

KIBERXAVFSIZLIK HODISALARGA JAVOB BERISHDA HUQUQIY VA AXLOQIY MASALALAR

Abdullayev Abdulaziz Abdurasul o'g'li

Toshkent davlat yuridik universiteti

Xalqaro huquq va qiyosiy huquqshunoslik fakulteti

4-kurs talabasi

abdullayevabdulaziz989@gmail.com

Annotatsiya: Mazkur maqolada raqamli texnologiyalarning jadallik bilan rivojlanishi va internet tarmog'ining kengayib borishi natijasida dolzarb ahamiyat kasb etayotgan kiberxavfsizlik hodisalariga javob berishdagi huquqiy va axloqiy masalalar tahlil qilingan. Bugungi kunda axborot texnologiyalari jamiyatning iqtisodiy va ijtimoiy hayotining ajralmas qismiga aylangani sababli, kiberxavfsizlikni ta'minlash masalasi global miqyosda muhim ahamiyat kasb etmoqda.

Maqolada kiberxavfsizlikka oid huquqiy me'yorlar va axloqiy tamoyillar, xalqaro tashkilotlarning (BMT, OECD, Yevropa Ittifoqi va boshqalar, MDH) bu boradagi roli, shuningdek, milliy qonunchilik doirasida amalga oshirilayotgan chora-tadbirlar ko'rib chiqilgan. Kiberjinoyatlarga qarshi kurashishda xalqaro hamkorlik, axborot almashinuvi va inson huquqlarini himoya qilish masalalariga alohida e'tibor qaratilgan.

Shuningdek, maqolada shaxsiy ma'lumotlarning o'g'irlanishi, ularni noto'g'ri ishlatish yoki tarqatish kabi holatlarga javob berishda axloqiy yondashuvlarning o'rni yoritilgan. Huquqiy va axloqiy muammolarni tahlil qilish asosida maqolada tegishli tavsifalar ishlab chiqilgan.

Kalit so'zlar: *Kiberxavfsizlik, kiber huquq, axloqiy masalalar, huquqiy me'yorlar, shaxsiy ma'lumotlar, axborot xavfsizligi, kiberjinoyatlar, xalqaro hamkorlik, raqamli texnologiyalar, internet huquqi, axborot erkinligi, kiberhujumlar, xalqaro tashkilotlar, ma'lumotlarni himoya qilish, axloqiy tamoyillar.*

KIRISH

Bugungi kunda texnologiyaning rivojlanishi, internetning keng tarqalishi va raqamli texnologiyalarni yanada faol qo'llash kiberxavfsizlikni global miqyosda muhim va dolzarb masalaga aylantirdi.

Ayni damda internet va raqamli texnologiyalar jamiyatning iqtisodiy jarayonlarida ajralmas qismga aylanishga ulgurdi, shu sababli, ularning xavfsizligini ta'minlash hamda foydalanuvchilarning ma'lumotlarini himoya qilish alohida e'tibor qaratish lozim. Kiberxavfsizlik, ayniqsa, davlatlar, tashkilotlar va shaxslar uchun keng qamrovli va ko'p qirrali masala bo'lib, uning shakllanishi va rivojlanishi xalqaro hamkorlikni ta'minlashda, muassasalar va hukumatlar o'rtasidagi axborot almashinuv mexanizmini kuchaytirishda

muhim ahamiyatga ega. Ushbu sohalarni kuchaytirish Kiberxavfsizlik hodisalariga javob berishning muhim omillaridan biri hisoblanadi.

Kiberxavfsizlik hodisalariga javob berish, dastlab, texnik muammolarni hal qilishni talab qiladi va shu bilan birga, huquqiy masalalar ham takomillashtirishni talab qiladi. Xalqaro huquq, milliy qonunchilik va kiberxavfsizlik siyosatlari barchasi birgalikda kiberxavfsizlikka qarshi kurashishning samarali yo'llarini belgilaydi. Kiberhujumlar hamda noqonuniy kiber hodisalar jahon miqyosida kiberjinoyatchilikka qarshi kurashish uchun yangi huquqiy qoidalar va normativlarni ishlab chiqishni talab qiladi.

Kiberxavfsizlikka oid huquqiy me'yorlar nafaqat davlatlar o'rtasida, balki hamkorlikni ta'minlash, balki davlat ichida ham axborot xavfsizligini ta'minlashni ko'zda tutadi. Ko'plab xalqaro tashkilotlar, masalan, Birlashgan Millatlar Tashkiloti (BMT), Iqtisodiy Hamkorlik va Taraqqiyot Tashkiloti (OECD), Yevropa Ittifoqi (EU) va boshqa yirik xalqaro tuzilmalar kiberxavfsizlikni tartibga soluvchi va kiberjinoyatlarni oldini olishga qaratilgan me'yorlar ishlab chiqmoqda.

Kiberxavfsizlikning huquqiy qirralaridan tashqari, axloqiy masalalar ham alohida ahamiyatga ega. Kiberxavfsizlik hodisalariga javob berishda axloqiy tomonlama, inson huquqlari, ma'lumotlarni himoya qilish va axborot erkinligi bilan bog'liq muammolarni yoritishga yordam beradi. Internet foydalanuvchilarining xavfsizligini saqlash, ma'lumotlarning maxfiyligini ta'minlash va shaxslarning huquqlarini hurmat qilish axloqiy masalalarni o'z ichiga oladi.

Kiberxavfsizlikning axloqiy muammolariga jiddiy qarash kerak hisoblanadi. Ayniqsa, ko'plab kiberxavfsizlikka oid hodisalar, masalan, shaxsiy ma'lumotlarning o'g'irlanishi, ma'lumotlarni notog'ri qo'llash yoki noto'g'ri ravishda ommalashtirish, odamlarning shaxsiy hayotiga tahdid solishi ham ushbu masala bilan bog'liq. Shu sababdan, axborot xavfsizligi tizimlarini yaratishda yoki kiberhujumga javob berishda axloqiy me'yorlar va qoidalar muhim rol o'ynaydi.

Mazkur ish mavzuga doir masallarda kiber huquq sohasida ish olib borgan soha mutaxassislari, jumladan S.W.Brenner, M.A. Geist, L.A. Reis, D.E. Sorkin, Прохотосердов М.А., J.Thomas, B.Schneier, D.J.Slove, K.D. Mitnick, S.S. Niyozova, N.S. Salayev, W.L., S.Gulyamov, Anorboyev A.U, Karpova D.N. larning ishlari hamda boshqa tadqiqotlar va boshqa rasmiy manbaalar o'rganilgan.

Mavzuning asosiy maqsadi kiberxavfsizlik hodisalariga javob berishda huquqiy va axloqiy masalalarning asosiy maqsadi yuzaga kelishi mumkin bo'lgan kiberxavfsizlik hodisalariga javob berish jarayonidagi huquqiy va axloqiy masalalarni tahlil qilish va ularni milliy va xalqaro miqyosda qanday tartibga solinishini ko'rsatishdir. Mazkur ishda kiberxavfsizlikka oid qonuniy va axloqiy masalalar, shuningdek, kiberxavfsizlikka javob berishning samarali tizimini yaratishda muhim bo'lgan normativ va me'yoriy hujjatlar yoritiladi hamda tahlil qilinadi.

Ishda kiberxavfsizlikni ta'minlash jarayonida yuzaga kelishi mumkin bo'lgan huquqiy va axloqiy ziddiyatlar, kiberxavfsizlikka javob berish jarayonida davlatlar va tashkilotlar o'rtasidagi hamkorlikni, axborot almashinuvini rivojlantirish uchun zarur bo'lgan huquqiy

va axloqiy me'yorlar ko'rib chiqiladi. Kiberxavfsizlikni ta'minlashda axloqiy masalalar, shaxsiy huquqlarni himoya qilish va xalqaro huquqni qo'llashning ahamiyati ta'kidlanadi.

ASOSIY QISIM

Axborot texnologiyalarining jadal rivojlanishi 21-asrning eng muhim hodisalaridan biri bo'lib, insoniyat hayotining barcha jabhalariga chuqur kirib bordi. U global miqyosda ijtimoiy, iqtisodiy va siyosiy jarayonlarga tub o'zgarishlar olib keldi. Internet va raqamli platformalar insonlarning kundalik hayotining ajralmas qismiga aylangan bir paytda, kiber makondagi huquqiy munosabatlar, xavfsizlik va shaxsiy hayotni himoya qilish masalalari dolzarb muammo sifatida maydonga chiqdi. Internet, kompyuter tarmoqlari va raqamli tizimlar yordamida ijtimoiy, iqtisodiy, siyosiy va madaniy faoliyatlar transformatsiyaga uchramoqda. Shu bilan birga, ushbu texnologiyalar bilan bog'liq xavflar, kiber jinoyatlar va ularni tartibga soluvchi huquqiy mexanizmlarning zarurati ham oshib bormoqda.

