



KIBERJINOYATCHILIK TUSHUNCHASI, TURLARI VA UNGA QARSHI KURASHISHNING HUQUQIY CHORRALARI

Otajonov Abrorjon Anvarovich

Toshkent Davlat Yuridik Universiteti

*Jinoyat huquqi, kriminalologiya va korrupsiyaga qarshi kurashish
kafedrasi professori*

Nazarov Shamshod O'ktam O'g'li

Toshkent Davlat Transport Universiteti

Iqtisodiyot fakulteti, Yurisprudensiya yo'nalishi 4-kurs talabasi

ANNOTASSIYA: Ushbu maqolada kiberjinoyatlar va uning turlari kabi zamonaviy global xavfsizlik muammolarini chuqur o'rganishga qaratilgan. Kiberjinoyatchilikka qarshi kurashda xalqaro hamkorlik va xorijiy davlatlar tajribasi, kiberjinoyatchilik uchun javobgarlik masalalari Unda Budapesht konvensiyasi kabi xalqaro huquqiy mexanizmlarining ahamiyati va ularning global kiberxavfsizlikni ta'minlashdagi roli keng yoritilgan. Shuningdek, ushbu maqolada AQSH, Yevropa Ittifoqi, Xitoy, Hindiston va boshqa davlatlarning milliy qonunchilik tizimlari qiyosiy tahlil qilinib, ularning kiberjinoyatlarga qarshi kurashda qo'llangan strategiyalarni ko'rib chiqilgan.

Kalit so'zlar: jinoyat huquqi, axborotlashtirish obyekti, xalqaro hamkorlik va xorijiy davlatlar tajribasi, kiberjinoyatchilik va kiberxavfsizlik hodisasi, xalqaro standartlar, amalga oshirish, jinoyat.

АННОТАЦИЯ: Это помогает глубоко изучить современные глобальные проблемы, такие как киберпреступность и ее виды в Узбекистане. Международные вопросы безопасности в борьбе с киберпреступностью, проблемы безопасности в контексте киберпреступности. В документе подробно рассматривается значение Будапештской конвенции как международно-правового механизма и роль глобального правосудия в



обеспечении кибербезопасности. Проводится сравнительный анализ национальных правовых систем США, Европейского союза, Китая, Индии и других стран, а также рассматриваются стратегии, используемые в борьбе с киберпреступностью.

Ключевые слова: уголовное право, объект информатизации, международное сотрудничество и опыт зарубежных стран, явление киберпреступности и кибербезопасности, международные стандарты, имплементация, преступление.

ABSTRACT: This article aims to provide an in-depth study of modern global security problems such as cybercrime and its types. International cooperation and the experience of foreign states in combating cybercrime, issues of liability for cybercrime. It extensively covers the importance of international legal mechanisms such as the Budapest Convention and their role in ensuring global cybersecurity. Also, this article provides a comparative analysis of the national legislative systems of the USA, the European Union, China, India and other countries, and examines the strategies used in combating cybercrime.

Keywords: criminal law, object of informatization, international cooperation and experience of foreign countries, cybercrime and cybersecurity phenomenon, international standards, implementation, crime.

Kirish: Ma'lumki, zamonaviy dunyoni turli texnologiyalarsiz tasavvur qilib bo'lmaydi. So'ngi yillarda internet va insoniyatning axborot texnologiyalari sohalaridagi ixtirolari natijasida axborot makonidan foydalanuvchilar soni kundan kunga ortib bormoqda, o'z navbatida, uning ta'siri ham doimiy ravishda kengaymoqda. Natijada butun insoniyat singari jinoyat olami ham rivojlanib, axborot texnologiyalari sohasini mukammal o'rgangan ba'zi shaxs yoki guruhlar jinoyat sodir etishning yangi texnologiyalarini o'zlashtirmoqdalar. Axborot makonini o'zlashtirish texnologiyasining paydo bo'lishi bilan jinoyatning yangi turi



