-son Budapesht Konvensiyasiga ko‘ra, tor ma’noda “*kiberjinoyatchilik* – kompyuter tizimlari va ma’lumotlari xavfsizligiga qarshi elektron operatsiyalar orqali sodir etiladigan g‘ayrihuquqiy qilmishlar” bo‘lsa, keng ma’noda “kompyuter tizimlari yoki tarmoqlaridan foydalangan holda yoki ular bilan bog‘liq holda sodir etiladigan har qanday noqonuniy qilmish, shu jumladan noqonuniy axborotga egalik qilish va tarqatish”ni o‘z ichiga oladi.

BMT ekspertlari tavsiyalariga ko‘ra, kiberjinoyatchilik atamasi kompyuter tizimi yoki tarmog‘i yordamida, uning doirasida yoki unga qarshi sodir etilishi mumkin bo‘lgan har qanday jinoyatni qamrab oladi. Huquqshunos T.L. Tropinaning fikricha, keltirilgan ta’rif “kompyuter jinoyatchiligi” tushunchasiga yaqin bo‘lib, ushbu tushuncha hisoblash texnikasi yordamida sodir etiladigan barcha qilmishlarni to‘liq qamrab ololmaydi. U kiberjinoyatchilikni kiberfazoda kompyuter tizimlari yoki tarmoqlari yordamida, shuningdek, ularga qarshi qaratilgan jinoyatlar majmui sifatida ta’riflaydi [4].

Shu sababli, axborot huquqiga oid adabiyotlarda *“Kiberjinoyatchilik* – bu shunchaki texnikadan foydalanish emas, balki virtual makonda axborot texnologiyalaridan foydalangan holda axborot xavfsizligiga, shaxs, jamiyat va davlat manfaatlariga tahdid soluvchi ijtimoiy xavfli qilmishlar yig‘indisi” degan ta’rif keltiriladi [5].

“Kiberjinoyatchilik” “kiberjinoyatlar”ga nisbatan keng va umumiy tushuncha bo‘lib, u kiberjinoyatlarning shunchaki mexanik yig‘indisi emas, balki ularning sifat va miqdor ko‘rsatkichlarini belgilab beruvchi murakkab tizimdir.

Yuqorida keltirilgan va yuridik adabiyotlardagi boshqa ta’riflar tahliliga asoslanib, bizningcha “kiberjinoyatlar” tushunchasiga shunday ta’rif berish mumkin: “*kiberjinoyatlar* – axborot texnologiyalari va raqamli tizimlardan jinoyat sodir etish quroli sifatida foydalangan holda, kompyuter ma’lumotlarining maxfiyligi, yaxlitligi va foydalanish imkoniyati hamda shaxs, jamiyat va davlatning axborot xavfsizligiga qarshi yo‘naltirilgan, jinoyat qonunchiligi bilan taqiqlangan ijtimoiy xavfli qilmishlar yig‘indisi”.

Kiberjinoyatlarning eng keng tarqalgan turi bu – kiberfiribgarlik. Fishing (phishing) esa eng xavfli firibgarlik shakli bo‘lib, u foydalanuvchilarning shaxsiy ma’lumotlarini (login, parol, bank kartasi raqamlari) aldov yo’li bilan qo’lga kiritishga qaratilgan harakat. Uning: klassik fishing – elektron pochta orqali ommaviy xabarlar yuborish; maqsadli (Spear) fishing – aniq bir shaxs yoki tashkilot haqida ma’lumot to’plab, unga yo’naltirilgan hujum; smishing va vishing – SMS yoki telefon qo’ng’iroqlari orqali amalga oshiriladigan aldov kabi turlari ajratib ko‘rsatiladi. Bir qator rus huquqshunos olimlari bunday kiberjinoyatlarni Rossiya va Xitoy tajribasi misolida o‘rganib, kelgan xulosalariga ko’ra, ko’p hollarda jinoyat kodekslaridagi normalar firibgarlik va o’g’rilik o’rtasidagi farqni aniq belgilab bermaydi, bu esa bu borada huquqni qo’llash amaliyotida qiyinchiliklar tug’diradi [6].

Kiberjinoyatlarning nisbatan yangi ko‘rinishlaridan yana biri – *kiberbulling* bo‘lib, u qurbonga nisbatan internet-platformalar (ijtimoiy tarmoqlar, o‘yinlar, chatlar) yordamida tizimli ravishda amalga oshiriladigan qasddan qilingan agressiv xulq-atvor harakati. Kiberbulling shakllariga: psixologik terror, shantaj, hayosiz hazillar, tuhmat, boyqot, shilqimlik kabilar kiradi hamda bunday ta’sir shaxs o‘z joniga qasd qilishgacha bo‘lgan oqibatlarga olib kelishi mumkin.