Kiberxavfsizlik kompyuter tizimlari, tarmoqlar va ma'lumotlarni ruxsatsiz kirishdan, foydalanishdan, oshkor qilishdan, buzilishdan, o'zgartirishdan yoki yo'q qilishdan himoya qilish amaliyatini anglatadi. U nafaqat biznes va davlat tashkilotlari uchun, balki har bir inson uchun ham dolzarb masaladir. Kiberxavfsizlik hodisalari deganda axborot tizimlariga, tarmoqlarga yoki ma'lumotlarga ruxsatsiz kirish, ularni o'zgartirish, yo'q qilish yoki ularga to'sqinlik qilish kabi salbiy holatlar tushuniladi. Bu hodisalar jiddiy zarar yetkazishi, tashkilotlarning obro'siga putur yetkazishi va yirik moliyaviy yo'qotishlarga olib kelishi mumkin. Kiberxavfsizlik hodisalari odatda inson omili, texnik zaifliklar va tashkiliy boshqaruvdagi kamchiliklar natijasida yuzaga keladi. Kiberxavfsizlik hodisalarini oldini olish uchun kiberxavfsizlik choralari ko'rilishi lozim hisoblanadi.

2024-yilning 1-choragidagi statistik ma'lumotlarga qaraganda davlat organlari va tashkilotlarning 19 ta veb-resursida 70 ta zaiflik aniqlanib, bartaraf etildi. Shuningdek, internet tarmog'ining milliy segmentida 3 million 290 mingdan ortiq kiberhujumlar kuzatilgan.

Dunyo miqyosida kiberjinoyatlar soni va ulardan kelib chiqadigan moliyaviy zararlar yildan-yilga ortib bormoqda. Masalan, 2022-yilda kiberjinoyatlar global iqtisodiyotga taxminan 6 trillion dollar zarar yetkazgan. Juniper Research tadqiqotlariga ko'ra, bu zarar har yili o'rtacha 11 foizga oshib, 2024-yilga kelib

5 trillion dollardan oshishi prognoz qilingan edi.

Kiberxavfsizlik hodisalarining asosiy turlari va ularning tavsifi quyidagicha tariflanadi. Texnik zaifliklar tizimdagi zaifliklar va yangilanishlarning kechiktirilishi oqibatida yuzaga kelgan zaifliklar bo'lib, dasturiy ta'minot yoki tarmoqlarda mavjud bo'lgan xavfsizlik nuqsonlari, vaqtida yangilanmagan tizimlar kiberhujumlarga yo'l ochadi. Tizimdagi zaifliklar esa tizimning zaif nuqtalari, masalan, noto'g'ri konfiguratsiyalar, eskirgan dasturiy ta'minot va zaif autentifikatsiya mexanizmlari hisoblanadi va ular keyinchalik kiberxavfsizlik hodisalariga olib keladi. Mazkul holat amaliyotda juda ko'p uchraydi. Bunga misol qilib MOVEit dasturida aniqlangan zaiflik natijasida, 2023-yilda 2,700 dan ortiq tashkilotning ma'lumotlari sizib chiqqanligini keltirish mumkin. Yangilanishlarning kechiktirilishi dasturiy ta'minot yoki operatsion tizimlardagi xavfsizlik

nuqsonlari hisoblanadi, vaqtida yangilanmagan tizimlar esa katta ehtimol bilan kiberhujumlarga yo'l ochadi. Bunday holat Apache Struts dasturidagi zaiflik vaqtida tuzatilmaganligi sababli Equifax kompaniyasida sodir bo'lgan. Hodisada 147 million foydalanuvchining ma'lumotlari sizib chiqqan.

Kiber xavfda inson omili foydalanuvchi shaxslarning kuchli bo'lmagan yoki juda oddiy bo'lgan parollardan foydalanishi, shubhali va havfli bo'lgan havolalarni bosishi yoki shaxsiy ma'lumotlarni oshkor qilish ga rusat bildirishi hisoblanadi. Inson omili kiberxavfsizlik hodisalarining asosiy sabablaridan biri hisoblanadi va kiberxavfsizlikka jiddiy tahdid tug'diradi. Verizon kompaniyasining 2023-yilgi hisobotiga ko'ra, kiberxavfsizlik hodisalarining 74% inson xatolari bilan bog'liq bo'lib, bu ko'rsatkich foydalanuvchilarning phishing hujumlariga uchrashi, kuchsiz parollardan foydalanishi va noto'g'ri havolalarga bosishi kabi holatlarni o'z ichiga oladi.

Ichki tahdidlar kompaniya yoki tashkilot ichidagi xodimlar tomonidan qasddan yoki bexosdan sodir etilgan harakatlar, maxfiy ma'lumotlarning sizib chiqishiga olib kelishi. Kompaniya yoki tashkilot ichidagi xodimlar tomonidan qasddan yoki bexosdan sodir etilgan harakatlar, maxfiy ma'lumotlarning sizib chiqishiga olib keladi. Masalan, SingHealth kompaniyasida sodir bo'lgan hodisada, xodimlarning ehtiyotsizligi va tizimdagi zaifliklar natijasida 1,5 million bemorning shaxsiy ma'lumotlari sizib chiqishiga olib kelgan.

Ijtimoiy muhandislik hujumlari orqali xakerlar foydalanuvchini aldash orqali axborotni qo'lga kiritadi, bu esa odatda firibgarlik (phishing) yoki yolg'on xabarlar orqali amalga oshiriladi. Bu hujum foydalanuvchilarni aldash orqali maxfiy ma'lumotlarni qo'lga kiritishga qaratilgan harakat. Phishing hujumlari, telefon orqali aldash va boshqa usullar orqali foydalanuvchilarning login ma'lumotlari, moliyaviy ma'lumotlari va boshqa maxfiy axborotlari o'g'irlanadi.

Tashqi hujumlar (masalan, DDoS) tarmoqlarga ommaviy hujumlar orqali ularning ishdan chiqishiga sabab bo'ladi. Mobil qurilmalar va Wi-Fi tarmoqlari zaifligi, xavfsiz bo'lmagan tarmoqlarga ulanilgan holatda yoki noma'lum manbalardan dastur yuklanganida zararli dasturlar tizimga kirib borishiga yo'l ochadi.

Tashkiliy boshqaruvdagi kamchiliklar siyosat va protseduralarning yetishmasligi axborot xavfsizligi siyosatining yo'qligi yoki unga rioya qilinmasligi, xavfsizlik bo'yicha treninglarning o'tkazilmasligi kiberxavfsizlik tahdidlarini kelib chiqishiga olib keladi

Kiber huquq raqamli texnologiyalar, internet va axborot tizimlari bilan bog'liq huquqiy munosabatlarni tartibga soluvchi huquq sohasi. U axborot xavfsizligi, shaxsiy ma'lumotlarni himoya qilish, kiberjinoyatchilikka qarshi kurash va intellektual mulk huquqlarini o'z ichiga oladi. Kiber makon transmilliy xarakterga ega bo'lganligi sababli, an'anaviy huquqiy yondashuvlar bu sohada yetarli darajada samarali emas. Kiberjinoyatlar nafaqat texnik jihatdan, balki huquqiy jihatdan ham murakkab hisoblanadi. Har bir davlatning huquqiy tizimi bu jinoyatlarga o'ziga xos tarzda yondashadi, biroq yagona xalqaro yondashuv mavjud emas.