Kiberjinoyat yuzaga keladi. Dunyo miqyosida kiberjinoyatlarning tarqalishi shaxdam qadamlar bilan kundan kunga rivojlanib bormoqda. Shu munosabat bilan kiberjinoyatchilik muammosini tushunish masalalari zamonaviy jamiyatda juda muhim. Kiberjinoyatlar har bir davrda axborot-kommunikatsiya

Texnologiyalarining rivoji tufayli turlicha doktrinal va rasmiy ta'riflarga ega. Xususan, Yevropa Kengashining 2001-yildagi "Kompyuter jinoyatlari to'g'risida"gi konvensiyasiga ko'ra, "kiberjinoyat kibermuhitda sodir etiladigan har qanday jinoyatdir"[1].

Darhaqiqat, texnologiya istalgancha rivojlanishi mumkin, biroq sodir etiladigan qilmishlarning barchasi kibermuhitda sodir etiladi. Barcha texnologiyalar ishtiroki bo'lgan ijtimoiy xavfli qilmishlar bajariladigan jarayonlarni qamrab oluvchi muhit esa kibermuhitga kiradi. Kiberjinoyatlar kibermuhitda sodir etiladigan jinoyat hisoblanadi. Misol uchun, kiberog'rilik sodir qilishdan oldin kiberjinoyatchi jabrlanuvchining pul mablag'lari saqlanayotgan kartasi paroliga ega bo'ladi hamda telekommunikatsiya yoki Internet tarmog'i yohud boshqa tarmoqdan foydalanib, o'z qilmishini sodir etadi. Kiber muhitda – aynan mana shu jarayondagi muhitni ko'z bilan ko'rolmaymiz, qo'l bilan ushlay olmaymiz, ammo jinoyatchi jabrlanuvchining kartasidagi kodni terib, qanday qilib ushbu mablag'larga ega bo'lishini bilmay qolamiz. Shuni aytib o'tish kerakki, kibermuhit yoki kibermakon tushunchalari birinchi marta 1982-yilda kanadalik fantastik yozuvchi U.Gibsonning "Burning Chrome" novellasida ishlatilgan bo'lib, ushbu tushuncha "Neuromancer" romani orqali ommalashib ketganini[2] ham aytib o'tish joiz. Tadqiqot natijalariga ko'ra, olimlar "kiberjinoyat" – kompyuter tizimlari yoki kompyuter tarmoqlari, shuningdek, kibermakonga kirishishning boshqa vositalari yordamida yoki ular orqali kibermakonda, kompyuter tizimlari yoki tarmoqlari vositalari doirasida hamda kompyuter tizimlariga, kompyuter tarmoqlariga qarshi sodir etilgan har qanday jinoyatlar majmuidir[3]. Shuningdek



Rossiyaning boshqa bir guruh olimlari, ya'ni T.N. Sharipova va A.A. Sidorenko o'z nazariyasida "kiberjinoyat" atamasi "kompyuter tizimi yoki tarmog'i yordamida, kompyuter tizimi yoki tarmog'i doirasida, kompyuter tizimi yoki tarmog'iga qarshi sodir etilishi mumkin bo'lgan har qanday jinoyatni" birlashtirgan deb hisoblaydilar. Ushbu yondashuv vakillari tomonidan berilgan ta'rif kengroq harakatlar doirasini o'z ichiga oladi va zamonaviylik talablariga yaxshiroq javob beradi.

