# XALQARO XUSUSIY HUQUQDA IJTIMOIY TARMOQLAR VA KIBER JINOYATLAR

**Mirgulshanbekov Hiloliddin O’ktamjon o’g’li**
*Toshkent davlat yuridik universiteti Xalqaro huquq fakulteti 3-kurs talabasi*

**Anotatsiya:** *Ushbu maqolada ijtimoiy tarmoqlar va u yerda sodir etilgan jinoyatlar, kiberjinoyatchilik, kiberjinoyatchilik turlari, ya’ni kiber tovlamachilik, kiberterrorchilik hamda behayo yoki haqoratomuz kontentlar yaratish va tarqatishga qarshi kurashish haqida keng yoritib berilgan. Shuningdek, kiber jinoyatchilarga qarshi xavfsizlik choralarini ko’rish va ularga barham berish haqida so’z yuritilgan.*

**Kalit so’zlar:** *ijtimoiy tarmoq, kiberjinoyatlar, internet, kiberhujum, jinoyat kodeksi, kiberterrorizm, tahdid, kiber tovlamachilik.*

**Аннотация:** *В этой статье подробно рассматриваются социальные сети и совершаемые там преступления, киберпреступность, типы киберпреступности, то есть кибер-вымогательство, кибер-терроризм, а также борьба с созданием и распространением непристойного или оскорбительного контента. В нем также говорилось о мерах безопасности и ликвидации киберпреступников.*

**Ключевые слова:** *социальная сеть, киберпреступления, интернет, кибератака, уголовный кодекс, кибертерроризм, угроза, кибервымогательство.*

**Anotation:** *this article provides extensive coverage of social networks and crimes committed there, cybercrime, types of cybercrimes, cyberterrorism and the fight against the creation and dissemination of obscene or offensive content. It also referred to the implementation of security measures against cybercriminals and their elimination.*

**Key words:** *social network, cybercrimes, internet, cyberattack, criminal code, cyber terrorism, threat, cyber extortion.*

## Kirish

Bugungi kunda, ko’pchilik ijtimoiy tarmoqlarda joylashtirgan shaxsiy yoki boshqa ma’lumotlarni har kim topishi va har doim ham yaxshi niyat bilan ishlatmasligi mumkinligini anglamaydi. Ijtimoiy tarmoqlardagi shaxs haqidagi ma’lumotlarni do’stlari, qarindoshlari, turli turdagi jinoyatchilar va boshqa shaxslar bemalol topishlari mumkin. Chunki, biz zamonaviy texnalogiyalar rivojlangan asrda yashamoqdamiz. Shuningdek, ba’zi korxonalarda, davlat organlarida, maktablarda va turli xildagi tashkilotlarda ijtimoiy tarmoqdan foydalanishda ba’zi cheklovlar bor. Bu nafaqat iqtisod nuqtayi nazaridan, balki shaxsiy ma’lumotlarni tarqalishini oldini olish uchun ham foydalidir. Sud ijrochilari esa ba’zan ijtimoiy tarmoqlardan qarzdorlarni topish yoki ularning mulki haqida ma’lumot olish uchun foydalanadilar[33].

Ijtimoiy tarmoq oddiy so’zlar bilan tushintirilganda, qiziqishlari o’xshash bo’lgan odamlar o’rtasida onlayn muloqot qilish, tanishish va turli musiqa va filmlar tomosha qilish hamda onlayn ishlarni amalga oshirish uchun foydalaniladigan platforma. Shuningdek,

[33] Banki lovyat doljnikov cherez „Odnoklassnikov“, „V kontakte“ i „Moy krug“ // NEWSru.com

ijtimoiy tarmoq orqali turli ish o’rinlarini kuzatib borish va hujjat topshirish, ish o’rganish, yangiliklarni o'qish va boshqa kerakli maqsadlarda foydalanishingiz mumkin.

Hozirda ijtimoiy tarmoqlarda juda ham ommalashib ketgan turli bloger, youtuber va tiktokerlarni tanqid, noto’g’ri sharxlar va turli haqoratlarga duch kelishayotganligini guvohi bo’lyapmiz.

Ijtimoiy tarmoqlarda muloqot qilishga qaramlik tufayli psixosomatik kasalliklar paydo bo‘lishi holatlari kuzatilgan — Belgradda foydalanuvchi Snejana Pavlovich “Facebook” ijtimoiy tarmog‘idagi qaydi uning onlayn do‘stlari orasida qiziqish uyg‘otmaganidan keyin psixiatriya klinikasiga yotqizilgan. Klinika shifokorlari ushbu holatni “Snejana sindromi” deb atashdi va bemorning xatti-harakatlarini zamonaviy dunyoda shaxsning ijtimoiy ehtiyojlarini qoniqtirilmasligidan kelib chiqqan oddiy stress deb izohladilar[34].

