УДК. 343.132:343.985:351.74
ORCID: 0009-0005-2988-8626

KIBERJINOYATCHILIKKA KARSHI KURASHISHNING AHAMIYATI

Yakubov Xushnudbek Sheribbayevich
O‘zbekiston Respublikasi IIV
Akademiyasi katta o‘qituvchisi.
xushnud6982@gmail.com.
Qaraxonov Murodbek Shermat o’g’li
O‘zbekiston Respublikasi IIV
Akademiyasi kursanti

ANNOTATSIYA

Mazkur makolada bugungi kunda jamiyatimizda eng xavfli va rivojlangan jinoyatlardan biri bo’lgan rakamli texrologiyalar yordamida sodir etilayotgan kiberjinoyatlar, ularning sodir etilish usul va uslublari haqida va ularning ayrim jihatlari, kiberjinoyat tushunchasiga aksariyat olimlar bergan fikrlar, kiberjinoyatchilikning bugungi kundagi statistikasi haqidagi ma’lumotlar, unga qarshi kurashishning o’ziga xos jihatlari, qarshi kurashishdagi ayrim kamchiliklar va ushbu sohada mamlakatimizda olib borilayotgan islohotlar aks ettirilgan.

Kalit so’zlar: kiberjinoyat, telekommunikatsiyalar tarmog’i, axborot tizimi, axborot, elektron hisoblash mashinalari, komp’yuter tizimi, global tarmoq jinoyatchiligi, kompyuter jinoyatchiligi, kiberterrorizm, kiberekstremizm, kiberxavfsizlik, kibermuxit, global tarmoq jinoyatchiligi.

АННОТАЦИЯ

В данной статье киберпреступления, являющиеся одними из самых опасных и сложных преступлений в нашем обществе сегодня, совершаются с помощью цифровых технологий, о способах и способах их совершения и некоторых их аспектах приводятся мнения большинства ученых. К понятию киберпреступности отражены сведения о статистике киберпреступности на сегодняшний день, конкретных аспектах борьбы с ней, некоторых недостатках в борьбе с ней, а также реформах, проводимых в этой сфере в нашей стране.

Ключевые слова: киберпреступность, телекоммуникационная сеть, информационная система, информация, электронные вычислительные машины, компьютерная система, глобальная сетевая преступность,

компьютерная преступность, кибертерроризм, киберэкстремизм, кибербезопасность, киберсреда, глобальная сетевая преступность.

ANNOTATION

In this article, cybercrimes, which are one of the most dangerous and advanced crimes in our society today, are committed with the help of digital technologies, about the methods and methods of their commission and some of their aspects, the opinions given by most scientists to the concept of cybercrime, information about the statistics of cybercrime today, specific aspects of fighting against it, some shortcomings in fighting against it, and the reforms carried out in this field in our country are reflected.

Key words: cyber crime, telecommunications network, information system, information, electronic computing machines, computer system, global network crime, computer crime, cyber terrorism, cyber extremism, cyber security, cyber environment, global network crime.

Davrimizning fan va texnika sohasidagi yutuqlari kundalik ijtimoiy hayotimizga yanada qulay imkoniyatlarni taqdim etmoqda. Biroq ana shu afzalliklar bilan bir qatorda, ayrim salbiy holatlar ham yuzaga kelmoqdaki, bundan ham ko’z yumib bo’lmaydi. Shulardan biri kiberjinoyatchilikdir.

Kiberjinoyatlar - bu kompyuter, kompyuter tarmog’i yoki tarmoq qurilmasidan suiiste’mol qilishga qaratilgan jinoiy faoliyat hisoblanadi. Ularning aksariyati kiberjinoyatchilar yoki xakerlar tomonidan undan noqonuniy daromad orttirish maqsadida sodir etiladi. Bugun texnologiyalar tobora rivojlanib borgani sari jinoyatchilar ham ulardan foydalanib, noqonuniy xatti-harakatlarni sodir etmoqdalar. Xususan, odamlarning plastik kartalaridan pulni o’marish sezilarli darajada oshdi. Tabiiyki, huquqni muhofaza qiluvchi organlar tomonidan bu jinoyatchilar aniqlanib, tegishli jazo choralari ko’rilmoqda va jabrlanuvchilarga zarar undirib berilmoqda. 2020-yilning birinchi yarmida O’zbekistonda firibgarlik jinoyatlari soni bir yil oldingiga qaraganda ikki barobarga ko’payib, olti oyda 3 ming 881 tani tashkil etgani biz uchun xavotirlidir. Boz ustiga texnologiya rivoj topgani sari firibgarlikning yangidan yangi turlari paydo bo’lmoqda[1].