Kiberjinoyat turlari: kiberjinoyatlar soni juda ko'p bo'lgani sababli ularni tasniflash va ma'lum bir guruhlarga ajratib o'rganish maqsadga muvofiq. Biroq kiberjinoyatlarning turini har kim turlicha tasniflaydi, xususan, Kasperskiy kompanyasi ularni elektron pochta va internet fribgarligi, shaxsiy ma'lumotlar fribgarligi (shaxsiy ma'lumotlarni o'g'rilanishi va noto'g'ri ishlatilishi), moliyaviy ma'lumot yoki bank kartasi ma'lumotlarini o'g'rilash, korporativ ma'lumotlarni o'g'rilash va sotish, kibertovlamachilik, kriptojecking, kiberjosuslik kabi turlari borligini inobatga olib ularni ikkita guruhga – kompyuterlarning o'ziga qaratilgan kiberjinoyatlar va kompyuterdan foydalanilgan holda amalga oshiriladigan kiberjinoyatlarga ajratadi[4]. "Tadviser" kompaniyasining fikricha, "kiberjinoyatlar spam, maqsadli fishing, pdf-hujum, qidiruv tizimini optimallashtirishni zararlash, ishlash qobiliyatini yo'qotish kabi turlarga ega.[5]. "IT Skills" loyihasi boshlig'i A. Sevostyanov hamda mualliflari – M. Ryabuxin va R. Tuychinning fikriga ko'ra, "kiberjinoyatlarning moliyaviy yo'naltirilgan kiberjinoyatlar, shaxsiy hayot bilan bog'liq kiberjinoyatlar, mualiflik huquqini buzish bilan bog'liq kiberjinoyatlar, ijtimoiy va siyosiy asoslangan kiberjinoyatlar, spam, o'zaro nafrat qo'zg'atish bilan bog'liq kiberjinoyatlar, terorizm, kiberbulling, noqonuniy xatti – harakatlar bilan bog'liq kiberjinoyatlar, noqonuniy pornografiya, gruming, giyohvandlik vositalari va qurol – yarog'larni tarqatish bilan bog'liq kiberjinoyatlar kabi turlari bo'lishi mumkin, bunda fishing,



kibertovlamachilik, moliyaviy fribgarlik kiberjinoyatlari moliyaviy yo'naltirilgan kiberjinoyatlar hisoblanadi[6].

Xorijiy mamlakatlarda Filippinda kiberjinoyatlarga qarshi kurashish va ularni turlarga ajratish, tasniflash juda ajoyib tartibga solingan. Unga ko'ra, 2012 – yilda qabul qilingan “Kiberjinoyatlarni oldini olish to'g'risida”gi 10175-son Flippin Respublikasi qonuni (RA101075) va u asosida qayta ko'rib chiqilgan Flippin Jinoyat kodeksiga asosan “Istalgan qilmish, agarda axborot-kommunikatsiya texnologiyalari orqali oshirilgan bo'lsa, bu kiberjinoyat deb hisoblanadi hamda mzkur jinoyatni sodir etgan shaxslarga filippin jinoyat kodeksida nazarda tutilgan sanksiyalardagi jazo miqdoridan bir darajaga ko'p bo'lgan jazo qo'llaniladi”[7]. Birlashgan Millatlar Tashkilotining giyohvand moddalar vajinoyatchilik bo'yicha boshqarmasi va seriya modul universitetidagilarning fikricha, “Kiberjinoyatlarni kompyuter ma'lumotlari yoki tizimlarining konfidensiallig, yaxlitligi va mavjudligiga qarshi jinoyatlar, kompyuter bilan bog'liq kiberjinoyatlar, komputer fribgarlik va qalbakillashtirish, shaxsiy ma'lumotlar va spamlardan foydalanish bilan bog'liq kompyuter jinoyatlari, shaxsiy zarar uchun kompyuterdan foydalanish bilan bog'liq kiberjinoyatlar, kompyuter axboroti bilan bog'liq kiberjinoyatlardir”[8]. Kiberjinoyatlarni tasniflash borasida ham olimlarning fikrlari turlicha, xususan T.L.Tropina “Kiberjinoyatlar ma'lumotlar maxfiyligini buzish, kompyuter va kompyuter tarmoqlariga ruxsatsiz kirish, tijorat siri bo'lgan ma'lumotlarning maxfiyligini buzish, kompyuter fitnasi (ishlashga xalaqit berish, ma'lumotlarni o'zgartirish, yo'q qilish va h. k.), iqtisodiy kiberhujumlar xususan, kompyuter fribgarligi kabi turlarga bo'linadi, deya qayd etadi[9]. Jinoyat faoliyatidan olingan daromadlarni legallashtirishga va terrorizmni moliyalishtirishga qarshi kurashish bo'yicha Yevrosiyo guruhining fikricha, “Kiberjinoyatlar internetdagi fribgarliklar, xususan tarmoqda “moliyaviy piramidalar” yaratish, internet orqali yoki onlayn auksionlar savdosidagi fribgarliklar, moliyaviy, tijorat yoki shaxsiy ma'lumotlarni o'g'rilash uchun dasturiy vositalarni yaratish



