

KIBERJINOYATCHILIK – YANGI GLOBAL XAVF**Ro'zimov Qudratbek Qurbonboyevich****Buxoro Davlat Universiteti****“Tarix va yuridik” fakulteti, “Yurisprudensiya” yo’nalishi 1-bosqich talabasi****e-mail: rozimovqudratbek@gmail.com****<https://doi.org/10.5281/zenodo.8046039>**

Annotatsiya. Bugungi kunda kiberjinoyatchilik butun dunyoda global muammoga aylanib boryapti. Millionlab insonlar kiberjinoyatchilarning maqsadlari girdobiga tushib, jabrlanuvchiga aylanib qolgan va katta miqdorda moliyaviy zarar ko'rgan holatlar ham ko'plab kuzatilmoqda. Ayniqsa, hozirgi globallashuv davrida bunday noxush vaziyatlar yanada ko'paymoqda. Shuni inobatga olgan holda, ushbu maqolani yozishdan asosiy maqsad: Kiberjinoyatchilarning yolg'on gaplariga aldanib qolishni oldini olish, dunyo hamjamiyatida, ayniqsa, O'zbekiston Respublikasida kiberjinoyatchilikka barham berish va bu borada olib borilayotgan ishlarni tahlil qilish, eng asosiysi, fuqarolarning huquq va manfaatlarini himoya qilgan va ta'minlagan holda, kiberjinoyatchilik bartaraf etilgan farovon jamiyat qurish borasida izchil fikrlarni bayon qilishdan iborat.

Kalit so'zlar: globallashuv, kiberjinoyat, reklama, veb-sayt, passport raqam, kiberxavfsizlik, kibermakon, firibgarlik, xisob raqam, kod, ijtimoiy sug'urta, kredit karta, antivirus dastur, ijtimoiy tarmoq, internet, kiberterrorizm.

Kirish

Hozirgi zamon, globallashuv davrida yashar ekanmiz, insoniyatda qulayliklar bilan birgalikda bir qancha muammolar ham mavjud. Juda tezlik bilan rivojlanib borayotgan ijtimoiy tarmoqlar dunyo xalqiga ijobiy va salbiy tomonlardan ta'sir ko'rsatmoqda. Bugungi kunda hech bir inson o'z hayotini internetsiz tasavvur qila olmaydi. Fuqarolar ijtimoiy tarmoqlardagi kerakli bo'lgan ma'lumotlardan foydalanish bilan bir qatorda ayrim firibgarlarning norasmiy xabarlariga aldanib qolishlari va katta miqdordagi pul mablag'larini yo'qotish xavfi ham mavjud. Shunday xavflardan biri kiberjinoyatchilik xavfi hisoblanadi.

Kiberjinoyatchilik – axborotni egallash, uni o'zgartirish, yo'q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda (axborot texnologiyalari yordamida yaratilgan virtual muhit) dasturiy ta'minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig'indisi hisoblanadi[1]. Sotsiologlarning fikricha XXI asrda an'anaviy jinoyatlardan ko'ra kiberjinoyatning xavfi yuqori deya baxolanmoqda. Insoniyat kompyuterlar va ijtimoiy tarmoqlardan foydalanar ekan, shaxsiy xavfsizligiga alohida e'tibor qaratishi zarur. Hozirgi kunda butun dunyoda kiberjinoyatning turli ko'rinishlari mavjud. Axborotlarni o'g'irlash, o'zgartirish yoki yo'q qilish, fuqarolarning shaxsiy xisob raqami kodini buzgan holda ularning pul mablag'larini yechib olish, reklama firibgarligi va boshqalar bunga misol bo'lishi mumkin. Bugungi kunda har qanday tadbirkorlikning rivojlanishida reklama katta ro'l o'ynaydi. Shu sababli tadbirkorlik subyektlari reklamalardan keng miqiyosda foydalanadilar. Fuqarolar ba'zi bir saytlarga kirganlarida, ushbu saytlarda “siz pul yutig'iga ega bo'ldingiz yoki yuqori daromadli ishga taklif qilamiz” degan manoda va shu kabi boshqa turdagi reklamalar ham ko'plab uchraydi. Aslida yo'q bo'lgan yutug'ingizni olish yoki ishga joylashtirib qo'yish uchun sizdan shaxsiy ma'lumotlaringizni (passport raqam, yashash manzil, shaxsiy karta raqami va boshqalar) so'rash orqali ham kiberjinoyatchilar o'zlarining maqsadlarini amalga oshirishlari, ya'ni, sizning kartangizdan pul mablag'ini yechib olishlari mumkin. Bugungi