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. 2022-yilda Toshkentda axborot texnologiyalari

yordamida 4332 ta yoki 2021-yilga (2281 ta) nisbatan qariyb 2 baravar, 2020-yil bilan (106 ta) taqqoslaganda esa 40 baravar ko‘p kiberjinoyat sodir etildi. Bu haqda Toshkent IIBB Axborot texnologiyalari sohasidagi jinoyatlarga qarshi kurashish boshqarmasi vakillari ishtirokida o‘tkazilgan brifingda ma’lum qilindi. Bir yilda qayd etilgan jami jinoyatdan 3372 ta yoki 82 foizi bank plastik kartalardan pul mablag‘larni talon-toroj qilish bilan bog‘liq. Anvar To‘xtayevning so‘zlariga ko‘ra, bunday jinoyatlar birgina O‘zbekistonda emas, balki dunyoning barcha davlatlarida ham ko‘p uchraydi. U MDH davlatlarini yoki boshqa rivojlangan davlatlarning poytaxtlarida ham aynan axborot texnologiyalari yordamida sodir etilayotgan jinoyatlar soni yil sayin ortmoqda. Misol uchun 2022-yil davomida:

Moskvada (Rossiya, 12,6 mln aholi yashaydi) axborot texnologiyalari sohasida 105 360 ta kiberjinoyat qayd etilgan (2021-yilda — 103 600 ta, 2020-yilda — 102 060 ta kiberjinoyat);

Ostonada (Qozog‘iston, 1,3 mln aholi) bunday jinoyatlar 4822 ta aniqlangan (2021-yilda — 4224 ta, 2020-yilda — 5807 ta);

Minskda esa (Belarus, 2 mln ga yaqin aholi) 4773 ta kiberjinoyat sodir bo‘lgani haqida aniq ma’lumotlar bor. (2021-yilda — 4761 ta, 2020-yilda-4 773 ta);

Seulda (Janubiy Koreya, 10,5 mln aholi) 2022-yil 60450 ta kiberjinoyat aniqlangan (2021-yilda — 56210 ta, 2020-yilda — 60450 ta).

Ushbu jinoyatlarga qarshi kurashish uchun IIBB tarkibida Axborot texnologiyalari sohasida jinoyatchilikka qarshi kurashish boshqarmasi ochildi. Boshqarma bank plastik kartalardan pul mablag‘lar talon-toroj qilinishining oldini olishga qaratilgan videorliklar tayyorlab, ularni OAV orqali yoritgan. Uni jami 2,5 mlndan ortiq kuzatuvchilar tomosha qilgan. Internetdan foydalanmaydigan aholi uchun esa hududiy profilaktika inspektorlari 25 mingdan ortiq xonadonlar bilan suhbatlashgan. Bundan tashqari, aholiga flayerlar tarqatilib, aholi gavjum joylarda fuqarolarga bukletlar berilgan[2].

Yuqoridagi holatga nazar tashlaydigan bo’lsak, jinoiy yo‘llar bilan topilgan pul mablag‘lari elektron va kriptohamyonlarda legallashtirilmoqda. Bundan tashqari, aholining axborot texnologiyalari sohasidagi bo‘lgan savodxonligi yetarli darajada emas.

Shu o’rinda kiberterrorizm va uning jamiyat hayotiga solayotgan xavfining ko’lami ham oshib borayotganini ta’kidlash joiz. Kiberterroristik harakat (kiberhujum) - kompyuterlar va axborot kommunikatsiya vositalari yordamida amalga oshirilgan, odamlarning hayoti va sog’lig’iga bevosita xavf tug’diradigan yoki potensial xavf tug’dirishi mumkin bo’lgan, moddiy ob’yektlarga katta zarar

yetkazishi yoki shunga olib kelishi mumkin bo'lgan, ijtimoiy xavfli oqibatlarning boshlanishi yoki maqsadi bo'lgan siyosiy sababdir. Zamonaviy terrorchilar uchun kibermakondan foydalanishning jozibadorligi kiberhujumni amalga oshirish katta moliyaviy xarajatlarni talab qilmasligi bilan bog'liq.