bo'yicha faoliyat soxta veb-saytlarni yaratish, kompyuter viruslari va troyan dasturlarining tarqalishi, trafikka to'sqinlik qilish va boshqalar, masofaviy bank xizmatiga oid fribgarliklar, yo'qotilgan o'g'rilangan, soxta karta to'lovlaridan foydalanish bilan bog'liq kiberjinoyatlar, "klonlash"ga oid texnik vositalardan foydalanilgan holda bank kartalardagi to'lov ma'lumotlarni o'g'rilash, bankomatlardan naqd pullarni olish uchun "oq plastik" – soxta plastik kartadan foydalanish, tranzaksiyani bekor qilish fribgarligi, naqd pul olish kabi jinoyatlarga bo'linadi"[10]. Kompyuter jinoyatlari to'g'risidagi Budapesht konvensiyasiga asosan, Internet va boshqa kompyuter tarmoqlari orqali sodir etilgan jinoyatlar, mualliflik huquqlarining buzilishi, kompyuter fribgarligi, bolalar pornografiyasi va tarmoq xafvsizligini buzish bilan bog'liq jinoyatlar kiberjioyatlarga qarshi kurashish bo'yicha birinchi xalqaro shartnoma hisoblanadi[11]. Kiberjinoyatlar amalga oshirish usuliga ko'ra, ikkita katta guruhga bo'linadi, ya'ni kibertexnologiyalardan foydalanib sodir etiladigan kiberjinoyatlar va kibertexnologiyalarga qarshi qaratilgan kiberjinoyatlar. Buni aniqroq tushuntiradigan bo'lsak, kiberjinoyatlar axborot – kommunikatsiya texnologiyalardan foydalanib sodir etiladigan kiberjinoyatlarga va axborot kommunikatsiya texnologiyalarga nisbatan sodir etiladigan jinoyatlarga bo'linadi.

Jinoyat kodeksi bo'yicha tartibga solish, jinoyat kodeksining

103 – moddasi ikkinichi qismi "g"-bandi, 103¹-moddasining ikkinchi qismi "v"-bandi, 139-moddaning ikkinchi qismi, 140-moddaning ikkinchi qismi, 167-moddasining uchinchi qismi "g" bandi, 168-moddaning uchinchi qismi "g" bandi, 169-moddasining uchinchi qismi "b" bandi, 188¹-,244¹-modda uchinchi qism "g" bandi, 244⁶-moddasi, 278-moddaning to'rtinchi qismlarida nazarda tutilgan ijtimoiy xavfli qilmishlar axborot-kommunikatsiya texnologiyalardan foydalanib, Jinoyat kodeksining 278¹-278⁷-moddalarida nazarda tutilgan ijtimoiy xavfli qilmishlar axborot-kommunikatsiya texnologiyalarga nisbatan sodir etilgan kiberjinoyatlar sanaladi.



Kibertexnologiyalar orqali shaxsning hayot daxlsizligini buzish jinoyati O'zbekiston Respublikasi Konstitutsiyasining 27-moddasida belgilangan norma – har kim erkinlik va shaxsiy daxlsizlik huquqiga egaligiga ziddir. O'zbekiston Respublikasi Jinoyat kodeksida kompyuter texnologiyasidan foydalanib sodir etiladigan qator jinoyatlar uchun ham javobgarlik belgilangan.