globallashuv davrida jamiyatda shunga o'xshash kiberjinoyatlar ko'payib bormoqda va keng tarqalmoqda, buni esa siz va bizni xushyorlikka chaqiruvchi belgi deya hisoblasak bo'ladi. Hozirda kiberjinoyatlar butun dunyo mamlakatlarida rivojlanib bormoqda. Xususan AQSh, Xitoy va Yevropaning ko'plab mamlakatlarida bunday jinoyatlar yildan-yilga avj olib bormoqda. AQSh Federal Qidiruv Byurosi (FBR) rahbari Robert Myullerning "Kiberxavfsizlik har bir davlat uchun strategik masala. Avval asosan davlat sirlari va yuqori texnologiyalar nishonga olingan bo'lsa, hozir jinoyatchilar mo'ljalni kengroq olmoqda" degan fikrlari bunga misol bo'lishi mumkin[2]. Bundan ko'rinib turibdiki, kiberjinoyat yangi global muammoga aylanib boryapti. Bu esa har bir davlatni va fuqarolarni o'zlarining xavfsizligiga e'tiborli bo'lishlarini talab qiladi.

Statistikaga qaraganda, 2014-yilda chop etilgan hisobotda jahon iqtisodiyotiga yetkazilgan yillik zarar 445 milliard dollarni tashkil qilgan. Cybersecurity Ventures tomonidan 2016-yilgi hisobotda kiberjinoyatlar natijasida yetkazilgan global zararlar 2021-yilga kelib yiliga 6 trillion dollargacha, 2025-yilga kelib esa 10,5 trillion dollargacha ko'tarilishi bashorat qilingan edi. 2012-yilda AQShda onlayn kredit va debet kartalaridagi fribgarlik oqibatida taxminan 1,5 milliard dollar yo'qotilgan. 2018-yilda Strategik va xalqaro tadqiqotlar markazi (CSIS) tomonidan McAfee bilan hamkorlikda o'tkazilgan tadqiqot shuni ko'rsatadiki, har yili global Yalpi Ichki Maxsulotning qariyb bir foizi, ya'ni 600 milliard dollarga yaqini kiberjinoyatlar tufayli yo'qoladi[3]. Shu sababdan ham har bir jismoniy va yuridik shaxslar, davlat organlari, nodavlat-notijorat tashkilotlar, korxonalar va boshqa muassasalar o'zlarining kiberxavfsizligi ta'minlanganligiga ishonch hosil qilishlari zarur.

Kiberxavfsizlik – tizim, tarmoq va dasturlarni raqamli hujumlardan himoyalash amaliyoti hisoblanadi[4].

Asosiy qism

Kiberjinoyatchilik termini taxminan 20 yillik yaqin o'tmishda paydo bo'lgan bo'lishiga qaramasdan jahon hamjamiyatida kiberjinoyatchilikka qarshi kurash insonning huquq va manfaatlarini himoya qilish yo'lidagi asosiy vazifalardan biriga aylangan. Fuqarolarning huquqlarini himoya qilish va ularning ijtimoiy tarmoqlardan erkin foydalanishlarini ta'minlash maqsadida jahon mamlakatlari, shu jumladan, O'zbekiston Respublikasida ham har bir fuqaroning shaxsiy bank xisob raqami va boshqa shaxsiy obyektlarini ishonchli kodlash tizimi yo'lga qo'yilgan. Bu esa fuqarolarni kiberjinoyatchilarning maqsadlari yo'lida jabrlanuvchiga aylanib qolishlarini oldini oladi.