Ijtimoiy tarmoqlardan foydalanish xavfi mavzusi turli ilmiy maqolalarda yoritilgan, jumladan:

- D. Boyd AQShning 16 shtatidagi so‘rovnoma materiallariga asoslanib, ijtimoiy tarmoqlardan kelib chiqadigan ikkita asosiy “qo‘rquv” bor, degan xulosaga keldi: jinsiy zo‘ravonlik va ma’lumotlarning maxfiyligi;

- Daniyada davriy nashrlarning mazmunini tahlil qilib, M. Larsen eng ko‘p tilga olinadigan ijtimoiy media muammolari ro‘yxatini tuzadi, jumladan: jinsiy zo‘ravonlik va pedofiliya, qo‘rqitish va ta’qib qilish, tahdid va zo‘ravonlik, millatchilik g‘oyalari tarqalishi;

- K. Fuks nemis va avstriyalik talabalar orasida o‘tgan onlayn so‘rovnomadan quyidagi xavflar ro‘yxatini oldi: ma’lumotlarning maxfiyligi, spam, shaxsiy ma’lumotlarni yo‘qotish ehtimoli, salbiy imidj yaratish, internetga qaramlik;

- S. V. Bondarenko Rossiya janubidagi virtual tarmoq hamjamiyatlarini o‘rganib, deviant xatti-harakatlarning quyidagi shakllari mavjud degan xulosaga keldi: xakerlik, maxfiylikni buzish, tuhmat, kiberterrorizm, kompyuter pedofiliyasi[35].

Shuningdek, hozirgi o’smirlar orasida turli onlayn o’yinlar va dasturlar keng tarqalgan va bularning ba’zilari insonni o’z joniga qasd qilishni targ’ib qiladi va bolalarni o’z joniga qasd qilishga undaydi. Bu ijtimoiy tarmoqlarda “O’lim guruhlari” faoliyati deb tushuniladi. Shunday o’yinlarga yaqqol misol: “O’lim guruhlari” ning xavfli o`yiniga 2015-yilda o`zini poyezd tagiga tashlagan, o’sha paytda 16 yoshda bo’lgan Rina Polenkovaning harakatlari turtki bo’lgan. U o`z joniga qasd qilishdan avval ijtimoiy tarmoqdagi sahifasida “nya, poka” deya post qoldiradi va shundan so’ng boshini kelayotgan poyezd tagiga tutadi. Joniga qasd qilishiga sabab esa yigitining tashlab ketgani bo’lgan. Bu baxtsiz hodisaga TV va taniqli blogerlar e`tibor qaratadi. Bu esa o’smirlar orasida o`z joniga qasd qilish ommalashishiga sabab bo`ladi. Birinchi “ko’k kit” guruhi tashkil etilishi ham aynan ana shu jarayonlarga to’g’ri keladi. Nega bu “o’lim guruhlari” aynan “ko’k kit” ni ramz sifatida tanlashgan? Chunki ko’k kitlar tez-tez depressiya sabab o’zini qirg’oqqa, quruqlikka tashlab joniga qasd qilishadi. Mazkur ilk guruh shu tariqa Rinaning o`limini yoshlar orasidan tatbiq qila boshlaydi. Qurbonlar esa o`tish davridagi o’smir yoshlar hisoblanadi[36]. 2016-yilda Rospotrebnadzor

[34] „Россия в социальных сетях: какой ущерб от виртуальной жизни?“. ТАСС.
[35] Ефимов, Кузнецов 2011
[36] https://darakchi.uz/oz/24470

hayotni ixtiyoriy ravishda tark etishni tashviqot qiluvchi va uning turli usullarini tavsiflovchi materiallarning uchdan biridan ko‘prog‘i VKontakte ijtimoiy tarmog‘ida to‘planganligini aytdi[37]. 2017-yil 7-iyundan boshlab Rossiyada Internetda “o‘lim guruhlari” ni tashkil etganlik uchun jinoiy javobgarlik to‘g‘risidagi qonun kuchga kirdi, u 6 yilgacha qamoq jazosini ko‘zda tutadi[38]. VKontakte ijtimoiy tarmog‘ining yaratuvchisi Pavel Durov DLD konferensiyasida bergan intervyusida internet-trolling muammolarini aytib o‘tdi va ularni Telegramning tayyor server yechimlari va protokollaridan foydalangan holda LiveOnce yangi ijtimoiy tarmog‘ini yaratish orqali hal qilishga va’da berdi[39].