Axborot texnologiyalari tez rivojlanib borayotgani sababli kiberhuquq ham doimiy o'zgarib bormoqda hamda uning shakllanayotgan talqinlari vujudga kelmoqda. Masalan

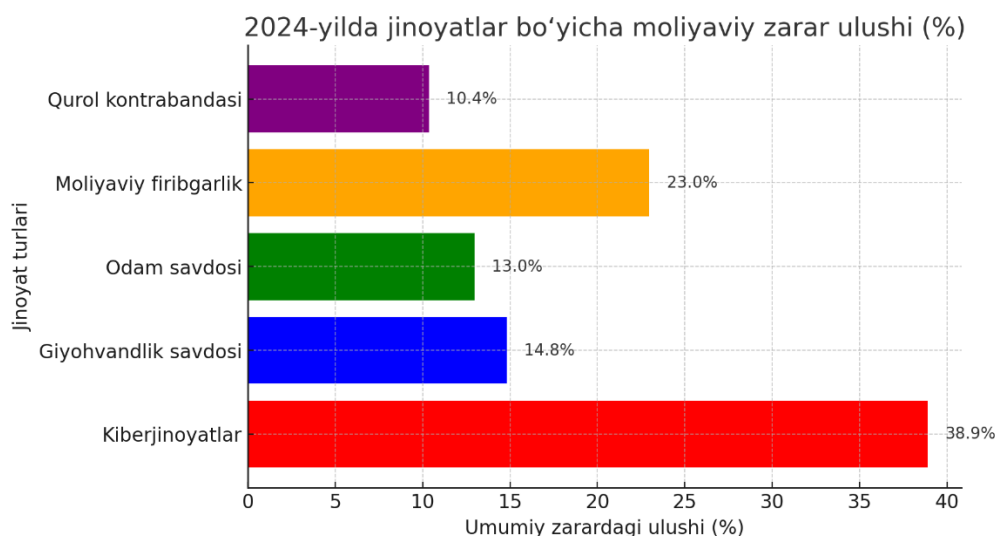
Sun'iy intellektning huquqiy maqomi, mas'uliyati va undan foydalanish qoidalari muhokama qilinmoqda. Kiberjinoyatchilik va xalqaro yurisdiksiya, internet chegaralarsiz ekanligi sababli, jinoyatchilarga qarshi kurash xalqaro huquqiy masalalarni keltirib chiqarmoqda. Ushbu masalalar qatorida Metaverse'da sodir bo'lgan firibgarlik yoki kiberjinoyatlar qanday tartibga solinishi kerakligi masalasi, Blokcheyn va kriptovalyutalar huquqi kriptovalyutalarning huquqiy maqomi har bir davlatda farq qilishi, raqamli maxfiylik va ma'lumotlar himoyasi, GDPR (Evropa Ittifoqining umumiy ma'lumotlarni himoya qilish qoidalari) kabi qonunlar foydalanuvchilarning shaxsiy ma'lumotlarini himoya qilishi ko'rish mumkin.

Intellektual mulk va raqamli maxfiylik sohalaridagi "Is a Global Solution Possible to the Technology Privacy Conundrum" texnologik rivojlanish va shaxsiy hayot daxlsizligi o'rtasidagi muvozanatni saqlashda xalqaro yondashuvlarning imkoniyatlari va cheklovlarini o'rganadi. Xulosa qilib aytadigan bo'lsak, kiberhuquqning an'anaviy yondashuvi internet va axborot tizimlari bilan bog'liq bo'lsa, zamonaviy yondashuvlar sun'iy intellekt, blokcheyn va metaverse kabi yangi texnologiyalarni o'z ichiga olmoqda. Kiberhuquqning kelajagi internet va raqamli makon rivojlanishi bilan chambarchas bog'liq, davlatlar va xalqaro tashkilotlar esa bu sohada hamkorlikni kuchaytirishi kerak.

Kiber tahdidlarning asosiy turlari raqamli tizimlardagi kiber tahdidlar, ma'lumotlar va tarmoqlarga zarar yetkazishga qaratilgan har qanday harakat yoki jarayonlar hisoblandi. Ular jismoniy shaxslarga, kompaniyalarga va davlat idoralariga xavf tug'dirishi mumkin.

Dunyodagi eng mashhur kiber hujumlar dan biri bu WannaCry (2017). Bu kiber hujum global miqyosda tarqalgan va asosan Microsoft Windows tizimlarida zaiflikdan foydalangan. WannaCry ransomware dasturi bir nechta davlatlar va kompaniyalarga zarar yetkazdi, shu jumladan, Britaniyaning sog'liqni saqlash tizimi (NHS) va ruslarning telekommunikatsiya kompaniyasiga ham. WannaCry EternalBlue nomli eksploitdan foydalangan, bu zaiflik Windows'ning Server Message Block (SMB) protokolidagi nuqson tufayli yuzaga kelgan. Yana bir misoldan biri, EternalBlue AQSh Milliy Xavfsizlik Agentligi (NSA) tomonidan kashf etilgan va yashirincha foydalanilgan, lekin 2017-yilda Shadow Brokers nomli xaker guruhi bu eksploitni oshkor qildi. Microsoft bu zaiflikni 2017-yil mart oyida tuzatgan bo'lsa ham, ko'plab foydalanuvchilar xavfsizlik yangilanishlarini o'z vaqtida o'rnatmagan.

Kiberjinoyatlar bo'yicha jahon reytingida Rossiya yetakchilik qilmoqda, undan keyingi o'rinlarda Ukraina, Xitoy, AQSh va Nigeriya joylashgan. Bu mamlakatlar kiberjinoyatlarning asosiy manbalari sifatida qayd etilgan. Ushbu ma'lumotlar kiberjinoyatlar global miqyosda jiddiy tahdid ekanligini ko'rsatadi. Shu sababli, barcha davlatlar kiberxavfsizlik choralari kuchaytirish, fuqarolarni ogohlikka chaqirish va zamonaviy texnologiyalardan xavfsiz foydalanishni targ'ib qilishlari zarur.



Kiberhuquqda maxfiylik va etika muhim tamoyillar bo'lib, raqamli dunyoda foydalanuvchilarning shaxsiy ma'lumotlarini himoya qilish va axborotdan to'g'ri foydalanishni ta'minlashga qaratilgan. Maxfiylikni ta'minlashning asosiy tamoyillari, ma'lumotlarga egalik qilish, yani foydalanuvchilar o'z ma'lumotlarini nazorat qila olishlari. Ruxsat bilan foydalanish ma'lumotlarni faqat egasining roziligi bilan ishlatish kerak. Ma'lumotlarni himoya qilish - kompaniyalar va davlat idoralari shaxsiy ma'lumotlarni saqlashda maxsus xavfsizlik choralarini ko'rish lozim. Maxfiylik huquqini tartibga soluvchi qonunlar General Data Protection Regulation (GDPR) Yevropa Ittifoqining shaxsiy ma'lumotlarni himoya qilish bo'yicha qonuni, California Consumer Privacy Act (CCPA) - AQShning Kaliforniya shtatidagi maxfiylik qonuni, O'zbekiston Respublikasining "Shaxsiy ma'lumotlar to'g'risida"gi qonuni (Shaxsiy ma'lumotlarni yig'ish va qayta ishlash qoidalarini belgilaydi).

Ma'lumotlarni himoya qilish shaxsiy, korporativ yoki davlat ma'lumotlarini ruxsatsiz kirish, o'g'irlik, buzish va yo'qotishdan saqlashga qaratilgan texnologik va huquqiy choralar majmui. Maxfiylik (Confidentiality)da ma'lumotlarga faqat ruxsat berilgan shaxslar kirishi mumkin.

Ma'lumotlarni himoya qilish qonunlari:

- GDPR (Yevropa Ittifoqi) - Shaxsiy ma'lumotlarni himoya qilish bo'yicha qat'iy qoidalar.
- CCPA (Kaliforniya) - Foydalanuvchilarga o'z ma'lumotlarini boshqarish huquqini beradi.
- O'zbekiston Respublikasining "Shaxsiy ma'lumotlar to'g'risida"gi qonuni shaxsiy ma'lumotlarni noqonuniy yig'ish va ishlatishga qarshi chora-tadbirlar belgilaydi.

Hozirgi kunda eng ko'p o'g'irlanayotgan shaxsiy ma'lumotlar, asosan, moliyaviy ma'lumotlar va onlayn hisoblar bilan bog'liq. O'g'irlangan shaxsiy ma'lumotlar turlarini va ular uchun ishlatiladigan kredit karta va bank ma'lumotlari, shaxsiy kimlik va identifikatsiya ma'lumotlari, elektron pochta va ijtimoiy tarmoqlardagi hisoblar, onlayn login va parol ma'lumotlari, tibbiy ma'lumotlar asosiy obekt hisoblanadi.

Rivojlangan davlatlar tajribasini ko'ra, AQShning kiberxavfsizlik bo'yicha federal siyosat Cybersecurity and Infrastructure Security Agency (CISA) faoliyatini yuritadi. Bu AQShning Kaliforniya shtatida 2018-yilda qabul qilingan va 2020-yil 1-yanvardan kuchga kirgan muhim maxfiylik to'g'risidagi qonun hisoblanadi. U Kaliforniya fuqarolarining shaxsiy ma'lumotlarini qanday to'planishi, ishlatilishi va tarqatilishini tartibga soladi. CCPA AQShdagi eng muhim va ta'sirli ma'lumotlarni himoya qilish qonunlaridan biri bo'lib, uni ko'pincha Yevropadagi General Data Protection Regulation (GDPR)ga qiyoslash mumkin. AQShda kiberjinoyatlar bo'yicha javobgarlik Computer Fraud and Abuse Act (CFAA) orqali tartibga solinadi hamda kiber jinoyatlarga qarshi kurashishda asosiy huquqiy tayanch hisoblanadi. Bu qonun doirasida bir qator yirik ishlar ko'rilgan, xususan, ruxsatsiz ma'lumotlarni yuklab olish, "phishing" hujumlar, "malware" tarqatish va boshqa zararli faoliyatlar ushbu qonun asosida baholangan.