2022-yil 15-aprelda "Kiberxavfsizlik to'g'risida" O'RQ-764-sonli O'zbekiston Respublikasi Qonuni qabul qilingan[5]. Ushbu qonunda kiberjinoyatni oldini olish borasidagi asosiy vazifalar belgilab beringan bo'lib, O'zbekiston Respublikasi Davlat Xavfsizlik Xizmati kiberxavfsizlik sohasidagi vakolatli davlat organi qilib belgilangan va unga qo'shimcha vakolatlar yuklatilgan. Kiberjinoyatchilik atalamasi mamlakatimizga yaqinda kirib kelgan bo'lsa ham uning xavflilik darajasi yildan-yilga ortib bormoqda. Shu sababli O'zbekiston Respublikasi fuqarolarning kiberxavfsizligini ta'minlashni o'zining asosiy vazifalaridan biri etib belgilagan. O'zbekiston Respublikasi Jinoyat kodeksida belgilab qo'yilgan normalar ham bunga misol bo'la oladi. Jinoyat kodeksining 2784 – moddasi "Kompyuter axborotini modifikatsiyalashtirish" deb nomlanadi va unda quyidagicha belgilab qo'yilgan:

"Kompyuter axborotini modifikatsiyalashtirish, ya'ni kompyuter tizimida saqlanayotgan axborotni qonunga xilof ravishda o'zgartirish, unga shikast yetkazish, uni o'chirish, xuddi

shuningdek bila turib unga yolg'on axborotni kiritish fuqarolarning huquqlariga yoki qonun bilan qo'riqlanadigan manfaatlariga yoxud davlat yoki jamoat manfaatlariga ko'p miqdorda zarar yoxud jiddiy ziyon yetkazilishiga sabab bo'lsa, – bazaviy hisoblash miqdorining yuz baravarigacha miqdorda jarima yoki bir yilgacha axloq tuzatish ishlari yoki ikki yilgacha ozodlikni cheklash yoxud ikki yilgacha ozodlikdan mahrum qilish bilan jazolanadi.

O'sha harakatlar:

- a) juda ko'p miqdorda zarar yetkazgan holda;
- b) bir guruh shaxslar tomonidan oldindan til biriktirib;
- v) takroran yoki xavfli retsidivist tomonidan sodir etilgan bo'lsa, – bir yildan ikki yilgacha axloq tuzatish ishlari yoki ikki yildan uch yilgacha ozodlikni cheklash yoki ikki yildan uch yilgacha ozodlikdan mahrum qilish bilan jazolanadi"[6]. O'zbekiston Respublikasida kompyuter axborotlari ustida noqonuniy harakatlarni amalga oshirish jinoiy javobgarlikka sabab bo'ladi. Bu esa mamlakatimizda kiberjinoyatchilikni oldini olish yo'lida muhim ro'l o'ynaydi.

Bugungi kunda O'zbekiston Respublikasida kiber jinoyatchilikni oldini olish va axborot xavfsizligini ta'minlaydigan Kiberxavfsizlik departamenti o'z faoliyatini olib bormoqda. Ijtimoiy tarmoqlarda foydali veb-saytlar bilan bir qatorda fuqarolarning, ayniqsa yoshlarning ongini zaxarlaydigan veb-saytlar ham ko'plab uchraydi. O'zbekiston Respublikasi Kiberxavfsizlik markazi shunday saytlar yuzasidan tekshiruvlar ham olib boradi. Tekshiruv statistikasiga qaraganda 2022-yilning birinchi yarim yillik holatiga ko'ra ekspertizadan o'tkazilgan veb-saytlar soni 124 nafarni tashkil qilgan[7]. Kiberjinoyatchilik yangi global muammo bo'lsa ham, milliy qonunchiligimizda unga barham berish va fuqarolarning huquqlarini himoya qilish borasidagi normalar qat'iy belgilab qo'yilgan hamda bu borada izchil vazifalar amalga oshirilmoqda.