**Xuddi shu voqelarda so’ng,** O’zbekiston Respublikasining 2017-yil 13-iyundagi O’RQ-436-sonli Qonuniga asosan, 103[1]-moddasi, ya’ni O‘zini o‘zi o‘ldirishga undash, ya’ni ko‘ndirish, aldash yoki boshqa yo‘l bilan o‘zga shaxsda o‘zini o‘zi o‘ldirish hissini uyg‘otish, agar shaxs o‘zini o‘zi o‘ldirgan yoki o‘zini o‘zi o‘ldirishga suiqasd qilgan bo‘lsa, ikki yildan besh yilgacha ozodlikni cheklash yoxud besh yilgacha ozodlikdan mahrum qilish bilan jazolanadi. O‘sha harakatlar: ikkinchi qism “v” bandiga ko’ra, telekommunikatsiya tarmoqlaridan, shuningdek Internet butunjahon axborot tarmog‘idan foydalanib sodir etilgan bo‘lsa, besh yildan yetti yilgacha ozodlikdan mahrum qilish bilan jazolanishi belgilangan.

Hozirgi rivojlangan asrda turli xil global muammolar uchramoqda va ular qatoriga kiber jinoyatlarni qo’shsak ham bo’ladi. Kiber jinoyatchilikning biz bilgan kompyuterlarga virus tarqatish, parollarni buzish va ma’lumotlarni o’zlashtirish, kredit karta mablag’larini o’zlashtirish, kompyuterlarni ishdan chiqarish, shuningdek, internetdagi turli saytlar orqali ma’naviy buzuq ma’lumotlarni, bo’hton izohlarni tarqatish orqali jamiyatga rahna solinyapti.

**“Kiberjinoyatchilik”** – bu rivojlangan kompyuterlar orqali turli tarmoq va web-saytlardan foydalangan holda turli onlayn jinoyatlarni amalga oshirish tushuniladi. Ushbu jinoyat paytida kompyuterlar jinoyat quroli ro’lini o’ynaydi. Ushbu jinoyat orasiga virtual tarmoqlarda daxshat uyg’otish, qonunga zid axborotlar yaratish va tarqatish, virus va shunga o’xshash dasturlar, begona shaxs ma’lumotlariga noqonuniy kirish, xakerlik hujumi, firibgarlik va boshqa turdagi jinoyatlar shular jumlasidandir. Kiber jinoyatlar yo kimningdir xavfsizligiga zarar keltirish yoki moliyaviy zaxirasini o’g’irlash maqsadida amalga oshiriladi.

Shu o’rinda maxfiy ma’lumotlar qonuniy tarzda himoya qilingan holatda yuz berayotgan kiberjinoyatlar soni kundan kunga oshib bormoqda. Kiber hujum kompyuterlar va turli axborot kommunikatsiya vositalari orqali amalga oshirilgan va insonlar hayoti va sog’lig’iga xavf tug’diradigan, moddiy obyektlarga zarar yetkazish va ijtimoiy xavfli oqibatlarga olib kelishi mumkin bo’lgan xarakatdir. Shuningdek, kiber hujumni katta xarajat talab qilinmaydigan jinoyatlar qatoriga kiritishimiz mumkin. Lekin, ba’zi bir terorchilik guruhlari internet tarmog’i orqali insonlarga moliyaviy yordam ko’rsatish, barqarorlikni ta’minlash kabi aldov yo’llar bilan fuqarolar ongiga ta’sir ko’rsatish, ularni turli yo’llar bilan o’z maqasadlari sari bo’ysundirishga urinishmoqda va bunga aldanganlar ham kam emas. Lekin ba’zi davlatlar yopiq tarmoq tizimiga o’tishga xarakat qilmoqda va bu ichki hududda xavfsizlik, ma’lumotlarni yaxshi saqlanishi, onlayn hujumlarni kamaytirish va boshqa funksiyalarni amalga oshirishda qulay usul deb hisoblayman. Misol uchun: yopiq tarmoq tizimiga o'tgan

[37] „Треть пропагандирующих суицид интернет-страниц пришлась на «ВКонтакте»“. Lenta.ru
[38] Putin podpisal zakon ob ugolovnoy otvetstvennosti za sozdanie „grupp smerti“ // Интерфакс, 07.06. 2017
[39] „Pavel Durov“. DLD Conference.

Xitoy davlatini va bunday jarayonga tayyorgarlik ko'rayotgan Rossiya davlatini keltirishimiz mumkin.

Maxfiy ma’lumotlar kuchli himoya tizimiga ega bo’lgan holatda ham turli xildagi kiberjinoyatlar yuz bermoqda. Shuningdek, kiber o’g’rilik, tovlamachilik, moliyaviy firibgarlik, josuslik va boshqa shu kabi jinoyatlar bilan davlat organlari izchil ishlar olib bormoqda. Amerikalik tadbirkor Warren Buffet esa kiberjinoyatni “insoniyatning birinchi raqamli muammosi” deb ta’riflaydi[40].