Yevropa Ittifoqi tajribasida ma'lumotlarni himoya qilish umumiy reglamenti (General Data Protection Regulation - GDPR) hisoblanadi. ENISA Yevropa Kiberxavfsizlik Agentligi faoliyatining asosiy vazifasini belgilab, a'zo davlatlar o'rtasida ma'lumot almashish va xavfsizlik tarmoqlarini muvofiqlashtiradi.

Janubiy Koreya davlati Raqamli texnologiyalar rivoji va hukumatning faol kiberxavfsizlik siyosatini yuritadi. Janubiy Koreya hukumati Milliy kiberxavfsizlik strategiyasi asosida barcha sektorlar uchun yagona xavfsizlik siyosatini ishlab chiqqan. Ushbu davlat Personal Information Protection Act (PIPA) asosida ma'lumotlarni himoya qiladi. Hamda ushbu davlatda Milliy kiberxavfsizlik markazi (NCSC) faoliya yuritadi. Yuqoridgi davlatlarning hozirgi kungacha ushbu huquqsohasida erishgan yutuqlari va kamchiligidan inobatga olib boshqa davlatlar o'z kiber xavfsizlik mexanizmlarini ishlab chiqishmoqda.

Kiberjinoyatlar tobora ko'proq transmilliy tus olayotgani sababli, ularni samarali tarzda jilovlash uchun davlatlararo hamkorlik zarur bo'lmoqda. Shu nuqtai nazardan, bir qator xalqaro tashkilotlar ushbu sohada muhim tashabbuslar va huquqiy mexanizmlar ishlab chiqmoqda. Birlashgan Millatlar Tashkiloti (BMT) BMT global miqyosda kiberjinoyatlarga qarshi kurashish bo'yicha yirik tashabbuslarni ilgari surmoqda. Tashkilot tomonidan davlatlar o'rtasida axborot xavfsizligini ta'minlashga qaratilgan muloqotlar va rezolyutsiyalar qabul qilinmoqda. Bundan tashqari raqamli huquqlar va fuqarolarning shaxsiy hayot daxlsizligini himoya qilish BMT rezolyutsiyalari orqali qo'llab-quvvatlanmoqda va BMTning ixtisoslashgan agentliklari orqali kiber tahdidlar monitoringi va xalqaro huquqiy normalarning ishlab chiqilishi yo'lga qo'yilgan.

Xalqaro jinoiy politsiya tashkiloti INTERPOL kiberjinoyatchilikka qarshi global kurashda muhim o'rin tutib, "Cybercrime Directorate" orqali turli mamlakatlar o'rtasida operativ ma'lumot almashish va qo'shma amaliyotlarni tashkil qiladi. INTERPOL transchegaraviy kiberhujumlar bo'yicha tezkor choralar ko'rish, jinoyatchilarni aniqlash va ularni qo'lga olishda xalqaro muvofiqlashtiruvchi rolni bajarib, a'zolar o'rtasida texnologik imkoniyatlar va tajriba almashinuvini ta'minlaydi.

Xalqaro telekommunikatsiya ittifoqi ITU BMTning ixtisoslashgan agentligi bo'lib, axborot-kommunikatsiya texnologiyalaridan foydalanish xavfsizligini targ'ib qiladi. U har yili "Global Cybersecurity Index" (GCI) orqali mamlakatlarning kiberxavfsizlik darajasini baholaydi. Axborot xavfsizligi standartlarini ishlab chiqadi va davlatlarga texnik ko'mak beradi, kiberhujumlar profilaktikasi va tezkor javob tizimlari bo'yicha metodik qo'llanmalar tayyorlaydi.

Yevropa Kengashi Budapesht Konvensiyasi ("Cybercrime Convention") 2001-yilda imzolangan, kiberjinoyatlarga qarshi birinchi xalqaro huquqiy hujjat hisoblanadi. U A'zo davlatlar o'rtasida tergov davomida o'zaro yuridik yordam va ma'lumot almashinuvini yo'lga qo'yadi. Jinoyatchilarning ekstraditsiyasi, raqamli dalillarni qonuniy ravishda olish va ularni xalqaro darajada tan olish mexanizmlarini belgilab, konvensiyaga qo'shilgan davlatlar uchun bir xil normativ-huquqiy asos yaratadi, shu orqali jinoyatga javoban muvofiqlashtirilgan choralar ko'rish imkonini beradi.

Xalqaro huquqiy me'yorlar va standartlar ham ushbu sohada muhim rol o'ynaydi, ushbu hujjatlar qatoriga ISO/IEC 27001 axborot xavfsizligini boshqarish tizimi standarti, OECD tavsiyalari raqamli iqtisodiyot va kiberxavfsizlikka oid xalqaro siyosat yo'nalishlari va Tallinn Manual (NATO Cooperative Cyber Defence Centre of Excellence) kiber urush holatlarida xalqaro gumanitar huquq qo'llanishini keltirish mumkin. Bu hujjatlar kiberxavfsizlikni xalqaro darajada boshqarishda, axborot xavfsizligi, kiber urushlar va raqamli infratuzilmani himoya qilishda qo'llaniladigan asosiy prinsiplarga asoslanadi. Ushbu hujjatlar va standartlar kiberxavfsizlik va axborot xavfsizligini ta'minlashda juda katta foyda keltiradi.

Har bir mamlakat o'zining siyosiy, iqtisodiy, madaniy va texnologik imkoniyatlaridan kelib chiqqan holda bu muammoga o'ziga xos yondashuvni ishlab chiqmoqda.

O'zbekiston kiberxavfsizlik sohasida so'nggi yillarda sezilarli islohotlar amalga oshirdi. 2022-yilda "Kiberxavfsizlik to'g'risida"gi Qonun qabul qilindi. Davlat xavfsizlik xizmati huzurida Axborot xavfsizligi markazi tashkil etildi. O'zbekistonda Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi, Raqamli texnologiyalar vazirligi, DXX, IIV va boshqa organlar hamkorlikda ishlaydi. Bundan tashqari, xalqaro hamkorlik (BMT, INTERPOL, ITU) orqali tajriba almashinuvi yo'lga qo'yilgan. O'zbekistonning yondashuvi huquqiy bazani mustahkamlash, texnik infratuzilmani rivojlantirish va kadrlar salohiyatini oshirishga qaratilgan.

O'zbekiston Raqamli transformatsiya va strategik yondashuvlarni amalga oshiradi. Bunda, "Raqamli O'zbekiston - 2030" strategiyasi: 2020-yil O'zbekiston Respublikasining "Raqamli O'zbekiston - 2030" strategiyasi qabul qilindi. Bu hujjat raqamli iqtisodiyot, elektron hukumat va axborot xavfsizligini rivojlantirishni ko'zda tutadi. Strategiyaning asosiy yo'nalishlaridan biri sifatida davlat boshqaruv tizimining raqamlashtirilishi va ushbu tizimlarda axborot xavfsizligining ta'minlanishi belgilandi.

O'zbekiston Raqamli texnologiyalar vazirligi AKT sohasidagi davlat siyosatini amalga oshiruvchi asosiy organ hisoblanadi. Vazirlik tomonidan axborot xavfsizligiga oid normativ hujjatlar ishlab chiqilmoqda, davlat organlarining AKT tizimlariga xavfsizlik talablarini

joriy etish bo'yicha ishlar olib borilmoqda. Vazirlig (sobiq Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi) Prezident farmoni va hukumat qarorlari asosida tashkil etilgan va o'z faoliyatini muayyan qonunlar, farmonlar, qarorlar va nizomlar asosida olib boradi. O'zbekiston Respublikasi Prezidentining qarori, 28.04.2020 yildagi PQ-4699-son ko'ra "Raqamli iqtisodiyot va elektron hukumatni keng joriy etish chora-tadbirlari to'g'risida" qarori qabul qilinadi. Bu hujjat orqali Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi bazasida Raqamli texnologiyalar vazirligi tashkil etildi. Bunda raqamli iqtisodiyot, kiberxavfsizlik va elektron hukumat sohalarini rivojlantirishni jadallashtirish kabi fazifalar vazirlik zimmasiga yuklatiladi. Ushbu vazirlik faoliyatini tartibga soluvchi quyidagi hujjatlar asosida amalga oshiriladi:

- O'zbekiston Respublikasining 11.12.2003 yildagi "Axborotlashtirish to'g'risida"gi 560-II-sonli qonuni. Bu qonun axborot tizimlari va texnologiyalarini yaratish, ishlatish va ularni himoya qilishning asosiy prinsiplarini belgilaydi.