Umuman olganda, kiberjinoyatlarning bir qator turlari mavjud bo‘lib, bu borada olimlarning qarashlari ham turlicha. Fikrimizcha, bu borada Al-Quds universiteti olimlari M. Axmead, N. Al-Sharif va I. Abuiramning kiberjinoyatlarning tasnifiga doir fikrlari nisbatan kengroq. Ular kiberjinoyatlarni: shaxsga qarshi jinoyatlar – kiberbulling, kiberquvg‘in (cyberstalking), pornografiya tarqatish, seksting va sekstorsiya (shahvoniy kontent orqali shantaj); mulkka qarshi jinoyatlar – kiberfiribgarlik, kredit kartalari bilan bog‘liq jinoyatlar, intellektual mulk o‘g‘riligi; davlatga qarshi jinoyatlar – kiberterrorizm va davlat axborot tizimlariga hujum kabilarga ajratadilar [7].

Kiberjinoyatlarning o‘ziga xos xususiyatlari haqida so‘z borganda, bu borada olib borilgan tadqiqotlarda uni an’anaviy jinoyatlardan ajratib turuvchi quyidagi asosiy xususiyatlari ko‘rsatiladi:

1) transchegaraviylik (chegaralarning yo‘qligi) – bu kiberjinoyatlarning eng muhim xususiyati bo‘lib, jinoyatchi bir qit’ada bo‘lishi, jinoiy harakat boshqasida amalga oshirilishi, oqibatlari esa uchinchi davlatda namoyon bo‘lishi mumkin. Global tarmoq tufayli jinoyatchi va jabrlanuvchi o‘rtasidagi masofa ahamiyatga ega emas;

2) yuqori darajadagi latentlik (yashirinlik) – turli sabablar bilan kiberjinoyatlarning aksariyati qayd etilmay qoladi. Tahlillar shuni ko‘rsatadiki, Rossiyada kibermakondagi latent jinoyatlar darajasi 85–97% ga yetadi. Buning sababi jabrlanuvchilarning huquqni muhofaza qilish organlariga murojaat qilmasligi yoki jinoyatni sezmay qolishidir [8];

3) anonimlik va masofaviylik – jinoyatchilar o‘z shaxsini yashirish va jismoniy aloqaga kirishmasdan turib jinoyat sodir etish imkoniyatiga ega. Kiberjinoyatlarga xos global tarmoqning anonimlik xususiyati va davlat institutlari nazoratidan tashqaridagi asosiy kriminogen omildir. Kibermakonda an’anaviy ijtimoiy institutlar o’z funksiyalarini to’liq bajara olmaydi, natijada foydalanuvchilar normativ nazoratdan chiqib ketadi;

4) intellektual tabiat va professionalizm – kiberjinoyatchilar ko‘pincha yuqori ma’lumotli, IT sohasida chuqur bilimga ega shaxslar bo‘lib, doimiy ravishda o‘z malakasini oshirib boradilar. Ular an’anaviy jinoiy guruhlarga o‘z xizmatlarini taklif qilib, uyushgan jinoyatchilikning bir qismiga aylanmoqdalar. Shuni alohida ta’kidlash kerakki, kiberjinoyatchilarda o‘ziga xos submadaniyat shakllangan, faqat ular tor doirada tushunadigan o‘z jargoni — «sleng»i paydo bo‘lgan;

5) dinamik o‘zgaruvchanlik, avtomatlashtirish va kuchlarni birlashtirish – jinoyat usullari doimiy ravishda yangilanib, texnologiyalar rivojiga moslashib bormoqda, jinoyatchilar jarayonni avtomatlashtirishi va bir vaqtning o‘zida ko‘plab hujumlarni amalga oshirish imkoniga ega bo‘lmoqdalar.

Ayniqsa, zamonaviy axborot texnologiyalarining sun’iy intellekt bilan uyg‘unlashuvi natijasida kiberjinoyatchilikning xavfi yanada ortmoqda. London fond birjasi guruhi (LSEG) katta maslahatchisi Rut Vandhyofer avtonom sun’iy intellekt tahdidlarining yangi davri haqida so‘z yuritib, so‘nggi vaqtlarda xakerlar

biznesga qaraganda sun’iy intellektni tezroq o‘zlashtirganini, “ransomware” hujumlari (ya’ni, foydalanuvchining ma’lumotlari yoki butun kompyuter tizimini blokga tushirib qo‘yib, uni qayta tiklash evaziga to‘lov talab qilish) holatlari 60% ga oshganini, jabrlanganlar orasida yirik brendlar, banklar va hatto yirik mudofaa tashkilotlari ham borligini, hujumchilar fishingni avtomatlashtirish va chuqur qalbakilashtirishlar uchun sun’iy intellektdan ommaviy ravishda foydalanishni boshlaganligini ta’kidlaydi. Unung fikricha bunda: inson aralashuvisiz murakkab operatsiyalarini mustaqil ravishda bajarishga qodir tizimlarning paydo bo‘lishi; an’anaviy shaxsni tasdiqlash usullarining ishonchsiz bo‘lib borayotganligi; xodimlar bilmasdan maxfiy korporativ ma’lumotlarni ommaga ochiq algoritmlarga uzatayotganligi; Onchain kiberjinoyatlari, ya’ni jinoyatchilar tobora ko‘proq DeFi platformalari (banklar yoki davlat ishtirokisiz, markaziy boshqaruvsiz amalga oshiriluvchi bank va moliyaviy xizmatlari tizimi)ga hujum qilish, javobgarlikdan qochish uchun infratuzilmalarini blokcheynga ko‘chirish holatlari ko‘payib borayotganligi; klassik shifrlashni buzib kirish imkoniyatiga ega bo‘lgan kvant kompyuterlarini yaratishga bo‘lgan intilishlar bu boradagi xavotirlarni kuchaytiradi [9].