Ekspertlarning xulosasiga ko'ra, bu rivojlanayotgan davlatlarning taraqqiyotiga ko'maklashish, umuminsoniy demokratik tamoyillarni qaror toptirish niqobi ostida fuqarolar ongiga ta'sir o'tkazish, ularni turli yo'llar bilan o'z maqsadlari sari bo'ysundirish orqali amalga oshirilmoqda. Afsuski, bu jarayonda kiberhujumlarni uyushtirish, bu yo'lda internet global tarmog'ining mislsiz imkoniyatlaridan "samarali" foydalanishga urinishlar tobora avj olmoqda. Internetda mavjud ijtimoiy tarmoqlar, ularning ishlab chiqaruvchilari va homiylarining suveren davlat ichki ishlariga "aralashishlari" qanday ahamiyat o'ynashi oxirigacha o'rganilmaganligi bois ba'zan bunday "aralashuv" mazkur davlatga qarshi ekanligi hali hanuz e'tirof etilgani yo'q.

Ijtimoiy tarmoqlar egalari ushbu tarmoqlar sahifalarida davlat tuzumini ag'darishga da'vat qilingani uchun javobgarlikka tortilishining xalqaro miqyosidagi huquqiy asoslari yaratilmagan. Vaholanki, har bir qilingan jinoiy xatti-harakat yoki harakatsizlik mazmun-mohiyatiga ko'ra, albatta, javobsiz va jazosiz qolmasligi kerak. Internet saytlari to'satdan paydo bo'lib, ko'pincha formatini, so'ngra manzilini o'zgartiradi. Shu bois ayrim ekspertlar internetning butkul ochiqligi kabi dastlabki konsepsiyalardan voz kechib, uning yangi tizimiga o'tishni taklif etmoqda. Yangi modelning asosiy mohiyati tarmoqdan foydalanuvchilarning anonimligidan voz kechishdir. Bu tarmoqning jinoiy tajovuzlardan yanada ko'proq himoyalangan bo'lishini ta'minlashga imkon berdi. Shuningdek, kiberjinoyatlar va kiberhuquqbuzarliklarni tergov qilish va ularni aniqlash, bartaraf etish hamda oldini olish bo'yicha zarur qarorlar qabul qilish, kiberjinoyatchilikka qarshi kurashish bo'yicha normativ-huquqiy hujjatlar loyihalarini ishlab chiqishda ishtirok etish, kiberterrorizm, kiberekstremizm, uyushgan jinoyatchilikka qarshi kurashish, davlat organlari manfaatlariga hamda kiberxavfsizligiga tahdid soluvchi kiberxatarlarni aniqlash va ularga qarshi kurashish, kiberjinoyatlar bo'yicha tergovga qadar tekshiruv va dastlabki tergovni o'tkazish, tezkor-qidiruv faoliyatini amalga oshirish, fuqarolarning huquq va erkinliklariga tahdid soluvchi kiberjinoyatlarning sodir etilishiga imkon yaratuvchi sabablar hamda shart-sharoitlarni aniqlash va bartaraf etish kabi muhim vazifalarni bajarishlari lozim[3].

Kiberjinoyatlar turli davrlarda turlicha rivoj topgan kabi uning doktrinal va rasmiy ta'riflari turlichadir. Xususan, **Yevropa Kengashining 2001-yildagi**

“Kiberjinoyat haqida”gi Konvensiyasiga asosan “kiberjinoyat kibermuxitda sodir etiladigan har qanday jinoyatdir[4]. Bu eng to’g’ri fikr, sababi istalgan bir texnologiya rivojlanishi mumkin, biroq ular tomonidan sodir etiladigan qilmishlarning barchasi kibermuxitda sodir etiladi va kibermuxitga barcha texnologiyalar ishtiroki bo’lgan ijtimoiy xavfli qilmishlar bajariladigan jarayonlarni qamrab oluvchi muhit kiradi.