Endigi navbatda kiberjinoyat turlari haqida ma’lumot berib o’tadigan bo’lsak, ulardan biri kiber tovlamachilikdir.

**Kiber tovlamachilik** – bu xakerlar tomonidan shaxsiy ma’lumotlarni, veb-saytni va kompyuter tizimini buzib kirish va xizmat ko’rsatishni o’chirib qo’yish, onlayn tahdid qilish yoki boshqa harakatlarni amalga oshirish jarayonida sodir bo’ladi. Shuningdek, ushbu jinoyatchi xakerlar hujumni to’xtatish va buning evaziga pul talab qilish orqali o’z jinoyatlarini davom ettirishadi.

Huddi shunday jinoyat turiga misol keltiradigan bo’lsam: IIV Kiberxavfsizlik markazi bergan ma’lumotga ko’ra, Buxoro viloyati G’ijduvon tumanida yashovchi, talaba yigit F.B. ariza bilan murojaat qilib, telegram messenjerida o’zini “Tojiboeva Rayxon” deb tanishtirgan noma’lum shaxsga boshqalar ko’rishi mumkin bo’lmagan shaxsiy fotosuratlarini ishonib, messenjer orqali yuborganligini, noma’lum shaxs fotosuratlarni olib, ijtimoiy tarmoqlar orqali tarqatmaslik uchun 900 ming so’m pul talab qilayotganligini ma’lum qilib, unga nisbatan qonuniy chora ko’rishlikni so’ragan. Tezkor-qidiruv tadbirlari natijasida o’zini “Tojiboeva Rayxon” deb tanishtirgan noma’lum shaxs Samarqand viloyati Oqdaryo tumanida yashovchi 1999-yilda tug’ilgan erkak jinsiga mansub fuqaro J.Sh. ekanligi aniqlangan. Fuqaro J. Sh. ga nisbatan Jinoyat Kodeksining 165-moddasi bilan jinoyat ishi qo’zg’atilib, tergov harakatlari olib borilyotganligi aytilgan[41].

Bundan ko’rish mumkinki, jamiyatimizda bunday holatlar juda ham ko’p sodir bo’lmoqda. Shuningdek, O’zbekiston Respublikasi jinoyat kodeksining 165-moddasi “Tovlamachilik” ya’ni jabrlanuvchiga zo‘rlik ishlatish, uning shaxsiy mulkiga zarar keltirish yoki jabrlanuvchi uchun sir saqlanishi lozim bo‘lgan ma’lumotlarni oshkor qilish bilan qo‘rqitib, undan pul yoki boshqa harakatlar sodir etishni talab qilish yoki majburlash kabi holatlarda qo’llaniladi.

Shuningdek, Federal Qidiruv Byurosi ma’lumotlariga ko’ra, kiberjinoyat tovlamachilar korporativ veb-saytlar va tarmoqlarga tobora ko‘proq hujum qilmoqda, ularning ishlash qobiliyatiga putur yetkazmoqda va xizmatlarini tiklash uchun to‘lovlarni talab qilmoqda. Har oy FQBga 20 dan ortiq holatlar haqida xabar beriladi va jabrlanuvchining ismini jamoatchilikka oshkor qilmaslik uchun ko‘plari xabar qilinmaydi. Jinoyatchilar odatda tarqatilgan xizmatni rad etish hujumidan foydalanadilar[42].

Shuni ma’lumot tariqasida aytib o’tadigan bo’lsam, Ransomware — bu zararli dasturlarning bir turi bo’lib, fayl va boshqa shaxsiy ma’lumotlarga kirishni cheklash orqali,

[40] „BUFFETT: This is 'the number one problem with mankind'“
[41] https://xabar.uz/post/yigitning-shaxsiy-suratlarini-tarqatish-bilan-shantaj-qilgan
[42] Lepofsky, Ron. „Cyberextortion by Denial-of-Service Attack”.

to‘lov talab qilish va to’lov to’lanmasa, ma’lumotlarga kirishni doimiy ravishda qulflash yoki o‘chirib tashlash bilan tahdid qiladigan usul hisoblanadi. Shuningdek, Ransomware dunyodagi eng tez o‘sib borayotgan kiberjinoyatlardan biri bo‘lib qolmoqda. 2021-yilda Ransomware global zarari 20 milliard dollargacha tushishi taxmin qilinmoqda[43].