Kiberjinoyatlarning sabablari va omillarini o‘rganish zamonaviy kriminologiya va axborot xavfsizligining eng dolzarb masalalaridan biridir. Ilmiy tadqiqotlar shuni ko‘rsatadiki, bu jinoyatlar shunchaki texnik yoki texnologik xatolik emas, balki murakkab tizimli muammolar mahsulidir.

Kiberjinoyatlarni keltirib chiqaruvchi omillarni quyidagicha tasniflab o‘rganish mumkin:

Psixologik omillar. Tadqiqotlar shuni ko‘rsatadiki, kibermakonda jinoyatchi va jabrlanuvchi o‘rtasida bevosita muloqot yo‘qligi sababli, jinoyat sodir etish psixologik jihatdan oson kechadi. Virtual buyumlar va harakatlar “haqiqiy emas”dek tuyuladi. Bu esa odamlarda, ayniqsa yoshlarda, axborot xavfsizligi talablari va mualliflik huquqlarini buzish kabi holatlarga nisbatan mas’uliyatsizlikni keltirib chiqaradi. Jinoyatchi o‘z harakatining yetkazayotgan

zararini o‘z ko‘zi bilan ko‘rmagani sababli, unda aybdorlik hissi va javobgarlik tuyg‘usi sust bo‘ladi.

AQSH Internetdan xavfsiz va mas’uliyatli foydalanish markazi direktori, kiberxavfsizlik sohasidagi taniqli amerikalik ekspert Nensi Villard to‘g‘ri ta’kidlaganidek, “axborot-kommunikatsiya texnologiyalari qayta aloqani, harakatlarimizning har qanday sezilarli qayta aloqa tuyg‘usini sezilarli darajada cheklaydi. Shu bois, bizga zarar yetkazganimizni anglash tuyg‘usi ta’sir qilmaydi, shuningdek, biz o‘z xulq-atvorimiz hech qanday zarar keltira olmaydi deb hisoblaymiz, chunki biz bu zararni ko‘rmaymiz” [10].

Rayder universiteti (AQSH) professori Jon Shuler kibermakonning insonga ko‘rsatadigan ta’sirini, ya’ni insonning real jamiyatdagiga qaraganda erkinroq harakat qilishini ifodalash uchun “onlayn jilovsizlik effekti” tushunchasini ilgari surdi. Uning fikricha, ushbu effektning asosini quyidagilar tashkil etadi: *dissotsiativ anonimlik* (“sen meni tanimaysan”) – anonimlik sharoitida odamlar kibermakondagi o‘z harakatlarini real dunyo va real shaxsiyatdan ajratib qo‘yib, bunday holatda inson o‘z harakatlari uchun javobgarlikni o‘z zimmasiga olmasa ham bo‘ladi, deb hisoblaydi; *ko‘rinmaslik* (“sen meni ko‘rmayapsan”) – psixologik aloqa o‘rnatilishidan qochish imkonini beradi; *asinxronlik* (“keyinroq ko‘rishamiz”) – alohida holatlarda suhbatdoshning so‘zlari yoki harakatlariga zudlik bilan munosabat bildirish zaruriyatisiz muloqot qilish imkoniyati bo‘lib, bu muhim dezingibitsiyalovchi (jilovni bo‘shatuvchi) omil hisoblanadi; *soliptik introyeksiya* (“bularning hammasi mening xayolimda”) – onlayn muloqot paytida hamma voqealar faqat bizning shaxsiy tasavvurimizda sodir bo‘layotgandek tuyg‘u paydo bo‘lishi ehtimoli; *hokimiyatning minimallashuvi* (“biz tengmiz”) – yuqori ijtimoiy mavqe belgilarining bilvosita qabul qilinishi, shuningdek, ularni e’tiborsiz qoldirish imkoniyati tufayli yuzaga keladi [11].

Viktimologik omillar. Zamonaviy empirik tahlillarga ko‘ra, kiberinsidentlarning salmoqli qismida inson omili ishtirok etadi. Xususan, Verizon kompaniyasining 2025-yildagi ma’lumotlar buzilishi bo‘yicha tahliliy hisoboti (Data Breach Investigations Report) xulosasida buzilishlarning taxminan 60 foizi

inson omili (masalan, kiberfiribgarlik, o‘g‘irlangan autentifikatsiya ma’lumotlari yoki noto‘g‘ri harakatlar) bilan bog‘liq ekani qayd etiladi. Kiberxavfsizlik va axborot xavfsizligi boshqaruvi sohasida tadqiqot olib borgan yevropalik olimlar M. Evans, L. A. Maglaras**,** Y. Xe va H. Yanike davlat sektorida axborot xavfsizligi masalalari xususidagi tadqiqotlarida davlat tashkilotlarida qayd etilgan axborot xavfsizligi hodisalarining har uchdan ikkidan (2/3) ortiq qismi inson xatosi bilan bog‘liq omillar natijasida yuzaga kelgani, inson omili hal qiluvchi rol o‘ynaganini ta’kidlaydilar [12]. Buning asosiy sababi foydalanuvchilarning internetdagi xavf-xatarlarni yetarlicha baholamasligi, jinoyatchilar esa ularning ishonuvchanligi va raqamli gigiyena qoidalarini bilmasligidan unumli foydalanishida namoyon bo‘ladi.