Olim “M.Gurcke”ning fikricha, kompyuter tizimi, tarmog’i, ularga ulanadigan boshqa vositalar orqali yoki ularning yordamida kompyuter tizimi, tarmog’i yoki kompyuter axborotiga qarshi kibermuxitda sodir etiladigan jinoyatlar majmui kiberjinoyatdir[5].

Biroq, “Telekommunikatsiyalar to’g’risida”, “Axborotlashtirish to’g’risida”, “Axborot erkinligi prinsiplari va kafolatlari to’g’risida”gi Qonunlarga asosan, telekommunikatsiyalar tarmog’i, axborot tizimi, axborot tushunchalarining mazmun-mohiyatiga asosan, telekommunikatsiya tarmog’i kompyuter tarmog’i hisoblanmaydi va faqatgina komp’yuter axboroti kiberjinoyatlarning tarkibini tashkil qilmaydi, sababi kiberjinoyatlar kibermuxitda sodir etiladigan har qanday texnologiyalar yordamida sodir etilishi mumkin. [6,7,8].

Olimlar K.E.Zinchenko, L.YU.Ismailova, A.N.Karaxan’yan, B.V.Kiselev, V.V.Krilov, Ya.M.Mastinskiy. N.S.Polevoy, Yu.N.Solov’yev, V.V.Xurgin, S.I.Tsvetkov olimlarning fikricha, bu kabi jinoyatlar elektron hisoblash mashinalari orqali sodir etilgan jinoyatdir [9].

Mazkur tushuncha 1994-yilda berilayotganligi orqali ta’kidlashimiz joizki, O’zbekiston tarixi nuqtai nazaridan O’zbekiston Respublikasining “Elektron hisoblash mashinalari uchun yaratilgan dasturlar va ma’lumotlar bazalarining huquqiy himoyasi to’g’risida” 1994-yil 6-maydagi 1060–XII-son Qonuni [10] aynan 1994-yilda qabul qilinganligi sababli ham mazkur tushuncha vaqt nuqtai nazaridan to’g’ri talqin qilingan. Olimlar N.Salayev va R.Ro’ziyev axborot xavfsizligiga tahdid soluvchi, bevosita kompyuter vositalari orqali yoki axborot texnologiyalari vositasida sodir etiladigan qonunga xilof ijtimoiy xavfli qilmishni axborot texnologiyalari sohasidagi jinoyatlardir deb atab, unga kompyuter jinoyatchiligi sinonim ekanligini ta’kidlashadi. Shuningdek, kompyuter tizimi, tarmog’i, shuningdek, ularga ulanadigan boshqa vositalar orqali yoki ularning yordamida hamda kompyuter tizimi, tarmog’i yoki kompyuter axborotiga qarshi kibermuxitda sodir etilgan ijtimoiy xavfli qilmishni kiberjinoyat deb bayon qilishib, yuqoridagi jinoyatlarni kiberjinoyatdan farqli jinoyat deb ta’rif berishadi[11].

Ma’lumki, kibermuxit komp’yuter jinoyatchiligida ham bo’ladi, hatto Yevropa Kengashining 2001-yildagi “Kiberjinoyat haqida”gi Konvensiyasining rus tilidagi matniga nazar tashlasak ba’zi holatlarda uning kompyuter jinoyatchiligi to’g’risidagi Konvensiya degan tarjimasiga ham guvoh bo’lamiz[12].

Mazkur holatni yanada aniqroq tushunish uchun bitta holatni ko’rib o’taylik, JKning 169-moddasining 3-qismi “b”-bandida nazarda tutilgan komp’yuter texnikasi orqali sodir etiladigan o’g’rilik jinoyatini amalga oshirish uchun kibermuhit, ya’ni virtual muhit bo’lishi kerak, ya’ni o’g’rilik sodir qilishdan oldin jinoyatchi jabrlanuvchining pul mablag’lari saqlanayotgan kartasining paroliga ega bo’ladi hamda telekommunikatsiya yoki Internet tarmog’i yohud boshqa tarmoqdan foydalanib o’zining qilmishini sodir etadi. Aynan mana shu jarayondagi muhitni biz ko’z bilan ko’rolmaymiz, qo’l bilan ushlolmaymiz, ammo jabrlanuvchining kartasidagi kodni terib, qanday qilib jinoyatchi ushbu mablag’larga ega bo’lishini anglay olamiz. Bu muhit esa, kibermuxit deyiladi.