- O'zbekiston Respublikasining 12.10.2022 yildagi O'RQ-793-son "Elektron hukumat to'g'risida"gi Qonun - davlat xizmatlarini elektron shaklda ko'rsatish va axborot almashinuvi tizimini tashkil etish bo'yicha normativ asosi hisoblanadi.

- O'RQ-764 "Kiberxavfsizlik to'g'risida"gi qonuni axborot infratuzilmasi va foydalanuvchilarni kiberxavflardan himoya qilishning yuridik asoslarini belgilaydi.

- 28.04.2020 yilgi PQ-4699 "Raqamli iqtisodiyot va elektron hukumatni keng joriy etish chora-tadbirlari to'g'risidaraqamli transformatsiyani joriy etish bo'yicha" muhim hujjat hisoblanadi.

DXX huzuridagi Axborot xavfsizligi markazi davlat muhim axborot infratuzilmasini himoya qilish, kiberxavfsizlik insidentlariga javob berish va tahdidlarni aniqlash bo'yicha faoliyat yuritadi. Markaz milliy miqyosda insidentlarga qarshi kurashishda muvofiqlashtiruvchi organ sifatida tan olingan. Uning Faoliyat "Kiberxavfsizlik to'g'risida"gi qonun (O'RQ-764-son, 2022-yil

15-aprel) orqali tartibga solinadi hamda kiberxavfsizlik sohasidagi asosiy tushunchalarni belgilab, Davlat xavfsizlik xizmatini vakolatli organ sifatida va kiberxavfsizlikni ta'minlashning asosiy prinsiplari, vazifalari va tartib-taomillarini belgilaydi. "Axborotlashtirish to'g'risida"gi qonun axborotlashtirish sohasidagi umumiy qoidalarni belgilaydi, shu jumladan axborot tizimlari va resurslarining xavfsizligini ta'minlashga doir talablarni o'z ichiga oladi.

"Kiberxavfsizlik markazi" DUK 2019-yilda tashkil etilgan. Ushbu markaz texnik audit, monitoring, xavfsizlik bo'yicha baholash va xalqaro tajribalarni joriy qilish bilan shug'ullanadi. U davlat va xususiy sektor uchun xizmatlar ko'rsatadi. O'zbekistondagi "Kiberxavfsizlik markazi" davlat unitar korxonasi (DUK) o'z faoliyatini 2013-yil 27-iyundagi PQ-1989-son qarori asosida faoliyatini boshlagan. Bu qaror "O'zbekiston Respublikasining Milliy axborot-kommunikatsiya tizimini yanada rivojlantirish chora-tadbirlari to'g'risida" bo'lib, unga muvofiq dastlabki "Axborot xavfsizligini ta'minlash markazi" tashkil etilgan. Hamda Vazirlar Mahkamasining 2013-yil 16-sentabrdagi 250-son qarori "Axborot xavfsizligini ta'minlash markazi" faoliyatini tashkil etish chora-tadbirlari

to'g'risida bo'lib, markazning tashkiliy asoslarini belgilagan. Bundan tashqari Prezidentning 2018-yil 21-noyabrdagi PQ-4024-son qarori, bu qaror "Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirish chora-tadbirlari to'g'risida" bo'lib, unga muvofiq markaz "Texnik ko'maklashish markazi" DUK sifatida qayta tashkil etilgan. Hozirda, "Kiberxavfsizlik markazi" davlat unitar korxonasi nomi bilan 14.09.2019 yildagi PQ-4452-son O'zbekiston Respublikasi Prezidentining "Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirishga oid qo'shimcha chora-tadbirlar to'g'risida"gi qaroriga muvofiq faoliyat yuritib kelmoqda.

Kiberxavfsizlikni mustahkamlash bo'yicha tashabbuslar, "Cyber Drill" va xalqaro hamkorlik O'zbekiston har yili xalqaro tashkilotlar, jumladan ITU va INTERPOL bilan hamkorlikda kiberxavfsizlik bo'yicha "Cyber Drill" amaliy mashg'ulotlarida ishtirok etadi. Ushbu mashg'ulotlar mutaxassislarni tayyorlash va tahdidlarga tayyorgarlikni oshirishga xizmat qiladi. U O'zbekiston milliy universitetlari, xususan TATU, INHA va Turin politexnika universitetlarida axborot xavfsizligi va kiberxavfsizlik bo'yicha o'quv dasturlarini yo'lga qo'yilgan va bu orqali sohaga malakali kadrlar yetkazib beradi.

Hozirda ijtimoiy axborot kompaniyalari raqamli savodxonlikni oshirish, firibgarlik va fishing tahdidlariga qarshi kurashish bo'yicha ommaviy axborot vositalari orqali aholiga tushuntirish ishlari olib borilmoqda. Maxsus "Kiberxavfsizlik oyligi" doirasida targ'ibot ishlari tashkil etiladi.

O'zbekiston kiber huquq sohasida oxirgi yillarda sezilarli islohotlarni amalga oshirmoqda. "Axborotlashtirish to'g'risida"gi qonun, "Kiberxavfsizlik to'g'risida"gi qonun va boshqa normativ hujjatlar orqali raqamli makondagi huquqiy munosabatlar tartibga solinmoqda. Shuningdek, Jinoyat Kodeksi va Ma'muriy javobgarlik to'g'risidagi Kodeks orqali kiberjinoyatlar uchun javobgarlik belgilangan.

Agar bu borada O'zbekistonni Singapur bilan solishtirsak, Singapurda bu qonunchilik ancha ilg'or va tizimli. Asosiy qonunlar qatoriga 1993-yilda qabul qilingan Computer Misuse Act, 2012-yilgi Personal Data Protection Act (PDPA) va 2018-yildagi Cybersecurity Act kiradi. Ushbu qonunlar orqali nafaqat texnologik jinoyatlar, balki shaxsiy ma'lumotlar muhofazasi, kompaniyalar xavfsizlik majburiyatlari ham qat'iy tartibga solingan. O'zbekistonda kiberxavfsizlikni ta'minlash bo'yicha davlat tomonidan muhim tashabbuslar ilgari surilmoqda. Xususan, "Raqamli O'zbekiston - 2030" strategiyasi orqali kiberxavfsizlikni mustahkamlash maqsad qilingan. Bu borada "Kiberxavfsizlik markazi", IIV va Davlat xavfsizlik xizmatining maxsus bo'limlari faoliyat yuritadi. Singapurda esa Cyber Security Agency (CSA) va Infocomm Media Development Authority (IMDA) kabi tashkilotlar kiberxavfsizlikni boshqaradi. Ushbu organlar davlat va xususiy sektor o'rtasida uzviy hamkorlikni yo'lga qo'ygan bo'lib, xavfsizlik standartlari, audit va monitoring tizimlari ishlab chiqilgan. Xalqaro reytinglarda, masalan, ITU Global Cybersecurity Index'da Singapur doimo yuqori o'rinlarni egallab kelmoqda.

Har ikki davlatda ham kiberjinoyatlar jinoyat deb e'tirof etilgan bo'lsa-da, yondashuv va jazo choralarida farqlar mavjud. O'zbekistonda kibermakon orqali amalga oshirilgan

huquqbuzarliklar uchun odatda jarima yoki 5-7 yilgacha ozodlikdan mahrum qilish jazolari nazarda tutilgan. Kiberjinoyat turlariga noqonuniy kirish, fishing, ma'lumotlarni buzish va boshqalar kiradi. Singapurda esa bu boradagi yondashuv nihoyatda qat'iy. Ransomware, zararli dasturlar tarqatish, hattoki ruxsatsiz etika xakerligi uchun ham 10 yilgacha ozodlikdan mahrum qilish mumkin. Bu qonunlar orqali xatarli texnologik faoliyatlar qat'iy nazorat ostiga olingan.