**Kiberterrorchilik –** bu internet orqali insonlarni qo’rqitish yoki tahdid qilish, aholi orasida vahima solish, turli saytlarda noto’g’ri ma’lumot tarqatish orqali tartibsizliklar keltirib chiqarish, odamlarning mol-mulki yoki hayoti va sog'lig'iga tahdid solish, siyosiy yoki mafkuraviy maqsadga erishish uchun amalga oshirilgan kiberjinoyat turlaridan biri hisoblanadi.

Bunday jinoyat turida kiberjinoyatchilar tomonidan viruslar yaratish va ularni internet orqali tarqatish, zararli dastur va apparatlar yaratish, shaxsiy ma’lumotlarni buzib kirish va ma’lumotlarni olish kabi vositalar orqali kiberterroristik harakatni amalga oshirishadi. Shuningdek, kiberterrorizmning bir necha asosiy va kichik holatlari yuz bergan. Al-Qoida tarafdorlari internetdan muloqot qilish va hatto yangi a’zolarni yollash uchun foydalangan[44].

Shuningdek, bunday jinoyatni amalga oshirishda turli usullardan foydalanish mumkin:

- Davlatga yoki harbiy sirlarga oid ma’lumotlarni buzib kirish;
- bank va shaxsiy ma'lumotlarga ruxsatsiz kirish;
- yashash yoki boshqa joylarda elektr ta'minoti tarmoqlarini uzib qo’yish;
- internetda va aholi orasida shovqinlarni keltirib chiqarish;
- aloqa vositalarini yo'q qilish va boshqalar.

Bunday holatlarni oldini olish uchun aholi orasida huquqiy ongni oshirish va kompyuter texnalogiyalardan to’g’ri foydalanish haqida tushuntirishlar olib borishimiz kerak. Chunki, aholining 70 – 80 foizi bugungi kunda kompyuter va telefondan ma’lumotlarni saqlash, jo’natish, muloqot qilish uchun foydalanib kelmoqda va bu albatta hamma uchun xavfsiz bo’lishi lozim.

Endigi navbatda, **behayo yoki haqoratomuz kontentlar** haqida so’z yuritadigan bo’lsam, hozirgi kunda ko’rishimiz mumkinki, har xil veb-saytlarda va turli joylarda odobga xilof, haqoratli, behayo video rolik yoki suratlarga ko’zimiz tushadi. Ushbu kontentlar turli davlatlar, shaharlar orasida qonuniymi yoki noqonuniylik yuzasidan turlicha farq qiladi. Shuningdek, internet pornografiyasi sohasida bolalarni jalb qilish keng tus olgan.

O’zbekiston Respublikasi Jinoyat kodeksining 130-moddasiga ko’ra: Pornografik mahsulotni tarqatish, reklama qilish, namoyish etish maqsadida tayyorlash yoki O‘zbekiston Respublikasi hududiga olib kirish, xuddi shuningdek pornografik mahsulotni reklama qilish, namoyish etish, tarqatish, shu jumladan ommaviy axborot vositalarida, telekommunikatsiya tarmoqlarida yoki Internet jahon axborot tarmog‘ida reklama qilish, namoyish etish, tarqatish, shunday harakatlar uchun ma’muriy jazo qo‘llanilganidan keyin sodir etilgan bo‘lsa bazaviy hisoblash miqdorining to‘rt yuz baravaridan olti yuz baravarigacha miqdorda jarima yoki uch yuz oltmish soatgacha majburiy jamoat ishlari yoxud uch yilgacha axloq tuzatish ishlari bilan jazolanadi.

[43] „Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021“
[44] Worth, Robert (25–iyun 2016–yil). „Terror on the Internet: The New Arena, The New Challenges“. New York Times Book Review. 21-bet.

Bolalar savdosi, bolalar fohishabozligi va bolalar pornografiyasi bilan bog'liq bolalar huquqlari to'g'risidagi Konvensiyaning ixtiyoriy protokoliga ko’ra, ushbu protokol ishtirokchilari, Bola huquqlari to'g'risidagi Konvensiyaning maqsadlariga erishish va uning qoidalarini, ayniqsa ishtirok etuvchi davlatlar bolani savdo amaliyotidan himoya qilish kafolatlarini ta'minlash uchun qabul qilishi kerak bo'lgan choralarga kengroq xarakter berish maqsadga muvofiq bo'ladi[45].