Aholi o‘rtasida kibersavodxonlik darajasining pastligi, xususan, foydalanuvchilarning shaxsiy kiberxavfsizlikka nisbatan beparvo yondashuvi zamonaviy kibertahdidlarning keng ildiz otishiga xizmat qilmoqda. Tadqiqotlar shuni ko‘rsatadiki, ko‘plab foydalanuvchilar murakkab parollar yaratish yoki ikki bosqichli autentifikatsiya tizimidan foydalanish bo‘yicha nazariy bilimga ega bo‘lsa-da, amaliyotda ushbu xavfsizlik protokollariga rioya qilmaydilar. Bu esa kiberjinoyatlar sodir etilishi uchun sharoit yaratadi. Xalqaro kompyuter va axborot savodxonligi tadqiqoti (ICILS) ma’lumotlariga ko‘ra, raqamli ko‘nikmalarning bazaviy darajasiga ega bo‘lmagan o‘quvchilar ko‘rsatkichi AQShda 51 foizni, Yevropa Ittifoqi mamlakatlarida esa 43 foizni tashkil etadi. Ushbu yo‘nalishda nisbatan ijobiy natija Janubiy Koreyada kuzatilib, u yerda o‘quvchilarning faqat 27 foizi yetarli ko‘nikmaga ega emasligi qayd etilgan. Tabiiyki, mamlakatimizda ushbu ko‘rsatkich yuqoridagi davlatlarga qaraganda ancha past.

Aytish joizki, hozirda ilm-fanda kiberviktimologiya kriminologiyaning yangi yo’nalishi sifatida shakllanib ulgurdi. Huquqshunos D.V. Jmurov kiberqurbonni “raqamli muhitda sodir etilgan jinoiy harakatlar natijasida zarar ko’rgan shaxs, guruh yoki tashkilot” deb ta’riflaydi [13]. S.A. Styajkina kiberfiribgarlik qurbonlarini ikki asosiy tipga ajratadi: *texnik ta’sir qurbonlari* – bu guruhga yangi texnologiyalardan faol foydalanuvchi, bilimli, ammo kompyuter xavfsizligi

masalalariga yuzaki qaraydigan yoshlar kirib, ularning o'z bilimiga haddan tashqari ishonishi va ehtiyotkorlikni yo'qotishi kiberhujumga sabab bo'ladi; *axborot ta'siri qurbonlari* – bunga haddan tashqari ishonuvchan, psixologik ta'sirga tez beriluvchi va ko'pincha kam xarajat bilan katta foyda olishga intiluvchi shaxslar kirib, ular firibgarlarga o'z xohishlari bilan pul o'tkazib beradilar yoki maxfiy ma'lumotlarini taqdim etadilar [1].

Texnologik va innovatsion omillar. Zamonaviy kompyuter texnologiyalari hamda sun'iy intellektning jadal taraqqiyoti kiberhujum vositalarining himoya tizimlariga qaraganda tezroq takomillashishiga xizmat qilmoqda. Tarmoqdagi anonimlik va global qamrov, xususan, IP-manzillarni niqoblash hamda masofaviy mahv etish imkoniyatlari kiberjinoyatchilik uchun keng yo‘l ochmoqda. Kibermakonga xos bo‘lgan qurilma yoki tarmoq foydalanuvchisining to‘liq anonim qolish imkoniyati nafaqat texnologik, balki psixologik kriminogen omil hisoblanadi. Anonimlik nafaqat shaxsni aniqlashga yo‘l qo‘ymaydi, balki o‘zi haqida yolg‘on ma'lumot berish, boshqa shaxs qiyofasida ijtimoiy muloqotga kirishish imkonini ham beradi. Anonimlik sharoitida har qanday inson salbiy harakatlarni jazosiz sodir etish mumkinligini his qiladi. Anonimlik kibermakonni kundalik hayotga nisbatan «parallel» olamga aylantiradi va o‘z shaxsining real hayotdagi qiyofasidan farq qiluvchi yangi obrazini yaratishga imkon beradi.