Shuningdek, bunda “Axborotlashtirish to’g’risida”gi Qonunning maqsadi axborotlashtirish, axborot resurslari va axborot tizimlaridan foydalanish sohasidagi munosabatlarni tartibga solishdan iborat bo’lgan holda, unda kompyuter texnikasining tushunchasi ko’rsatib o’tilmagan va u texnik imkoniyatlari nuqtai nazaridan o’zida boshqa axborot texnologiyalarini qamrab ololmasligini, biroq axborot texnologiyasi barcha kompyuter texnologiyalarini, tizimini, tarmog’ini ham qamrab olishini inobatga olish zarur. JKning 4, 10, 14, 16-moddasiga asosan, jinoyat va jazo qonuniylik prinsipiga amal qilishi lozimligini ko’rsatadi. Yuqoridagilarga asosan, mazkur olimlarning fikri ham texnik, ham doktrinal, ham huquqiy jihatdan fikrimizcha rivojlantirilishi maqsadga muvofiq. 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. 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.Toraxodjayeva kiberjinoyatchilikning kompyuter jinoyatchiligidan kengroq tushuncha hisoblanishini ta’kidlab o’tadi[13].

Kiberjinoyatlar tushunchasining vaqtga nisbatan o'zaro bog'liqligini yana 1979 yilda Dallas advokatlar assotsiatsiyasining konferensiyasi tomonidan dastlab kompyuter jinoyatlarining asosiy belgilari o'sha paytdagi mavjud axborotkommunikatsiya texnologiyalarining texnik imkoniyatlari yuzasidan belgilanganligi orqali ta'kidlashimiz mumkin[14].

Olim L.Kochkina kiberjinoyatchilikni "komp'yuter ma'lumotlari sohasidagi jinoyatlar", "axborot jinoyatlari", "komp'yuter uskunalari bilan bog'liq jinoyatlar", "yuqori texnologiyalar kompyuterlaridagi jinoyatlar", "axborot sohasidagi jinoyatlar" deb[15], T.Borodkina ushbu jinoyatlarni axborot sohasidagi jinoyat deb atagandi[16].

Olim I.M.Rassolov esa, ushbu toifadagi jinoyatlarni jinoyat qonunchiligida alohida jinoyat sifatida ko'rishni taklif qiladi.[17].

Sh.Tolmasovning fikricha kiberjinoyat insonlar tomonidan jinoyat maqsadida axborot texnologiyalaridan noqonuniy foydalanishdir[18].

V.A.Dulenko, R.R.Mamlev, V.A.Pestrikovning fikricha, "kiberjinoyat" bu kompyuter tarmog'idan foydalanib sodir etilgan har qanday jinoyat, ya'ni elektron muhitda sodir etilgan har qanday jinoyatdir[19].

I.G.CHekunov ushbu jinoyatni kompyuter va mobil (uyali) aloqa vositalariga qilingan jinoyatdir deb atagan[20].

Olim V.A.Nomokonovning fikriga ko'ra, kiberjinoyatlar kompyuter jinoyatlariga qaraganda ancha kengdir va axborot makonida ular jinoyat fenomenini aniq aks ettiriladi[21]. Bunga o'xshash fikrlarni I.V.Ramanov ham ta'kidlab o'tadi[22].

Ushbu holatni O.A.Kuznetsova tushuntirishga harakat qilib, kiberjinoyatchilik kompyuterdan tashqari, boshqa axborot texnologiyalari va internet tarmoqlari orqali ham sodir etilganligi uchun ham keng tushunchaligini ta'kidlab, kompyuter jinoyatchiligini faqatgina elektron qurilmalar va ularda saqlanayotgan ma'lumotlarga qarshi qaratilgan bo'ladi deb tushuntirish bergan[23].