Bugungi kunda, bolalar pornografiyasi va bolalar savdosi keng avj olmoqda. Shuningdek, bir qator odobsiz bolalar guruhlari, shu jumladan balog’at yoshiga yetmagan qizlar fohishalik qilayotganini va jinsiy eksplutatsiya qilinganlarning orasida yosh qizlar sonining yuqori ekanligi odamni xavotirga solmoqda. Ijtimoiy tarmoqlarda voyaga yetmagan yosh yigit-qizlar pornografik videolari va pornografiyasi ko’payib ketishini oldini olish va unga qarshi kurashish bo’yicha 1999-yilgi Xalqaro Vena konferensiyasiga va butun dunyoda bolalar pornografiyasini ishlab chiqarish, tarqatish, saqlash va shu kabi holatlarni jinoiyat deb topishga chaquruvchi qarorga murojaat qildi.

1996-yil 27-31 avgust kunlari Butunjahon Kongressi bo’lib o’tgan. Bunda asosiy masala bola huquqlariga e’tibor qaratish, ya’ni bolalar o'z huquqlaridan foydalana oladigan muhit yaratish, hukumat, davlat hokimiyati organlari hamda ota-onalarni bola tarbiyasiga chuqur ahamiyat berishiga chaqirish, bola tarbiyasiga ahamiyat berish, bolalar pornografiyasi va fohishabozligi, jinsiy maqsadlarda voyaga yetmagan bolalar savdosiga qarshi kurashish, bolalarni jinsiy ekspluatatsiyadan himoya qilish bo'yicha turli masalalar keltirib o’tilgan. Shuningdek, Bolalar savdosi, bolalar fohishabozligi va bolalar pornografiyasi bilan bog'liq bolalar huquqlari to'g'risidagi Konvensiyaning ixtiyoriy protokolining 1-moddasida Ishtirokchi davlatlar ushbu protokolda nazarda tutilganidek, bolalar savdosi, bolalar fohishabozligi va bolalar pornografiyasini taqiqlaydi deya so’z yuritilgan[46].

Demak, ushbu protokol orqali, unga a’zo bo’lgan davlatlar bolalarning jinsiy jinoyatlarga, fohishabozlikka, bolalar pornografiyasini targ’ib qilmaslik va uni oldini olish uchun izchil ishlar olib borishishi kerak. Shuningdek, bularning barchasiga nafaqat davlat organlari va ularning joylardagi bo’linmalari balki bolalarning ota-onasi, o’qituvchisi, murabbiyi hamda boshqa shaxslar ham ogoh bo’lishi va nazorat qilishi shartdir.

Shuningdek, hozirgi rivojlangan asrda turli xildagi ekstremistik qarashlar, buzg'unchi yoshlar ongi ijtimoiy tarmoqlar va internet orqali rivojlanib kelmoqda. Shuni ta'kidlash kerakki, yuqorida keltirib o’tilgan kiberjinoyatlar sodir etilganlik uchun javobgarlik to'liq mukammal emas. Shuni bilamizki, Internet orqali sodir etilyotgan jinoiyatlar kundan-kunga ko’payib bormoqda. Demak, qonun chiqaruvchi buni hisobga olishi va Internetda sodir etilgan jinoyatlar jazosiz qolmasligi kerak. Shuningdek, huquqni tartibga solishda ushbu muammolarga yechim berilishi va qonunchilikda Internet orqali sodir etilgan jinoyatlar uchun bir qator o'zgartirishlar kiritilishi kerak.

Shuni ma’lumot tariqasida aytib o’tadigan bo’lsam, eng katta jinoyatlardan biri 2017-yilning may oyida xakerlar tomonidan sodir etilgan. Xakerlar, kompyuter ma’lumotlarini

[45] https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-sale-children-child

[46] Факультативный протокол к Конвенции о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии

shifrlaydigan va shifrni ochish uchun to'lov talab qiladigan wannacry Ransomware virusini ishga tushirishgan. Natijada, virus dunyoning 150 dan ortiq mamlakatlaridagi qurilma va gadjetlarga hujum qilgan. Shuningdek, 2007-yil aprel oyida Estoniyada kuchli kiberjinoyat sodir etildi va bu barcha davlat idoralarining ishini falaj qildi. Bundan ko’rish mumkinki, xar bir davlat ogoh bo’lishi va ichki tuzilmalarini mustahkam saqlashi lozim.