1) Kompyuter vositasidan foydalanib, oilaga, yoshlarga, axloqqa qarshi qaratilgan jinoyatlar

2) Kompyuter vositasidan foydalanib, shaxsning ozodligi, sha'ni va qadr – qimmatiga qarshi qaratilgan jinoyatlar

3) Kompyuter vositasidan foydalanib, fuqarolarning konstitutsiyaviy huquq va erkinliklariga qarshi qaratilgan jinoyatlar

4) Kompyuter vositasidan foydalanib, O'zbekiston Respublikasiga qarshi qaratilgan jinoyatlar

5) Kompyuter vositasidan foydalanib, o'zgalar mulkini talon – toroj qilish jinoyatlari

6) Kompyuter vositasidan foydalanib, tinchlik va insoniyat xavfsizligiga qarshi qaratilgan jinoyatlar.

7) Kompyuter vositasidan foydalanib, iqtisodiyot asoslariga qarshi qaratilgan jinoyatlar

8) Kompyuter vositasidan foydalanib, xo'jalik faoliyat sohasidagi jinoyatlar

9) Kompyuter vositasidan foydalanib, boshqaruv tartibiga qarshi qaratilgan jinoyatlar

10) Kompyuter vositasidan foydalanib, odil sudlovga qarshi jinoyatlar

11) Kompyuter vositasidan foydalanib, jamoat xavfsizligi va jamoat tartibiga qarshi jinoyatlar

Axborot texnologiyalari sohasidagi jinoyatlar: Axborotlashtirish qoidalarini buzish, ya'ni belgilangan himoya choralarini ko'rmagan holda axborot tizimlari ma'lumotlar bazalari va banklarini, axborotga ishlov berish



hamda uni uzatish tizimlarini yaratish, joriy etish va ulardan foydalanish hamda axborot tizimlaridan ruxsat bilan foydalanish fuqarolarning huquqlariga yoki qonun bilan qo'riqlanadigan manfaatlariga yoxud davlat yoki jamoat manfaatlariga ko'p miqdorda zarar yoxud jiddiy ziyon yetkazish; kompyuter axborotidan, ya'ni axborot – hisoblash tizimlari, tarmoqlari va ularning tarkibiy qismlaridagi axborotlardan qonunga xilof ravishda ruxsatsiz foydalanish, agar ushbu harakat axborotning yo'q qilib yuborilishi, to'sib qo'yilishi, agar ushbu harakat axborotning yo'q qilib yuborilishi, to'sib qo'yilishi, modifikatsiyalashtirishi, undan nusxa ko'chirilishi yoxud unga qo'lga kritilishiga, elektron hisoblash mashinalari tizimi yoki ularning tarmoqlari ishining buzilishi; himoyalangan kompyuter tizimida, shuningdek, telekommunikatsiya tarmoqlaridan qonunga xilov ravishda ruxsatsiz foydalanish uchun maxsus dasturiy yoki apparat vositalarini o'tkazish maqsadini ko'zlab tayyorlash yoxud o'tkazish va tarqatish; kompyuter axborotni 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 mafaatlarga yoxud davlat yoki jamoat mafaatlarga yoxud jiddiy ziyon yetkazish.

- 1) Virusli dasturiy ta'minotni tarqatish;
- 2) Foydalanuvchilarning maxfiy ma'lumotlarini o'g'rilash
- 3) Ijtimoiy tarmoqlarda boshqalarning akkauntini buzish
- 4) Yolg'on ma'lumot tarqatish, tuhmat qilish
- 5) Bank plastik kartalari (karta rekivizitlari) bilan noqonuniy operatsiyalar
- 6) Qimmatli qog'ozlar bozoridagi internet-fribgarlik
- 7) Internetdagi moliyaviy piramidalar
- 8) Mobil aloqaa bilan bog'liq jinoyatlar
- 9) Elektron tijorat sohasidagi boshqa jinoyatlar



O‘zbekiston Respublikasining 2022-yil 15-aprelda “Kiberxavfsizlik to‘g‘risida”gi O‘RQ – 764 sonli Qonuni 2-bobida kiberxavfsizlik sohasi davlat tomonidan tartibga solinishiga doir masalalar berib o‘tilgan. Qonunning 11-moddasida O‘zbekiston Respublikasi Davlat xavfsizlik sohasidagi vakolatli davlat organi ekani qayd etilgan. Vakolatli davlat organing kiberxavfsizlik sohasidagi vakolatlari jumlasiga quyidahilar kiradi.