O'zbekiston kiber jinoyatlarga qarshi kurashishda xalqaro tashkilotlar, jumladan BMT, ITU va MDH doirasida hamkorlikni yo'lga qo'ygan. Shuningdek, xorijiy davlatlar bilan ikki tomonlama memorandumlar orqali axborot almashinuvi yo'lga qo'yilmoqda. Ammo hali Budapest Konvensiyasi (Kiberjinoyatlarga qarshi kurashish bo'yicha xalqaro konvensiya) imzolanmagan. Singapur esa ASEAN, Interpol, BMT va boshqa xalqaro tuzilmalar bilan yaqindan ishlaydi. Garchi Budapest Konvensiyasiga rasmiy a'zo bo'lmasada, mamlakat qonunchiligi unga moslashtirilgan va xalqaro hamkorlik faol amalga oshiriladi. "Kiber jinoyatlar nafaqat texnik jihatdan, balki huquqiy jihatdan ham murakkab. Har bir davlatning huquqiy tizimi bu jinoyatlarga o'ziga xos tarzda yondashadi, biroq yagona xalqaro yondashuv mavjud emas." Bu fikr O'zbekistonning hali Budapest Konvensiyasiga qo'shilmaganligini va xalqaro me'yorlar bilan integratsiya qilish zaruratini ko'rsatadi. "Raqamli makonda shaxsiy hayot daxlsizligini ta'minlash nafaqat texnik, balki kuchli qonunchilik orqali bo'lishi kerak. Ma'lumotlar himoyasi - zamonaviy demokratiyaning poydevoridir."

O'zbekistonning "Shaxsiy ma'lumotlar to'g'risida"gi qonuni hozirda bu jihatdan mustahkamlanayotganiga urg'u berish mumkin. "Raqamli huquqlar doimiy ravishda kengayib borayotgan soha. Kiber huquq faqat jinoyat emas, balki internetdagi ijtimoiy, iqtisodiy va madaniy huquqlarni ham o'z ichiga oladi." Bu fikr orqali kiber huquq nafaqat xavfsizlik, balki fuqarolarning raqamli erkinliklari bilan ham bog'liqligini ko'rsatish mumkin. "Kiber makonda faoliyat yuritish - bu axloqiy mas'uliyatni ham o'z ichiga oladi. Kiber qonunchilik axloqiy prinsiplar asosida shakllanishi kerak." O'zbekiston qonunchiligini ishlab chiqishda ham etik tamoyillarni hisobga olish zaruriyati haqida dalil. "Kiber qonunchilik rivojlanayotgan davlatlarda an'anaviy huquqiy doiralardan chiqib, texnologiyaga mos yondashuvlar asosida shakllanishi kerak. Bu esa tezkor moslashuvchanlikni talab qiladi." Bu aynan O'zbekiston holatiga mos keladi, chunki mamlakat hozir texnologik yuksalish davrida turibdi va qonunlar zamonga moslashtirilmoqda. Natijalar shuni ko'rsatadiki, kiber huquq zamonaviy jamiyatning har bir qatlamiga ta'sir qiluvchi, murakkab va ko'p qirrali sohaga aylangan. O'zbekiston bu yo'nalishda sezilarli siljishlarga ega bo'lsa-da, xalqaro tajriba va yondashuvlarni chuqur o'rganib, qonunchilikni yanada takomillashtirish zarur. Ayniqsa, Susan Brenner va Talat Fatima fikrlari orqali rivojlanayotgan davlatlar oldida turgan muammolar va imkoniyatlar yanada ravshan ko'rinadi.

So'nggi yillarda O'zbekistonning axborot texnologiyalari sohasidagi jadal rivojlanishi raqamli infratuzilmaning kengayishiga, shu bilan birga, kiberxavfsizlikka oid tahdidlarning ortishiga olib keldi. Elektron hukumat tizimlarining keng joriy etilishi, internet

xizmatlarining ommalashuvi, mobil ilovalarning ko'pligi va raqamli xizmatlar hajmining oshishi O'zbekiston kiberxavfsizligi oldiga yangi va murakkab muammolarni qo'yimoqda.

O'zbekiston Respublikasida raqamli texnologiyalar, sun'iy intellekt, elektron hukumat, onlayn xizmatlar va elektron savdo kabi yo'nalishlarning jadal rivojlanishi natijasida axborot makoni va kiberhududda huquqiy tartibotlarni ta'minlash zarurati keskin ortdi. Natijada, davlat tomonidan kiber huquq sohasini huquqiy jihatdan tartibga solish, milliy xavfsizlikni ta'minlash va fuqarolarning axborotdagi huquq va erkinliklarini himoya qilishga qaratilgan tizimli qonunchilik bazasi shakllantirila boshlandi. Axborot texnologiyalari sohasidagi jinoyatlarning oldini olish choralari huquqiy tartibga solish asosi sifatida O'zbekiston Respublikasi Konstitutsiyasining bir qator qoidalari, xususan, axborot olish erkinligi amal qiladi, bu esa davlatga mazkur huquqlarga rioya etish va ularni himoya qilish majburiyatini yuklaydi.

Axborotni izlash, olish va tarqatishga bo'lgan huquqni cheklashga faqat qonunga muvofiq hamda faqat konstitutsiyaviy tuzumni, aholining sog'lig'ini, ijtimoiy axloqni, boshqa shaxslarning huquq va erkinliklarini himoya qilish, jamoat xavfsizligini hamda jamoat tartibini ta'minlash, shuningdek davlat sirlari yoki qonun bilan qo'riqlanadigan boshqa sir oshkor etilishining oldini olish maqsadida zarur bo'lgan doirada yo'l qo'yiladi" deb keltirilgan.

Konstitutsiyaviy normalarda qayd etilganidek, har kim istalgan axborotni izlash, olish va tarqatish huquqiga ega. Bu huquq Internetdagi so'z erkinligi, raqamli axborot erkinligi, onlayn jurnalistika, ijtimoiy tarmoqlardagi faollik kabilarni ham o'z ichiga oladi.

O'zbekiston Respublikasi jinoyat kodeksiga ko'ra XX1-bob axborot texnologiyalari sohasidagi jinoyatlarni tartibga soladi

Hamda MJKga ko'ra 461-moddadan boshlab axborot sohasidagi qoidabuzarliklar tartibga solish uchu qaratilgan moddalar mavjudligini ko'rishimiz mumkin.

O'zbekiston Respublikasi qonun va qonunosti hujjatlariga to'x'taladigan bo'lsak birinchi navbatda "Axborotlashtirish to'g'risida"gi qonunni talqin qilib o'tish kerak. Qonun "Axborot sohasidagi munosabatlarni tartibga solish, axborot infratuzilmasini shakllantirish, axborot texnologiyalaridan foydalanishni huquqiy asosda yo'lga qo'yish" kabi funksiyalarni tartibga soladi. Ushbu qonun moddalariga batafsilroq to'xtaladigan bo'lsak: Axborotdan foydalanish huquqi Fuqarolar, yuridik shaxslar axborotdan erkin foydalanish huquqiga ega. Bu internetdan erkin foydalanish va so'z erkinligi kabi tamoyillar asosida ishlaydi. Ushbu qonunning asosiy maqsadi axborot tizimlari, texnologiyalari va resurslaridan foydalanishning huquqiy asoslarini yaratish, ushbu qonun orqali davlat va jamiyat manfaatlariga mos holda raqamli axborotni himoya qilish, shaxsiy ma'lumotlarni saqlash, va axborot tizimlarining barqaror ishlashini ta'minlash mexanizmlari yaratilgan. Axborotni himoyalash vositalar, maxfiy axborotlar, shaxsiy ma'lumotlar va boshqa resurslarni himoya qilishda texnik va tashkiliy choralari ko'riladi. Bu qonun O'zbekistonda ilk bor axborot, texnologiya va xavfsizlik masalalarini qonuniy doiraga olib kirgan. U keyingi barcha kiberxavfsizlik, elektron hukumat, shaxsiy ma'lumotlar, elektron imzo qonunlariga zamin yaratdi. Bugungi kunda "axborot xavfsizligi", "axborot resurslari", "axborot tizimi" kabi

kiber huquqiy terminlar aynan shu qonun orqali yuridik ahamiyatga ega bo'ldi hamda uning asosida 2019-yilda qabul qilingan "Shaxsga doir ma'lumotlar to'g'risida"gi qonun, "Elektron raqamli imzo to'g'risida"gi Qonun, "Elektron hukumat to'g'risida"gi Qonun, "Kiberxavfsizlik to'g'risida"gi qonun loyihalari va strategik dasturlar ishlab chiqildi. Bundan tashqari barcha davlat organlarining ma'lumotlar bazalari, onlayn xizmatlar va raqamli portallar xavfsizligini ta'minlashga qaratilgan huquqiy infratuzilma paydo bo'ldi.

"O'zbekistonda kiber huquqiy tizimning shakllanishi aynan 2003-yildagi "Axborotlashtirish to'g'risida"gi Qonun bilan boshlangan. Bu hujjat nafaqat axborot texnologiyalarini rivojlantirdi, balki huquqiy tafakkurda ham raqamli soha madaniyatini shakllantirdi deb takidlagan. Bugungi kunda elektron hukumat, masofaviy ta'lim, raqamli xavfsizlik - bularning barchasiga huquqiy asos sifatida aynan ushbu qonun xizmat qiladi deb ushbu qonunga tarif bergan. Bundan tashqari "Elektron raqamli imzo to'g'risida"gi Qonunning o'rni va ahamiyatiga to'xtaladigan bo'lsak. Qonun davlat organlari faoliyatini raqamlashtirish, fuqarolarga elektron xizmatlar ko'rsatishni takomillashtirish va davlat boshqaruvining ochiqligini ta'minlash maqsadida qabul qilingan. Qonun elektron hujjat almashinuvi, axborot tizimlari integratsiyasi va axborot xavfsizligini ta'minlashni o'z ichiga oladi.