Bugungi kunda jinoiy guruhlar zararli kodlarni yaratish va fishing hujumlarini avtomatlashtirishda sun'iy intellekt imkoniyatlaridan samarali foydalanayotgani axborot xavfsizligiga nisbatan tahdidlarning sifat jihatidan yangi bosqichga chiqishiga sabab bo‘lmoqda. M. Brandij, SH. Avin, J. Klark, H. Toner, P. Ekersli kabi sun'iy intellekt va kiberxavfsizlik sohasidagi amerikalik yetakchi ekspert va olimlar tomonidan “Sun'iy intellektdan g‘arazli maqsadlarda foydalanish: prognoz qilish, oldini olish va oqibatlarini yumshatish” mavzusida o‘tkazilgan tadqiqotda keltirilganidek, sun'iy intellekt ishtirokidagi kibertahdidlarning o‘ziga xos xususiyatlari: *birinchidan*, hujumlarning samaradorligi, ya'ni avtomatlashtirish hisobiga kamroq resurs sarflab, ko‘proq zarar yetkazish imkonini berishida; *ikkinchidan*, dezinformatsiya va dipfeyk (inson qiyofasi yoki ovozini sun'iy

intellekt yordamida almashtirish yoki soxtalashtirish) texnologiyasiga egaligi, xususan sun’iy intellekt videolarni haqiqatdan ajratib bo‘lmaydigan darajada o‘zgartirish orqali jamoat fikrini chalg‘itish va insonlarni aldash uchun xizmat qilishi mumkinligi; *uchinchidan*, nazorat qilishning qiyinligi bilan ajralib turadi [14].

Iqtisodiy omillar. Zamonaviy ilmiy maqolalarda kiberjinoyatchilik yuqori rentabelli iqtisodiy soha sifatida tavsiflanadi. Kiberhujum uyushtirish uchun kam mablag‘ talab etiladi, ammo undan keladigan foyda millionlab dollar bo‘lishi mumkin. Axborot xavfsizligi sohasidagi nufuzli olimlar, “Kiberxavfsizlik iqtisodiyoti” ilmiy yo‘nalishi asoschilari Ross Anderson va Tayler Mur o‘z tadqiqotlarida qayd etishicha, axborot tizimlaridagi xatolik va muammolar texnik kamchiliklardan ko‘ra ko‘proq noto‘g‘ri iqtisodiy rag‘batlar (motivlar) tufayli yuzaga keladi. Zamonaviy kiberjinoyatlar havaskorlikdan ixtisoslashgan mehnat taqsimotiga o‘tganiga ancha bo‘ldi. Xususan, alohida virus yozuvchilar, botnet ijaraga beruvchilar, o‘g‘irlangan ma’lumotlarni sotuvchilar va pul yuvuvchilar kabi “xizmatlar” paydo bo‘lgan. Bu ixtisoslashuv kiberjinoyatchilikning samaradorligini oshirib, uning xarajatlarini kamaytirgan [15].

Qolaversa, Moliyaviy amaliyotlar, ya’ni tranzaksiyalarning anonimligi jinoiy faoliyatdan olingan daromadlarni legallashtirish hamda tovlamachilik vositasida mablag‘larni o‘zlashtirish uchun qulay muhit yaratadi.

Jahon iqtisodiyotida kriptovalyutalarning ommalashuvi, ularning davlat chegaralarini tan olmasligi, jinoiy yo‘l bilan egallangan millionlab dollarni bir necha soniya ichida dunyoning narigi chekkasiga o‘tkazish imkoniyatining mavjudligi kiberjinoyatlarga qarshi kurashda jiddiy muammolarni keltirib chiqarmoqda. Xususan, egallangan mablag‘lar boshqa davlat yurisdiksiyasiga o‘tgan hollarda, shuningdek kiberjinoyatlarning eng xavfli ko‘rinishi bo‘lgan “ransomware”da xakerlar jinoiy yo‘l bilan talab qiluvchi to‘lovni Bitcoin kabi kriptovalyutalarda to‘lashni talab qilayotganligi huquq-tartibot organlari tomonidan ularni muzlatish yoki qaytarishni deyarli imkonsiz qilib qo‘ymoqda.

Blokcheyn ma’lumotlarini tahlil qilish bo‘yicha dunyodagi yetakchi platformalardan biri “Chainalysis”ning 2025-yildagi kriptojinoyatchilik bo‘yicha hisoboti tahlilida keltirilganidek, so‘ngi yillarda kriptojinoyatchilik nafaqat hajm jihatidan o‘smoqda, balki professionallashib va diversifikatsiyalanib bormoqda. Xususan, ilgari kriptojinoyatlar asosan kiberhujumlar bilan cheklangan bo‘lsa, endilikda u milliy xavfsizlikka tahdid soluvchi sohalar va uyushgan jinoyatchilikning ajralmas qismiga aylandi, jinoiy guruhlar jinoiy mablag‘larni yuvish uchun blokcheyn texnologiyalaridan yanada mohirlik bilan foydalanmoqda, of-cheyn va on-cheyn faoliyatlarini uyg‘unlashtirmoqda. Raqamlar shuni ko‘rsatadiki, 2024-yilda noqonuniy manzillar tomonidan qabul qilinganligi aniqlangan mablag‘larning umumiy qiymati 50 milliard dollardan oshgan.