1) Kiberxavfsizlik sohasidagi normativ-huquqiy hujjatlarni va davlat dasturlarini ishlab chiqish

2) Kiberxavfsizlik to‘g‘risidagi qonunchilik hujjatlarining ijro etilishi ustidan nazoratni amalga oshirish

3) Kiberxavfsizlik hodisalari yuzasidan tezkor-qidiruv tadbirlarini, tergovga qadar tekshiruvlarni va tergov harakatlarini amalga oshirish

4) Kiberxavfsizlik hodisalarining oldini olish, ularni aniqlash va bartaraf etish hamda ularga nisbatan tegishli chora-tadbirlarni, shu jumladan, ularning oqibatlarini tugatish bo‘yicha tashkiliy-texnik chora-tadbirlarni ko‘rish

5) Favqulodda vaziyatlarda axborot tizimlari va resurslarini kiberhimoya qilish hamda kiberxavfsizlik sohasidagi boshqa masalalar bo‘yicha chora-tadbirlarni o‘z ichiga olgan rejalarni ishlab chiqish

6) Kiberxavfsizlikni ta‘minlashga doir ishlarni, shuningdek muhim axborot infratuzilmasi obyektlarida kiberhujumlarining oldini olishga, ularni aniqlashga va ularning oqibatlarini tugatishga doir ishlarni tashkil etish

7) Axborot tizimlaridan hamda resurslaridan foydalanuvchilarning huquqlari va qonuniy manfaatlarini himoya qilish choralarini ko‘rish

Xulosa va Takliflar:

Xulosa “Xalqaro statistik ma’lumotlarga ko‘ra, kiberjinoyatlarning qariyb 50 foizi AQShga qaratilgan bo‘lib, eng ko‘p zarar moliya va bank sektorida (40% gacha) kuzatiladi. Bu holat kiberjinoyatchilikning raqamlashtirish va moliyaviy resurslar yuqori bo‘lgan hududlarda jamlanishini ko‘rsatadi.” qiladigan bo‘lsak, internet foydalanuvchilari uchun ularga nisbatan



sodir etilishi mumkin bo'lgan noqonuniy huquqbuzarliklarning oldini olish bo'yicha quyidagi tavsiyalarni beramiz:

Internetga kirish, zararli faoliyatga qarshi kurashish uchun mo'ljallangan maxsus dasturiy ta'minotga ega qurilmalardan foydalaning, ularni o'z vaqtida yangilang. Saytlardan foydalanganda ularning tashqi ko'rinishiga, veb-manziliga e'tibor bering, ehtimol, uning soxta nusxasiga kirgandirsiz; o'zlarini bank xodimi deb tanishtirgan va bank kartangiz ma'lumotlarini berishingizni so'ragan notanish odamlar bilan hech qachon telefonda gaplashmang. Internet orqali to'lovlarni amalga oshirishda, iloji bo'lsa, "Visa" va "MasterCard" xalqaro to'lov tizimlari uchun "3D Secure" kabi to'lovlarining qo'shimcha xavfsizligini ta'minlash texnologiyalaridan foydalaning.

Kibermaydondagi jinoyatlardan himoyalaniishning yana bir yo'li zamonaviy tahdidlardan xabardor bo'lish hamda xakerlarning tuzog'iga tushib qolmaslik uchun ijtimoiy tarmoqlardagi yolg'on xabarlariga ishonib qolmaslikdir. Shuni ham aytish lozimki, qonunni bilmaslik javobgarlikdan saqlab qolmaydi, kiberjinoyatchilar uchun jazo muqarrardir.

Taklif

1 "Bir bosishda bloklash" tizimi (FAST BLOCK)

Agar fuqaro: bankka, yoki 102/ maxsus Telegram-botga murojaat qilsa 30 daqiqa ichida, bir bosishda esa karta, hisob, shubhali tranzaksiya avtomatik muzlatiladi, pulni chiqarib ketishga ulgurmaydi. "O'zbekistonda kiberjinoyatlar natijasida fuqarolar yiliga yuzlab milliard so'm zarar ko'rmoqda. Muammoni hal etish uchun asosiy e'tibor jazolashga emas, balki tranzaksiyalarni real vaqt rejimida aniqlash va zudlik bilan bloklashga qaratilgan huquqiy mexanizmni joriy etish zarur."