Shu kabi fikrlar "urist.one" veb saytida ham qayd etilgan bo'lib, unga asosan kiberjinoyat - elektron sohada komp'yuter tizimlari yoki tarmoqlari yordamida yohud ularga qarshi qaratilgan har qanday jinoyatdir[24].

Komp'yuterlar tomonidan modellashtirilgan, insonlar,ob'yektlar, hodisalar, holatlar va jarayonlar to'g'risidagi ma'lumotlarni o'z ichiga olgan, matematik, ramziy yoki boshqa har qanday ma'noda ifodalangan, mahalliy va global kompyuter tarmoqlarida harakat qiladigan yoki har qanday jismoniy yohud virtual qurilma xotirasida saqlanadigan ma'lumotlar, shuningdek, ularni saqlash, qayta ishlash va

uzatish uchun maxsus ishlab chiqilgan dasturlar orqali sodir etiladigan har qanday jinoyatni olim A.V.Fedorov kiberjinoyat deb ataydi[25].

Umumlashtirib shuni aytishimiz mumkinki **kiberjinoyat** deb axborot xavfsizligiga tahdid soluvchi, bevosita kompyuter vositalari orqali yoxud elektron texnologiyalar yordamida internet tarmog'i orqali sodir etiladigan qonunga xilof ijtimoiy xavfli qilmishga aytiladi.

Kiberjinoyatlar qanday uslublarda sodir bo'lmoqda?

1. Bunday jinoyatni sodir etuvchi jinoyatchilar asosan aholining ishonuvchanligidan foydalanib, fuqarolarni turli yo'llar bilan aldaydi va telefonlarga kelgan hech kimga berilmaslik haqida ogohlantirish SMS xabari bilan birga keladigan "maxsus kod" raqamlarini egallab oladi.

2. Masalan, telefonda rusiyzabon shaxs o'zini bank yoki mobil to'lov tizimi xodimi deb tanishtirishi mumkin. U fuqaroning bank plastik kartasiga xakkerlar tomonidan kiberhujum uyushtirayotgani va shunga o'xshash boshqa yolg'on ma'lumotlarni aytib ishontiradi. Keyin uning kartasi haqidagi ma'lumotlarni olib, pullarni o'zlashtiradi.

3. Bank yoki mobil to'lov tizimlarining soxtalashtirilgan saytlari orqali "Foizsiz onlayn kredit" va shunga o'xshash odamlarga qiziq (feyk) xabarlar Telegram, Instagram va Facebook kabi ijtimoiy tarmoqlardan turli havolalar kela boshlaydi.

4. Jinoyatchilar OLX platformasida uyali telefon apparati, dam olish maskanlari yoki boshqa buyumlarni arzon narxlarda savdoga qo'yish orqali fuqarolarning qiziqishini o'yg'otishi mumkin.

5. Internet do'konlarining soxtalashtirilgan ilovalarida fuqarolarni aldov yo'li bilan ro'yxatdan o'tkazish ham hozirgi jinoyat usullaridan biri hisoblanadi.

6. Davlat tomonidan moddiy yordam puli berilayotgani haqida ijtimoiy tarmoqlarda xabar kela boshlaydi. Hozirda prezidentning soxtalashtirilgan saytlari orqali fuqarolarni "chuv tushirish" ommalashmoqda.

7. Ijtimoiy tarmoqlarda o'zini treyderlik bilan shug'ullanuvchi shaxs deb tanishtirib, pul mablag'larini ikki va undan ortiq barovar ko'paytirib berish haqidagi aldovlari bilan fuqarolarning ishonchiga kirish orqali ularning pullari o'zlashtirilmoqda.

8. Jinoyatchilar Telegram orqali viloyatlararo kirakashlik bilan shug'ullanuvchi xaydovchilarning ishochiga kirib, ularni aldashi mumkin. Misol uchun: viloyatlararo qatnovchi taksichilarning Telegram guruhiga noma'lum shaxs uning plastik karta hisobiga pul yuborishi to'g'risida aytib, manzilga yetib kelganda uni naqd ko'rinishda berishga ishontiradi.