Kiberjinoyatning eng keng tarqalgan turlaridan biri bu – shaxsni o'g'irlash, ya'ni, boshqa bir shaxsning shaxsiy ma'lumotlarini (ijtimoiy sug'urta raqami, bank xisob raqami, kerdit kartalari va boshqalar) o'g'irlash va ulardan noqonuniy maqsadlar yo'lida foydalanish hisoblanadi. Ushbu kiberjinoyat va uning boshqa turlaridan himoyalashning bir nechta usullari mavjud bo'lib, ular quyidagilardan iborat:

- Xushyorlik – bank xisob raqami va boshqa shaxsiy ma'lumotlarni tekshirib turish lozim. Agar shubhali harakatlar mavjud bo'lsa tegishli organlarga zudlik bilan murojaat qilish kerak.
- Shaxsiy ma'lumotlar va rasmlarni xavfli bo'lgan ijtimoiy tarmoq saytlariga joylashtirishdan ximoyalash – fuqarolar o'zlarining shaxsiy ma'lumotlari va shaxsiy rasmlarini xavfsizligini tekshirmasdan turib, istalgan saytlarga yoki boshqa tarmoqlarga joylashtirmasliklari zarur.
- Shaxsiy kodlarni o'zgartirib turish – ushbu amaliyot kibrtjinoyatchilar tomonidan fuqarolarning ijtimoiy tarmoqlardagi xisob raqamlariga kirib ularning mulklari va boshqa shaxsiy ma'lumotlarini o'g'irlab olish xavfini oldini olishga ko'maklashadi.
- Murakkab kodlarni yaratish – har bir fuqaro o'zlarining shaxsiy ma'lumotlarini himoyalashda katta va kichik harflar hamda raqamlar ishtirok etgan murakkab kodlardan foydalanishlari maqsadga muoffiq bo'ladi.
- Ikki bosqichli kod tizimini o'rnatish – bunda kiberjinoyatni maqsad qilib olgan firibgarlar fuqaroning shaxsiy kodini buzib uning hisob raqamiga kirgan taqdirda ham ikkinchi bosqich kodi kibrtjinoyatning xavfini oldini oladi.

- Antivirus dasturlaridan foydalanish – ushbu dasturlar kibrtjinoyat xavfini oldini olish xususiyatiga ega bo'lib, fuqarolarning shaxsiy ma'lumotlarini himoya qilishda yordam beradi. Har bir fuqaro internet tarmoqlarida o'z shaxsiy daxlsizligiga alohida e'tibor qaratishlari va yuqorida sanab o'tilgan tavsiyalarni e'tibordan chetda qoldirmasliklari shart.

Ko'pchilikka ma'lumki, hozirda eng ko'p rivojlangan internet tarmog'i "Facebook" hisoblanadi. Ushbu tarmoqda va bundan tashqari "Telegram", "Instagram" kabi ijtimoiy tarmoqlarda, turli veb-saytlarda kiberterrorizm targ'ibotchilari ham mavjud. Bunday targ'ibotchilarning asosiy maqsadi fuqarolarni va asosan yoshlarning ongini zaxarlash, turli terroristik va ekstremistik g'oyalarni targ'ib qilish, ommaviy qo'rquvni yuzaga keltirishdan iborat. Shunday kiberjinoyatchilarning changaliga tushib qolmasliklari uchun, fuqarolar har doim xushyor bo'lishlari va xavfsizligini tekshirmasdan turib turli ijtimoiy tarmoqlarga kirmasliklari zarur. Bunday kiberjinoyatchilar mamlakat tinchligiga ham tahdid qilishlari mumkin va ayni shunday holatda davlatlar ham xushyorlikni yo'qotmasliklari shart. Zero, tinchlik eng oliy ne'matlardan biri hisoblanadi!