2 "Budapesht konvensiyasi kiberjinoyatlarga qarshi kurashda jinoyatlarni yagona standart asosida belgilash, elektron dalillarni tezkor saqlash va davlatlar o'rtasida 24/7 hamkorlikni yo'lga qo'yish modelini joriy etgan."



“Budapesht konvensiyasi talablari asosida milliy qonunchilikni takomillashtirish O‘zbekistonda kiberjinoyatlarni erta aniqlash, fuqarolarning moliyaviy zararini kamaytirish va transchegaraviy jinoyatlarga samarali qarshi kurashish imkonini beradi.”

REFERENCES

- 1 2001-yil 23-noyabrdagi Yevropa ittifoqining “Kiberjinoyatchilik to‘g‘risidagi” konventsiyalar Budapesht, 185-sonli Yevropa shartnomalari seriyasi: <https://rm.int/1680081580>.
- 2 Abduljalilov A. Internetda fuqarolik huquqiy munosabatlarning nazariy muammolari. Yuridik doktori dissertatsiyasi. Dushanbe 2015. <https://lawbook.online>.
- 3 ITU Toolkit For Cybercrime Legislation. ITU,2017.
- 4 Tahdidlar haqida/ <https://www.kaspersky.ru/resouce-center/threats/what-is-cybeercrime>.
- 5 Dunyodagi kiberjinoyatchilik.2020. <http://www.tadviser.ru>.
- 6 <https://sys-team-admin.ru/stati/bezaposnost/170-kiberprestupnost-ponyatie-vidy-i-metody-zashchity.html>.
- 7 kiberjinoyatchilikni belgilovchi, uning oldini olish,tergov qilish, jinoiy javobgarlikka tortish va jazolashni hamda boshqa maqsadlarni nazarda tutuvchi qonun. 10175-sonli Respublika qonuni. 2012-yil 12-sentabr, <https://www.officalgazeta.gov.ph/2012/09/12/respublic-act-no10175/>.
- 8 Adolat uchun ta’lim universiteti modullar seriyasi. Kiberjinoyatchilik. 2-modul. Kiberjinoyatchilikning umumiy turlari. Birlashgan Millatlar Tashkilotining Giyohvand moddalar va jinoyatchilik bo‘yicha boshqarmasi.Vena.2019.39-42-betlar <http://www.unodc.org/documens/e/4j/Cybercrime/Cybercrime,2-modul> Kiberjinoyatchilikning umumiy turlari RU.pdf.
- 9 Tropina T.L. Kiberjinoyatchilik: tushunchasi,holati va unga qarshi kurashishning huquqiy chorralari. Rossiya Federatsiyasi Oliy Attestatsiya



Komissiyasi ma'lumotlariga ko'ra dissertatsiya va referat mavzusi. 12.00.08.

Yuridik dissertatsiyasining referati. Vladivostok.2005.10 va 17 betlar.

10 Jinoiy daromadlarni legallashtirish va terrorizmni moliyalashtirishga qarshi bo'yicha Yevrosiyo guruhi. Kiberjinoiyatchilik va jinoiy daromadlarni legallashtirish.2014.-13-14betlar.

11 Budapesht konvensiyasi.2001-yil.<https://www.coe.int>.

12 O'zbekiston Respublikasi Konstitutsiyasi. <https://lex.uz/docs/20596>

13 O'zbekiston Respublikasi Jinoyat kodeksi. <https://lex.uz/docs/111453>

14 O'zbekiston Respublikasi "Kiberxavfsizlik to'g'risida"gi qonun. 2022-yil 15-aprel. <https://lex.uz/uz/docs/5960604>

15 O'zbekiston Respublikasi "Axborotlashtirish to'g'risida"gi qonuni. 2003-yil 11-dekabr. <https://lex.uz/docs/83472>