"Elektron hukumat to'g'risida"gi Qonun davlat va jamiyat o'rtasida ochiq, ishonchli hamkorlik tizimini yaratishda huquqiy kafolat bo'lib xizmat qiladi. Shuningdek, bu qonunni raqamli islohotlar asosini tashkil etuvchi yadro hujjat

2022-yilgi "Reklama to'g'risida"gi qonun kiber makonda axborot muhitining sifati va tozaligini ta'minlashga qaratilgan bo'lib, foydalanuvchilarning huquqlarini himoya qilishda muhim ahamiyatga ega. Ushbu qonun internet va boshqa raqamli platformalarda tarqatilayotgan reklamalar orqali foydalanuvchilarning huquqlari buzilishining oldini olish, shuningdek, axborot muhitining sifati va tozaligini ta'minlashdan iborat. Hamda kiber hququdagi axloqiy masalalarda, foydalanuvchilarning roziligisiz ularga reklama yuborilishini cheklash, shuningdek, shaxsiy ma'lumotlarning qonuniy ishlatilishiga e'tibor qaratadi.

2019-yilgi "Shaxsga doir ma'lumotlar to'g'risida"gi qonun shaxsga oid ma'lumotlarni yig'ish, saqlash, qayta ishlash va uzatish tartiblarini belgilaydi. Shuningdek, O'zbekistonda faoliyat yurituvchi xorijiy internet-resurslarni milliy reyestrda kiritish talabi ham ushbu qonun orqali nazarda tutilgan.

"Axborot erkinligi prinsiplari va kafolatlari to'g'risida"gi qonun - so'z va axborot erkinligini huquqiy jihatdan mustahkamlash, ommaviy axborot vositalari faoliyatini tartibga solish, davlat axborotlaridan erkin foydalanish imkoniyatini ta'minlashni nazarda tutadi. Ushbu qonun "fuqarolarning axborot olish, uni tarqatish va undan foydalanish erkinligini mustahkamlovchi konstitutsiyaviy prinsiplarni amaliyotda qo'llash uchun zarur bo'lgan muhim huquqiy asosdir" deb takidlangan.

Yan bir kiber huquq sohasidagi eng muhim qonundan biri bu 15.04.2022 yilgi O'zbekiston Respublikasining O'RQ-764-sonli "Kiberxavfsizlik to'g'risida"gi qonuni davlat, raqamli infratuzilmani himoya qilish, jamiyat va shaxsning axborot sohasidagi

xavfsizligini ta'minlashga va axborot texnologiyalari sohasidagi tahdidlarga qarshi samarali tizim yaratishga qaratilgan hisoblanadi. Mazkur qonun ilgari mavjud bo'lgan tarqoq huquqiy me'yorlarni yagona huquqiy platformaga birlashtirgan holda kiberxavfsizlik sohasidagi munosabatlarni to'liq qamrab oldi hamda turli sohalarda sezilarli rivojlanishlarga olib keldi. Bunda birinchi navbatda Davlat organlarining IT infratuzilmasini mustahkamlash, kiberjinoyatlarga qarshi kurashish bo'yicha mexanizmlarni aniqlashtirish, kiberxavfsizlik siyosati va strategiyalarini ishlab chiqish uchun huquqiy asos yaratishga sababchi bo'lganligini takidlash lozim. Mazkur qonun kiberxavfsizlik bo'yicha respublika miqyosida yagona huquqiy maydon yaratdi, hamda unda davlat organlarining roli, fuqarolarning majburiyatlari va biznes subyektlarining javobgarligi aniq belgilab berildi. Qonun raqamli xizmatlarning ishonchliligini ta'minlab, fuqarolar va investorlar ishonchini oshirishga xizmat qiladi. O'zbekiston ushbu qonun orqali xalqaro axborot xavfsizligi sohasidagi konvensiyalar, jumladan, Budapest konvensiyasi tamoyillariga yaqinlashmoqda. Bu esa xalqaro maydonda kiberjinoyatlarga qarshi hamkorlik qilish imkonini yaratadi.

Xulosa qilib aytadigan bo'lsak, "Kiberxavfsizlik to'g'risida"gi qonunning qabul qilinishi O'zbekistonning raqamli suverenitetini ta'minlash, ijtimoiy barqarorlikni saqlash va axborot makonini havflardan himoyalash yo'lidagi muhim huquqiy qadam hisoblanadi. Qonun nafaqat davlat organlari, balki barcha fuqaroga ham o'z axborot xavfsizligini ta'minlashda mas'uliyat yuklaydi. Huquqshunoslar tomonidan ushbu qonunning dolzarbligi va amaliy o'rni yuqori baholanadi.

O'zbekiston Respublikasi tomonidan qabul qilingan ushbu qonunlar kiber huquqiy infratuzilmani rivojlantirish, raqamli xavfsizlikni ta'minlash, fuqarolarning axborot huquqlarini himoya qilish va raqamli iqtisodiyotga o'tish jarayonini huquqiy jihatdan qo'llab-quvvatlashda hal qiluvchi rol o'ynaydi. Huquqshunoslar tomonidan ham yuqori baholangan ushbu qonunlar nafaqat zamonaviy axborot texnologiyalariga moslashuv, balki ularning xavfsiz va huquqiy jihatdan asosli foydalanilishini ta'minlovchi poydevor sifatida xizmat qilmoqda.

2020-yilda O'zbekistonda axborot texnologiyalari sohasida milliy xavfsizlikni ta'minlashga qaratilgan maxsus strategiya ishlab chiqildi. Bunda davlat va xususiy sektor o'rtasidagi hamkorlikka alohida e'tibor qaratildi. Ushbu

2022–2026-yillarga mo'ljallanib o'zbekistonning axborot suverenitetini mustahkamlash, kritikal axborot infratuzilmalari xavfsizligini oshirish, kiberxavfsizlik bo'yicha xalqaro hamkorlikni kengaytirish kabi yo'nalishlarni rivojlantirish uchun qaratilgan hisoblanadi. O'zbekiston Respublikasining Raqamli O'zbekiston 2030 strategiyasi raqamli iqtisodiyotni rivojlantirish, davlat boshqaruvini raqamlashtirish va xavfsiz raqamli infratuzilmani yaratishni, Axborot tizimlari va ma'lumotlar bazalarini himoya qilish, davlat organlarining IT infratuzilmasida xavfsizlik standartlarini joriy etish, kiberxavfsizlik bo'yicha mutaxassislar tayyorlash kabi muhim masalalarni o'z ichiga oladi.

O'zbekiston Respublikasi Davlat xavfsizlik xizmati raisining 22.09.2023 yilda ro'yxatdan o'tgan buyrug'iga asosan O'zbekiston Respublikasi kiberxavfsizlik va muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta'minlash darajasini baholash

tartibi to'g'risidagi nizomi qabul qilingan. Mazkur Nizom O'zbekiston Respublikasi kiberxavfsizlik va muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta'minlash darajasini baholash (bundan buyon matnda baholash deb yuritiladi) tartibini belgilaydi.

Global raqamli transformatsiya jarayonida O'zbekiston Respublikasi ham axborot texnologiyalaridan keng foydalanish orqali davlat boshqaruvi, iqtisodiyot, ta'lim va sog'liqni saqlash kabi muhim sohalarni raqamlashtirishga katta e'tibor qaratmoqda. Shu bilan birga, bu jarayonlar bilan birga kiber xavfsizlik, shaxsiy ma'lumotlarni himoya qilish, raqamli identifikatsiya va axborot erkinligini tartibga soluvchi kiber huquqiy muhitning mukammalligi dolzarb masalaga aylanmoqda. Aynan ushbu asosiy tahdidlar va bo'shliqlar yoritib o'tiladish otish ushbu kamchiliklarni oldini olish ushun kiberxavfsizlik chorasi sifatida xizmat qilishi mumkin.