9. PUBG, WORLD OF TANK internet o‘yinlarida kuchaytirilgan akkauntni savdoga qo‘yish bilan yoshlarning ishonchiga kirayotganlar ham mavjud.

10. Ijtimoiy tarmoqlarda “arzon tilla buyumlar sotilishi to‘g‘risida"gi yolg‘on e’lonlarni qo‘yish orqali fuqarolarning ishonchiga kirib, ularning mablag‘larini o‘zlashtirayotganlarni ham misol keltirish mumkin.

Xulosa o’rnida bugungi kunda kibermakondagi tahdidlardan samarali himoyalanish uchun xar bir davlat kuchli himoyalangan axborotlari tizimlarini yaratishi, raqamli texnologiyalar sohasida malakali kadrlarni tayyorlash, e’lonlardagi har qanday aksiyalar, pul yutuqlari hamda boshqa takliflarni tashkilotlarning rasmiy veb-sahifasidan qayta tekshirish, saytning rasmiyligiga ishonch hosil qilmasdan ularga o‘z shaxsiy ma’lumotlarni kiritmaslik, ijtimoiy tarmoq hamda messenjerlarda tarqatilayotgan, aksiya va yutuqli lotereya o‘yinlari to‘g‘risidagi reklamalar keltirilgan havolalarni tekshirmasdan oldin ochmaslik, rasmiy bo‘lmagan havolalarni boshqalarga tarqatmaslik, Telegram orqali jo‘natilayotgan yolg‘on xabarlardan kelib chiqib, akkauntga buzib kirmasliklari hamda ishonchliroq himoyalanish uchun ikki bosqichli autentifikatsiyani faollashtirish lozim.

Kirberjinoyatlarga qarshi kurashish uchun bizning O‘zbekiston Respublikasi IIV Akademiyasida kiberjinoyatlarga qarshi kurashish faoliyati kafedrasini tashkil etish, hamda bu sohada malakali kadrlarni tayyorlash lozim deb hisoblaymiz. Shu bilan birgalikda axolining xuquqiy ong va xuquqiy madaniyatini yuksaltirish ham dolzarb masala xisoblanadi.

FOYDALANILGAN ADABIYOTLAR:

1. https://strategy.uz/index.php?news=1150
2. https://iiv.uz/uz/news/kiberjinoyatchilikka-qarshi-kiberxavfsizlik
3. https://www.gazeta.uz/oz/2023/02/21/cyber/
4. YeC от 23.11.2001 года «Конвенцию о компьютерных преступлениях». Будапешт, Серии европейских договоров - № 185. https://rm.coe.int/1680081580.
5. M.Gurcke. Understanding Cybercrime: A Guide for Developing Countries. ITU. 2009.
6. O’zbekiston Respublikasining 1999-yil 20-avgustda qabul qilingan “Telekommunikatsiyalar to’g’risida”gi 822-I-sonli Qonuni // O’zbekiston Respublikasi Oliy Majlisining Axborotnomasi, 1999-yil, № 9, 219- modda; 2004-yil, № 9, 171-modda.
7. O’zbekiston Respublikasining 2003-yil 11-dekabrda qabul qilingan “Axborotlashtirish to’g’risida”gi 560- II-sonli Qonuni // O’zbekiston Respublikasi Oliy Majlisining Axborotnomasi, 2004-yil, № 1-2, 10- modda.