O'zbekiston Respublikasida mamlakat rahbarining izchil sa’y-harakati tufayli axborot-kommunikatsiya texnologiyalari keng joriy etilib, rivojlanishni boshladi. O'zbekistonda tijorat va notijorat tashkilotlar o'z veb-saytlari va avtomatlashtirilgan ma'lumotlar bazalarini, o’z platformasini va zamonaviy mobil texnologiyalarini joriy etishmoqda. Shuningdek, so'nggi yillarda O'zbekiston Respublikasi Qonunchilik tizimida bir qator normativ-huquqiy hujjatlarni qabul qilish harakatlari amalga oshirilmoqda. Unga muvofiq axborot-kommunikatsiya sohasi rivojlantirilib, takomillashtirila boshlandi va ularda axborot xavfsizligini ta'minlash masalalari ham ko'zda tutilgan. Unga misol keltiradigan bo’lsam: Jinoyat kodeksi O'zbekiston Respublikasining 2007-yil 25-dekabrdagi O’RQ-137-sonli "axborotlashtirish va ma'lumotlarni uzatish sohasida qonunga xilof harakatlar sodir etganlik uchun javobgarlik kuchaytirilganligi munosabati bilan O'zbekiston Respublikasining ayrim qonun hujjatlariga o'zgartish va qo'shimchalar kiritish to'g'risida" gi qonuniga muvofiq "axborot texnologiyalari sohasidagi jinoyatlar" 20-bob bilan to'ldirildi[47]. Unda kompyuter ma'lumotlariga qonuniy (ruxsatsiz) kirish emas, balki axborotlashtirish qoidalarini buzganlik uchun jazo choralari belgilangan.

2016-yilda O'zbekiston Respublikasi axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi hamda mamlakat huquqni muhofaza qilish organlari o'rtasida axborot makonida ruxsatsiz, noqonuniy yoki buzg'unchi harakatlarni amalga oshirishda foydalaniladigan huquqbuzarlarni tahlil qilish, aniqlash, usul va vositalar bo'yicha Nizom imzolandi va kuchga kirdi. Bu vazirlik hamda huquqni muhofaza qilish organlari o'rtasida samarali o'zaro ta'sir va ishni jadal ketishiga imkon berdi. O'zbekiston Respublikasi Bosh prokuraturasi huzurida kiberhujumlar va kiberjinoyatlarni oldini olish va to’xtatish maqsadida yangi bo'lim tashkil etildi. Uning vazifalaridan biri professional darajani oshirishdir.

Bugungi kunda, kiber jinoyatchilarning tajovuzlaridan himoya qilish davlatlar bilan birga xalqaro tashkilotlarning ham shaxsiy ishiga aylandi. Shunday xalqaro aktlardan biri bu - Kiberjinoyatlar to’g’risidagi konvensiya (Budapesht, 2001 yil 23-noyabr). U jahon hamjamiyatini kiberhujumlardan himoya qilish maqsadida qabul qilingan. U kiber jinoyatlar deb hisoblanadigan kompyuterlardan foydalangan holda quyidagi tadbirlarni nomlaydi: ma'lumotlarni ruxsatsiz ravishda o'g'irlash, kompyuter tizimlari buzish, noqonuniy qimor o'yinlari, mualliflik huquqining buzilishi, internetda taqiqlangan narsalarni ko’rish, tarqatish, bolalar pornografiyasini ta'qib qilish, saqlash va ishlab chiqarish.

**Qanday qilib kiber jinoyatchilardan himoyalanish kerak?**

Bugungi kunda kiberjinoyatlarning keng avj olib ketayotganini hisobga olgan holda, shaxsiy kopyuteringizni va ma’lumotlaringizni kiber hujumlardan himoya qilishingiz kerak.

[47] 2007-yil 25-dekabrdagi "axborotlashtirish va ma'lumotlarni uzatish sohasida qonunga xilof harakatlar sodir etganlik uchun javobgarlik kuchaytirilganligi munosabati bilan O'zbekiston Respublikasining ayrim qonun hujjatlariga o'zgartish va qo'shimchalar kiritish to'g'risida"gi O’RQ -137-sonli qonuni // O'zbekiston Respublikasi qonunchiligining Milliy ma'lumotlar bazasi. URL: https://lex.uz/ru/docs/1295264

Chunki, kiberjinoyatchilar o’z maqsadlariga erishishda asosan kompyuterlarga zararli virus va dasturlarni, noqonuniy ma’lumotlarni yoki rasmlarni tarqatib yuborish orqali tahdidlar uyushtirishlari mumkin. Shuningdek, kiberjinoyatchilar ko'pincha ikki ishni birdaniga bajarish orqali zarar keltirishadi. Ular avval kompyuterlarga viruslar tarqatishadi va kompyuterni ishdan chiqarib ma’lumot o’g’irlashni boshlashadi.

Birinchi navbatda ushbu holatlarni bartaraf qilish va kiberhujumlarni oldini olish uchun yuqumli viruslarni kompyuter tarmog’iga kirishiga yo’l qo’ymasligingiz kerak. Kompyuterlarni shunday jinoyat va hujumlardan himoya qilish usullarini keltirib o’tadigan bo’lsam:

- Kompyuterlarni himoya qilish uchun eng so'nggi xavfsizlik dasturlaridan foydalanish va ularni tez-tez yangilab turish;
- Internet xavfsizligini ta'minlashda antiviruslardan foydalanish;
- Topish qiyin bo'lgan parollardan foydalanish va uni kompyuterning ichiga yozib qo’ymaslik;
- Notanish veb-saytlarda zararli havolalarga bosmaslik va kirmaslik;
- Telefon aloqasi yoki elektron pochta himoyalanganligiga ishonch bo'lmasa, shaxsiy ma'lumotlarni telefon yoki boshqa vositalar orqali jo’natmaslik.