Huquqiy omillar. Kiberjinoyatlar sodir etilishining huquqiy omillari: qonunchilikdagi bo‘shliqlar, xalqaro huquqiy normalarning yetishmovchiligi va jinoiy javobgarlikni belgilashdagi murakkabliklarda namoyon bo‘ladi. Kiberjinoyatlarning huquqiy jihatdan eng katta muammosi – yurisdiksiya masalasi bo‘lib, bunda jinoyatchi bir davlatda, server boshqa davlatda, jabrlanuvchi esa uchinchi davlatda bo‘lishi mumkin. Kibermakonda hududiy chegaralarning yo‘qligi milliy huquq tizimlari uchun asosiy to‘siq bo‘lib, ko‘plab davlatlar o‘rtasida kiberjinoyatchilarni ekstraditsiya qilish yoki raqamli dalillarni almashish bo‘yicha ikki tomonlama shartnomalarning mavjud emasligi bu borada muayyan muammolarni keltirib chiqaradi.

Kiberxavfsizlik sohasidagi xalqaro ekspert Shtayn Shyolberg to‘g‘ri ta’kidlaganidek, kibermakon quruqlik, dengiz, havo va koinotdan keyingi beshinchi umumiy makon sifatida xalqaro darajada muvofiqlashtirishni, hamkorlikni va alohida huquqiy choralarni talab etadi [16].

Kiberjinoyatlar sodir etilishining huquqiy omillaridan yana biri – ularga qarshi kurashning xalqaro hujjatlar bilan yetarlicha tartibga solinmaganligidadir. Budapesht konvensiyasi (2001) ushbu sohadagi birinchi va eng muhim xalqaro hujjat bo‘lsa-da, barcha davlatlar, xususan Rossiya va Xitoy uni imzolamagan, bu

esa global hamkorlikni susaytiradi. Kiberjinoyatchilikka qarshi kurashda yagona global tizimning yo‘qligi jinoyatchilar uchun “huquqiy boshpanalar” yaratadi.

Bu boradigi huquqiy omillardan yana biri – raqamli dalillarni to‘plash va ularni sudda tan olinishi tartibining murakkabligi bilan bog‘liq bo‘lib, bu huquqni muhofaza qiluvchi organlardan yuqori texnik malaka talab qiladi.

Yuqoridagi fikrlar, xususan kiberjinoyatlarga xos xususiyatlar, ularning keltirib chiqaruvchi va oziqlantiruvchi omillar hamda shu orqali namoyon bo‘ladigan kiberjinoyatchilikning ijtimoiy xavfi unga qarshi tizimli, izchil va kompleks chora-tadbirlarni amalga oshirishni taqozo etadi. *Fikrimizcha, ushbu jarayonda quyidagilarga alohida e’tibor qaratish maqsadga muvofiqdir:*

1. Axborot xavfsizligini ta’minlashda intellektual himoya tizimlariga o‘tish. Kiberhujumlarni amalga oshirish va avtomatlashtirish sun’iy intellektdan foydalanilayotgan bir paytda, an’anaviy (statik) himoya vositalari o‘z samaradorligini yo‘qotmoqda. Shu sababli, kiberhujumlarni real vaqt rejimida prognoz qiluvchi va ularga moslashuvchan “Intellektual monitoring” (AI-driven security) tizimlarini joriy etish zarur.

“Katta yettilik” (G7) davlatlari tashabbusi bilan 1989-yilda Parij shahrida o‘tkazilgan sammitda tashkil etilgan Pul yuvishga qarshi kurashish bo‘yicha moliyaviy chora-tadbirlar guruhi (FATF) tadqiqoti xulosasiga ko‘ra kiberjinoyatchilikka qarshi kurashda faqatgina blokcheynni kuzatish yetarli emas, balki bunda eng samarali usul – texnik ma’lumotlarni (IP, hamyon izlari) va ijtimoiy xulq-atvorni (“O‘z mijozingni bil” tamoyili (KYC), iqtisodiy mantiq) birlashtirgan holda kompleks monitoring o‘rnatishdan iboratdir.

2. Kibermakondagi jinoyatchilikning transchegaraviy va anonim xususiyatini inobatga olgan holda, jamiyatda “raqamli viktimizatsiya” (kiberjinoyat qurboniga aylanish) xavfini kamaytirish maqsadida huquqni muhofaza qiluvchi organlar va fuqarolik jamiyati institutlarining ijtimoiy sherikligiga asoslangan ixtisoslashgan «Kiberviktimologiya markazi» jamoatchilik tuzilmasini tashkil etish maqsadga muvofiq. Mazkur markazning faoliyat yo‘nalishlari sifatida quyidagilarni belgilash tavsiya etiladi: *viktimologik profilaktika* – aholining zaif qatlamlari (yoshlar,

keksalar, raqamli ko‘nikmasi past shaxslar) o‘rtasida maqsadli targ‘ibot ishlarini olib borish orqali kiberprevensiya tizimini shakllantirish; *reabilitatsiya va psixologik ko‘mak* – kiberjinoyat oqibatida moliyaviy va ma’naviy zarar ko‘rgan shaxslarga ixtisoslashgan psixologik hamda yuridik konsultativ yordam ko‘rsatish tizimini yo‘lga qo‘yish; *kiberfiribgarlikka qarshi immunitetni oshirish* – foydalanuvchilarda firibgarlikning psixologik manipulyatsiya usullariga nisbatan kriminologik barqarorlikni shakllantirish.