Xulosa

Tadqiqotlar natijasi shuni ko'rsatyaptiki, kiberjinoyatlar faqat fuqarolarning shaxsiy daxlsizligiga tahdid solibgina qolmay, davlat organlari va boshqa tashkilotlarning ham manfaatlariga zarar yetkazishlari mumkin. Kiberjinoyatni maqsad qilib olgan firibgarlarning g'oyalari dunyo hamjamiyatining diqqat markazida bo'lishi zarur va bunga qarshi birgalikda kurash olib borish maqsadga muvofiq bo'ladi. Aks holda bunday jinoyatlar dunyo bo'ylab yanada keng tarqalishi va ko'plab insonlarning aziyat chekishiga sabab bo'lishi ehtimoldan holi emas.

O'zbekiston Respublikasida ham kiberjinoyatni oldini olish birasida ko'plab ishlar olib borilmoqda. Shunga qaramasdan, mamlakatimizda kiberjinoyatlarni tergov qilish sohasidagi ayrim kamchiliklar ko'zga tashlanmoqda. Kiberxavfsizlik sohasidagi malakali kadrlarning yetishmasligi, zamonaviy texnika va texnologiyalarning kamligi, banklar va shu kabi boshqa muassasalarni kiberjinoyatchilardan himoya qilish bo'yicha dasturlarning yetarli darajada ishlab chiqilmaganligi, ekspertizadagi muammolarni bunga misol qilib ko'rsatish mumkin. Davlatimiz ushbu muammolarni oldini olish yuzasidan ko'plab islohotlarni amalga oshirmoqda. O'zbekiston Respublikasida yashovchi har bir fuqaroning huquqlari va erkinliklari davlat muhofazasiga olingan. Shunday bo'lsa ham fuqarolar har qanday ishni amalga oshirayotganlarida yoki ijtimoiy tarmoqlardan foydalanayotganlarida o'z xavfsizliklarini ta'minlagan xolda, xushyor bo'lishlari shart. O'zbekistonning kelajagi hisoblanmish rivojlanib, o'sib-ulg'ayib borayotgan yosh avlodning o'rtasida ham kiberjinoyatchilik xavfini oldini olishga alohida e'tibor qaratish zarur. Buni amalga oshirishda yoshlarning huquqiy ongi, huquiy bilimi va ko'nikmalarini yanada oshirishga qaratilgan qo'shimcha chora-tadbirlar, tashviqotlar, kiberjinoyatlarga qarshi kurash xissini uyg'otuvchi festivallar va shuningdek bellashuvlarni o'tkazish alohida ahamiyat kasb etadi.

Aziz yurtdoshlar, internet tarmoqlaridan foydalanar ekanmiz, shaxsiy xavfsizligimizga e'tiborli bo'laylik!

References:

1. O'zbekiston Respublikasining 2022-yil 15-apreldagi "Kiberxavfsizlik to'g'risida"gi O'RQ-764-son Qonuni.

2. amerikaovozi.com sayti.
3. kiberjinoyat – vikipediya.
4. S.K.Ganiev, A.A.Ganiev va Z.T.Xudoyqulov. Kiberxavfsizlik asoslari. O'quv qo'llanma. Toshkent 2020-yil. 8-bet.
5. lex.uz sayti.
6. 1995-yil 1-aprelda qabul qilingan O'zbekiston Respublikasi Jinoyat kodeksi.
7. O'zbekiston Respublikasi Kiberxavfsizlik markazi – bosh sahifasi (csec.uz sayti).