Yuqoridagilardan kelib chiqqan holda, kiberjinoyatchilik bugungi jamiyat va insoniyat tinchligiga haqiqiy tahdid solishi mumkin bo’lgan davrda yashamoqdamiz. Shuning uchun yuqorida keltirib o’tilgan fikrlar va misollardan tashqari, har bir inson fan va texnika yutuqlaridan doimiy xabardor bo’lib yurishi lozim. Shuningdek, davlat organlari va tashkilotlariga ham ishga olishda kompyuter texnologiyalari va dasturlash ko’nikmalariga ega bo’lgan kadrlarni tayyorlash va ishga olish zarur.

Shuni takidlash joizki, O’zbekiston Respublikasi va undagi fuqarolar huquqiy ongi va ma’daniyatini oshirishda ommaviy axborot vositalari orqali, maktab, kollej, universitetdagi dars mashg’ulotlari orqali, turli xil tadbirlar va konferensiyalar orqali to’g’ri shakllantirish va rivojlantirish kerak. Shuningdek, yurtimizda kiberjinoyatga qarshi kurashuvchi davlat organlariga kerakli kadrlarni qabul qilish va tayyorlash lozim. Chunki, mamlakatimizni qonuniy himoya qilish, ichki va tashqi kiberxavfsizligi, kiberjinoyatlarni oldini olish va unga barham berish, ushbu sohani takomillashtirish va amaliyotda to’g’ri qo’llash kabi vazifalar ular qo’lidadir.

Shuningdek, kiberjinoyatning turli ko’rinishlarini aniqlash, ya’ni kiber tovlamachilik va firibgarlik, kiberterrorizm, behayo yoki haqoratomuz kontent yaratish va tarqatish kabi jinoyatlarni aniqlash bo’yicha ishlar olib borish, kiberjinoyatchilarni ushlash va ularni tergov qilish hamda eng asosiysi fuqarolar hayotiga tahdid soluvchi holatlarni bartaraf qilish lozim.

## FOYDALANILGAN ADABIYOTLAR RO’YXATI:

1. Banki lovyat doljnikov cherez „Odnoklassnikov“, „V kontakte“ i „Moy krug“ // NEWSru.com
2. „Россия в социальных сетях: какой ущерб от виртуальной жизни?“. ТАСС.
3. Ефимов, Кузнецов 2011
4. https://darakchi.uz/oz/24470
5. O’zbekiston Respublikasi Jinoyat kodeksi

6. „Треть пропагандирующих суицид интернет-страниц пришлась на «ВКонтакте»“. Lenta.ru
7. Putin podpisal zakon ob ugolovnoy otvetstvennosti za sozdanie „grupp smerti“ // Интерфакс, 07.06. 2017
8. „Pavel Durov“. DLD Conference
9. „BUFFETT: This is 'the number one problem with mankind'“
10. https://xabar.uz/post/yigitning-shaxsiy-suratlarini-tarqatish-bilan-shantaj-qilgan
11. Lepofsky, Ron. „Cyberextortion by Denial-of-Service Attack”.
12. „Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021“
13. Worth, Robert (25–iyun 2016–yil). „Terror on the Internet: The New Arena, The New Challenges“. New York Times Book Review. 21-bet.
14. https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-sale-children-child
15. Факультативный протокол к Конвенции о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии
16. 2007-yil 25-dekabrdagi "axborotlashtirish va ma'lumotlarni uzatish sohasida qonunga xilof harakatlar sodir etganlik uchun javobgarlik kuchaytirilganligi munosabati bilan O'zbekiston Respublikasining ayrim qonun hujjatlariga o'zgartish va qo'shimchalar kiritish to'g'risida"gi O’RQ -137-sonli qonuni // O'zbekiston Respublikasi qonunchiligining Milliy ma'lumotlar bazasi. URL: https://lex.uz/ru/docs/1295264
17. Авчаров И. В. Борьба с киберпреступностью // Информатизация и информационная безопасность правоохранительных органов. Материалы XI межд. конф. М., 2012. С. 191–194.
18. Зверева Е. Б. Киберпреступность как угроза безопасности современного общества: виды, особенности, методы борьбы и профилактики // Молодой ученый. 2020. № 10 (300). С. 35–37.