Ushbu tuzilmaning barqaror faoliyat yuritishini ta’minlash maqsadida davlat tomonidan ijtimoiy buyurtmalar ajratish, soliq imtiyozlarini qo‘llash hamda huquqni muhofaza qilish organlarining tezkor ma’lumotlar bazasi bilan (shaxsiy daxlsizlikni saqlagan holda) integratsiya qilish bo‘yicha zarur huquqiy mexanizmlarni ishlab chiqish lozim.

3. Kiberjinoyatlarga qarshi kurash sohasida qonunchilik va xalqaro hamkorlikni takomillashtirish. Milliy jinoyat qonunchiligini raqamli transformatsiya sharoitiga moslashtirish maqsadida Jinoyat kodeksiga “kiberjinoyat” va “virtual mulk” tushunchalarini definitsiya sifatida kiritish dolzarb ahamiyat kasb etadi. Xususan, sun’iy intellekt tizimlaridan foydalanib sodir etilgan jinoiy qilmishlarni javobgarlikni og‘irlashtiruvchi holat sifatida e’tirof etish, shu bilan birga sun’iy intellektning algoritmik xatoliklari va foydalanuvchining jinoiy qasdi o‘rtasidagi huquqiy chegarani belgilash bo‘yicha “texnologik ekspertiza” institutini joriy etish lozim. Shuningdek, O‘zbekiston Respublikasi Oliy sudi Plenumining kiberjinoyatlarni kvalifikatsiya qilishga doir tushuntirishlarida texnologik usul bilan o‘zganing mulkini egallashni – o‘g‘rilik, ijtimoiy muhandislik orqali irodani manipulyatsiya qilishni esa – firibgarlik sifatida ajratuvchi yagona huquqni qo‘llash amaliyotini shakllantirish zarur.

Shuningdek, O‘zbekiston Respublikasining 2001-yildagi “Kiberjinoyatchilik to‘g‘risida”gi Budapesht konvensiyasiga a’zo bo‘lishi imkoniyatlarini har tomonlama ko‘rib chiqish va ushbu jarayonni jadallashtirish maqsadga muvofiqdir. Binobarin, Budapesht konvensiyasini ratifikasiya qilish mamlakatimizning milliy jinoyat va jinoyat-prosessual qonunchiligini sohaga doir xalqaro standartlarga

muvofiqlashtirish hamda raqamli dalillarni to‘plashda global hamkorlik mexanizmlarini yo‘lga qo‘yish, shuningdek kiberjinoyatlarning transchegaraviy xarakterini inobatga olgan holda, mazkur turdagi jinoyatlarni tergov qilishda xorijiy davlatlar bilan tezkor axborot almashinuvini ta’minlovchi “24/7 aloqa tarmog‘i”ga qo‘shilish imkonini beradi.

4. Aholining kibersavodxonligini oshirish, raqamli gigiyenani kuchaytirish, kiberjinoyatchilikka qarshi tizimli va izchil targ‘ibotni olib borish. Jamiyatda barqaror “raqamli gigiyena” ko‘nikmalarini shakllantirish va kiberjinoyatlarga qarshi tizimli preventiv choralarni amalga oshirish maqsadida quyidagi majmuaviy ta’lim strategiyasini joriy etish lozim: a) *uzluksiz ta’lim tizimiga integratsiya* – umumiy o‘rta ta’lim maktablari, akademik litseylar, professional ta’lim muassasalari va oliy ta’lim muassasalarining o‘quv dasturlariga “Kiberxavfsizlik asoslari” fanini (yoki tegishli o‘quv modulini) majburiy tartibda kiritish, bunda asosiy urg‘u nafaqat texnik bilimlarga, balki “raqamli xulq-atvor madaniyati” va xavflarni identifikatsiya qilish ko‘nikmalariga qaratilishi zarur;
b) *segmentatsiyalangan yondashuv* – aholining ijtimoiy va yosh xususiyatlaridan kelib chiqib, maxsus adaptiv dasturlarni ishlab chiqish, xususan o‘smirlar uchun: kiberbulling, ijtimoiy tarmoqlardagi manipulyatsiyalar va o‘yin platformalaridagi firibgarliklarga qarshi geymifikatsiya usulidagi ta’lim kontentini yaratish, keksa avlod vakillari uchun: raqamli moliyaviy xizmatlardan xavfsiz foydalanish, kiberfiribgarlikdan himoyalanish bo‘yicha soddalashtirilgan, vizuallashtirilgan andragogik qo‘llanmalar tayyorlash.

Kiberjinoyatchilikka qarshi targ‘ibotni aynan ommaviy axborot vositalari va internetning o’zi orqali, ijtimoiy foydali kontentlarni ko’paytirish yo’li bilan amalga oshirish samaraliroqdir.