8. O’zbekiston Respublikasining 2002 yil 12 dekabrda qabul qilingan “Axborot erkinligi prinsiplari va kafolatlari to’g’risida”gi 439-II-sonli Qonuni // O’zbekiston Respublikasi Oliy Majlisining Axborotnomasi, 2003 yil, № 1, 2-modda; O’zbekiston Respublikasi Oliy Majlisi palatalarining Axborotnomasi, 2015 yil, № 12, 452-modda.
9. К.Е.Зинченко, Л.Ю.Исмаилова, А.Н.Караханьян, Б.В.Киселев, В.В.Крылов, Я.М.Мастинский. Н.С.Полевой, Ю.Н.Соловьев, В.В.Хургин, С.И.Цветков. Компьютерные технологии в юридической деятельности. Учебное и практическое пособие. –М.: издательство “БЕК”. 1994 г., –с. 304,
10. O’zbekiston Respublikasining “Elektron hisoblash mashinalari uchun yaratilgan dasturlar va ma’lumotlar bazalarining huquqiy himoyasi to’g’risida” 1994-yil 6-maydagi 1060–XII-son Qonuni // O’zbekiston Respublikasi Oliy Kengashining Axborotnomasi, 1994-y., 5-son, 136-modda; O’zbekiston Respublikasi Oliy Majlisining Axborotnomasi, 2002-y., 4-5-son, 74-modda, 9-son, 165-modda; O’zbekiston Respublikasi qonun hujjatlari to’plami, 2011-y., 52-son, 555-modda; Qonun hujjatlari ma’lumotlari milliy bazasi, 04.12.2019-y., 03/19/586/4106-son; 07.01.2020-y., 03/20/600/0023-son
11. N.S.Salayev, R.N.Ro’ziyev. Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar. Monografiya., – T.: TDYUU, 2018, 139-b.
12. https://www.coe.int/ru/web/conventions/full-list/-/conventions/ treaty/185.
13. I.Toraxodjayeva. O’zbekistonda internet tarmog’i orqali sodir etiladigan jinoyatchilikka qarshi kurash muammolari // – T.: Yuridik fanlar axborotnomasi / Vestnik yuridicheskix nauk / Review of law sciences. ilmiy-amaliy jurnali. 2019 (03)-son. 128-132 b.
14. В.А.Широков, Е.В.Беспалова. Киберпреступность: история уголовно-правового противодействия. – М.: “Информационное право”, 2006, № 4. http HYPERLINK "http://center-bereg.ru/h1846.html":// HYPERLINK "http://center-bereg.ru/h1846.html"center HYPERLINK "http://center-bereg.ru/h1846.html"- HYPERLINK "http://center-bereg.ru/h1846.html"bereg HYPERLINK "http://center-bereg.ru/h1846.html". HYPERLINK "http://center-bereg.ru/h1846.html"ru HYPERLINK "http://center-bereg.ru/h1846.html"/ HYPERLINK "http://center-bereg.ru/h1846.html"h HYPERLINK "http://center-bereg.ru/h1846.html"1846. HYPERLINK "http://center-bereg.ru/h1846.html"html.
15. L.Kochkina. Definition of the concept “cybercrime”. Selected types of cybercrime // Сибирские уголовно - процессуальные и криминалистические чтения. 2017. №3 (17). –с 2

16. Т.Н.Бородкина, А.В.Павлюк. Киберпреступления: понятие, содержание и меры противодействия. Социально-политические науки. № 1. 2018. –135-137 с.
17. И.М.Рассолов. Право и Интернет. Теоретические проблемы. –М.: Изд-во НОРМА, 2003. –251-253 с.
18. Sh.Tolmasov. Global makondagi kiberjinoyatchilik. Manba: http://uz.denemetr.com/docs/768/index-29121- 1.html.
19. В.А.Дуленко. Использование высоких технологий криминальной средой. Борьба с преступлениями в сфере компьютерной информации: учебное пособие. Уфа, 2007. – с. 27.
20. И.Г.Чекунов. Киберпреступность: понятие и классификация // Российский следователь. 2012. № 2. – 37-44 с.
21. В.А.Номоконов/ Киберпреступность, как новая криминальная угроза / В.А. Номоконов, Т.Л. Тропина // Криминология. Вчера. Сегодня. Завтра. 2012. №1 (24). – с. 47.
22. И.В.Романов. Понятие киберпреступлений и его значение для расследования // Сибирские уголовнопроцессуальные и криминалистические чтения. 2016. №5 (13). –106 с.
23. Третий пермский конгресс ученых-юристов : материалы междунар. науч.-практ. конф. Пермь, 12 окт. 2012 г. / отв. ред. О.А. Кузнецова. – Пермь : Перм. гос. нац. иссл. ун-т, 2012. – 289 с.
24. Urist.oneвебсайтидан:Киберпреступление.https://urist.one/dolzhnostnyeprestupleniya/kiberprestupnost/.html.
25. А.В.Федоров. Информационная безопасность в мировом политическом процессе. – М.: МГИМОУниверситет, 2006. – 11 с