Aholida, ayniqsa yoshlarda “onlayn jilovsizlik” psixologiyasini kamaytirish, ularda raqamli etika va mas’uliyatni kuchaytirish uchun virtual olamda sodir etilgan harakatlar uchun real jazo muqarrarligini ko‘rsatuvchi ijtimoiy reklamalarni yaratish va keng yoritish, shuningdek ijtimoiy tarmoqlar va sharh qoldirish platformalarida “anonimlik” va “so‘z erkinligi” o‘rtasidagi muvozanatni

ta’minlovchi, ammo jinoyat sodir etilganda shaxsni tezkor aniqlash imkonini beruvchi (masalan, OneID bilan bog‘lash) tizimlarni rivojlantirish maqsadga muvofiqdir.

Xulosa o‘rnida ta’kidlash joizki, kiberjinoyatlar faqat texnik yoki texnologik muammolar mahsuli emas, balki chuqur ildizlarga ega bo‘lgan kompleks ijtimoiy-huquqiy fenomendir. Ushbu tadqiqot doirasida ilgari surilgan konseptual takliflarning amaliyotga tatbiq etilishi davlatning kiberxavfsizlik strategiyasini “himoyalanish” bosqichidan tizimli «proaktiv profilaktika» bosqichiga transformatsiya qilish imkonini beradi. Bunda asosiy e’tibor nafaqat infratuzilmaviy barqarorlikni ta’minlashga, balki inson omili bilan bog‘liq xavflarni minimallashtirish, aholining raqamli madaniyatini yuksaltirish va jinoyat qonunchiligini texnologik progress sur’atlariga moslashtirishga qaratilishi lozim. Shu tariqa, kibermakonda huquqbuzarliklar sodir etilishiga imkon beruvchi shart-sharoitlarni oldindan prognoz qilish va jinoiy deviantlikning yangi shakllariga nisbatan jamiyatda barqaror “raqamli immunitet” shakllantiriladi.

FOYDALANILGAN ADABIYOTLAR:

1. Стяжкина С.А. Виктимологическая профилактика кибермошенничества // Вестник Удмуртского университета. Экономика и право. – 2022. – № 3. – С. 546-552.

2. Аккаева Х.А. Киберпреступления: криминологический анализ // Право и управление. – 2025. – № 1. – С. 317-322.

3. Huquq-tartibot idoralarining faoliyati tanqidiy ko‘rib chiqilib, jamoat xavfsizligini ta’minlash sohasida yangi vazifalar belgilab berildi// [Elektron manba] URL: https://president.uz/oz/lists/view/8882 (murojaat vaqti: 16.02.2026).

4. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: диссертации кандидат юридических наук. – Владивосток, – 2005.

5. Рассолов И.М. Информационное право. – Москва: Юрайт, 2011.

6. Сергеева А.А., Гурев М.С., Кириллова Я.М. и др. Некоторые особенности противодействия мошенничеству, совершаемому с использованием электронных средств платежа, по законодательству России и Китая / Вопросы безопасности. – 2024. – № 1. – С.10.

7. Ahmead M., El Sharif N., Abuiram I. Risky online behaviors and cybercrime awareness among undergraduate students at Al-Quds University: a cross-sectional study // Crime Science. – 2024. – №13. – Article 29.

8. Маслиенко М.А. Киберпреступность на современном этапе // Проблемы правоохранительной деятельности. – 2021. – №2. – С. 30.

9. Wandhöfer R. Top cyber threats and prevention trends in 2026 // [Elektron manba] URL: https://www.finextra.com/the-long-read/1507/top-cyber-threats-and-prevention-trends-in-2026 (murojaat vaqti: 19.02.2026).

10. Transcript of the National Summit on Cyberethics // [Elektron manba] – URL: http://connect.marymount.edu/ethics/cyberethics/sessions/gensession3.PDF. – pp.23. (murojaat vaqti: 19.02.2026).

11. John Suler. The Psychology of Cyberspace // [Elektron manba] – URL: http://users.rider.edu/~suler/psycyber/psycyber.html (murojaat vaqti: 22.02.2026).

12. Evans M., Maglaras L.A., He Y., Janicke H. Human behaviour as an aspect of cybersecurity assurance // Information & Computer Security. – 2019. – № 1 (27), – pp. 2–23.

13. Жмуров Д.В. Индивидуальная виктимологическая профилактика киберпреступности // Сибирский юридический вестник. – 2023. – № 1. – С. 52-59.

14. Brundage M., Avin S., Clark J., Toner H., Eckersley P., Garfinkel B., Dafoe A., et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. – Oxford: Future of Humanity Institute, 2018. – 101 p.

15. Moore T., Anderson R. Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research. – Cambridge: Harvard University, 2011. – 34 p.

16. Stein Schjolberg. A cyberspace treaty – A United Nations convention or protocol on cybersecurity and cyber crime // [Elektron manba] – URL:

http://cybercrimelaw.net/documents/UN_12th_Crime_ Congress.pdf (murojaat vaqti: 22.02.2026).