O'zbekistonda kiberxavfsizlikni ta'minlovchi asosiy organlar jumlasiga Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi, Milliy CERT, DXX, IIV, hamda Davlat raqamli texnologiyalar markazi kiradi. Biroq bu organlar o'rtasida institutsional aloqalar asosan epizodik va loyihaviy shaklda, yani muntazam emas. Ushbu muammolarning sabablari tashkilotlar o'rtasida ruxsatsiz ma'lumot almashishdan qo'rquv mavjudligi hisoblanadi. Bunga asosiy sabab qulay bo'lgan mexanizmlarni ishlab chiqilmaganligi. Kiberhujumlar haqida xabar berish tizimi normativ-huquqiy jihatdan majburiy emas. Ko'p hollarda kiber tahdidlar haqida xabardorlik ichki darajada qolib ketadi.

O'zbekistonda ma'lumot almashinuvi va interoperabilitetning past darajada ekanligini kuzatish mumkin. Hozirda O'zbekistonda ishonchli va avtomatlashtirilgan ma'lumot almashinuvi uchun to'liq shakllangan standartlar va texnik platformalar mavjud emas. Buning asosiy sabablari hozirgi kunda mavjud davlat axborot tizimlarining aksariyati yopiq va o'zaro bog'lanmagan. Tizimlararo API va standart protokollar orqali ma'lumot almashish faqat yirik loyiha doirasida amalga oshirilib, xavfsizlik nuqtai nazaridan differensial ruxsatnoma siyosati keng joriy etilmaganligiga olib kelmoqda. Ushbu muammolardan tashqari O'zbekistonda davlat va xususiy sektor o'rtasidagi munosabatlar hozirgi kun talablariga taqqoslab qaraganda davlat va xususiy sektor o'rtasidagi munosabatlar juda zaif hisoblanadi. Ushbu hamkorliklar strategik va muvofiqlashtirilgan shakllanmagan.

Kiberjinoyatchilikka qarshi kurashda eng murakkab muammolardan biri ushbu turdagi jinoyatlarning virtual muhitda va istalgan hududdan sodir etilishi imkoniyatining mavjudligi hisoblanadi. Aksariyat hollarda tashqi xavflar manbai O'zbekiston Respublikasi qonunchiligi yurisdiksiyasi doirasiga kirmaydi. Bu esa huquqiy choralar tizimini qo'llashni muayyan darajada murakkablashtiradi. Kiberjinoyatchilar, odatda, milliy chegaralarni chetlab o'tgan holda, jahon tarmog'iga ulangan har qanday kompyuterga, elektron dasturga hujum qiladi. Yoki go'yo boshqa manbalar yoxud bunday xatti-harakatlar jinoyat hisoblanmaydigan mamlakatdan turib shunday hujumni amalga oshiradi. Bu esa qator huquqiy ziddiyatlarni keltirib chiqarmoqda.

Mazkur bobdan xulosa qiladigan bo'lsak kiber xavflar globallashib borayotganini e'tiborga oladigan bo'lsak, bugun hech qaysi mamlakat ushbu xavfga nisbatan mustaqil ravishda bir o'zi qarshilik ko'rsata olmaydi. Shu sababdan kiberjinoyatchilik muammosi jahon hamjamiyatini unga qarshi kurashish yuzasidan zarur choralar ko'rishga undamoqda. Bunday sharoitda O'zbekistonda xalqaro hamkorlikni kengaytirish, kiberjinoyatchilikka qarshi birgalikda harakat qilish va uni tekshirish borasida tegishli organlar faoliyatini tartibga solish hamda o'zaro hamkorlikning xalqaro huquqiy mexanizmlariga qo'shilishi kerak.

XULOSA

O'zbekiston Respublikasida kiber huquqiy infratuzilma shakllanish bosqichida bo'lib, mavjud qonunlar bilan bir qatorda, yangi tahdid va zamonaviy texnologiyalarni hisobga olgan holda yangi huquqiy tartibotlarni ishlab chiqish zarurati ortib bormoqda. Mavjud bo'lgan bo'shliqlarni bartaraf etish va kiber xavfsizlikni kuchaytirish uchun qonunlar va huquqiy tashabbuslar qabul qilinishi lozim.

Birinchidan, 2022-yil 15-aprelda qabul qilingan O'zbekiston Respublikasining O'RQ-764-sonli "Kiberxavfsizlik to'g'risida"gi qonuni mavjud. Biroq ushbu qonun kiber huquq sohasida davlat, biznes va jismoniy shaxslar uchun kiber xavfsizlik standartlari, raqamli hujumlar va ularning oqibatlariga nisbatan javobgarlik choralari, kiber xavfsizlik bo'yicha favqulodda holat tartibi, kiber xavfsizlikka oid tahdidlar ro'yxatini yuritish va maxsus vakolatli organ faoliyati kabi masallarni to'la tartibga soluvchi tartiblar mavjud hozircha emas. Agar rivojlangan davlatlar yani Estoniya, Isroil va Janubiy Koreya bu borada alohida qonunlar va agentliklarga ega bo'lib, ularning samaradorligi hozirgi kunda ancha yuqori hisoblanadi.

Ikkinchidan, Aynan hozirgi kunga kelib jamiyatda suniy intellektning o'rni, uning qo'llanish sohalari kengayib bormoqda, biroq hozircha O'zbekiston qonunchiligida sun'iy intellekt texnologiyalaridan foydalanish, etik me'yorlar, javobgarlik va ularni nazorat qilish masalalari to'liq tartibga solinmagan. Albatta bu holatni ko'pgina rivojlangan davlatlarda ham kuzatish mumkin, biroq ushbu sohani tezroq tartibga solish kelgusida vujudga kelishi mumkin bo'lgan ko'pgina salbiy oqibatlarni oldini olgan bo'lar edi.

Yangi qonun sun'iy intellekt asosida ishlovchi tizimlarning huquqiy maqomi, algoritmik qarorlarning shaffofligi va inson nazorati, etik prinsiplar va inson huquqlarini hurmat qilish talablar va eng asosiysi sun'iy intellekt tomonidan yetkazilgan zarar uchun javobgarlik masalalarini o'z ichiga olishi kerak.

Kiberjinoyatchilikning oldini olish va javobgarlik masalasi bo'yicha xorijiy davlatlar tajribasini o'rganib, kiber jinoyatlarning turlariga qarshi kurashishga qaratilgan qat'iy qonunlarini aks ettirilishi lozim. Ko'plab davlatlar hozirda o'zlarining Jinoyat kodekslariga kiberjinoyatlar bo'yicha maxsus bo'limlar yoki moddalarni qo'shishgan. Bu normativ-huquqiy bazaning samaradorligi kiberjinoyatchilikni jazolash va oldini olishni yanada takomillashtirishga xizmat qiladi. Masalani misol sifatida Daniya Jinoyat kodeksining 279-

moddasi olib qaraganda, ushbu modda kompyuter firibgarligiga qarshi kurashish uchun mo'ljallangan. Bu ayniqsa, onlayn firibgarlikni va virtual muhitda noqonuniy operatsiyalarni taqiqlaydi. Bundan tashqari Fransiya Jinoyat kodeksining 263-moddasi kompyuter orqali amalga oshirilgan jinoyatlarni, masalan, dasturiy ta'minotlar orqali noqonuniy faoliyatni jazolashni ko'zda tutadi. Hozirgi kunda onlayn yo'l bilan pul o'g'irlash, noqonuniy operatsiyalarni amalga oshirishga, oddiy o'g'irlik sifatidan qarashimiz noto'g'ri hisoblanadi. Shu sababdan jinoyat ko'dekisiga yanada yangi o'zgarishlar ilib kirish kerak.

Kiberjinoyatlar soni va miqdorini kamaytirish uchun qaysi kiberhujumlarga og'irroq jazo belgilanishi bo'yicha ro'yxat ishlab chiqilishi va u amaliyotga tatbiq etilishi zarur. O'zbekiston huquq sohasida ko'pgina islohotlar olib borishi kerak buing asosiy sababi ko'pgina konvensiyalar, haqaro tashkilotlarga qo'shilish uchun yuridik majburiyatlar va o'zaro huquqiy aloqalarni ta'minlashni talab qiladi, va bu ba'zi hollarda mavjud huquqiy tizimga qiyinchilik tug'dirishi mumkin. Ayni damda O'zbekiston xalqro konvensiyasiga qo'shilish va yangi kelishuvlar tuzish choralari yanada tezlashtirishi zarur. Buning asosiy sababi, kiber havflarning oldini olishning xalqaro hamkorliksiz iloji yo'qligida. Xalqaro hamkorlik kiberjinoyatchilikka samarali qarshi kurashishga yordam beradi. Bunday holatda esa kiber havflar oldida biz manashunday ustunlikga erishgan bo'lamiz. Albatta O'zbekiston hozirga qadar ko'pgida davlatlar, jumladan MDH davlatlari o'rtasida kelushuvlar imzolangan bo'lsada, axborot almashinuvi borasida funksional hamkorlik mavjud emas. Milliy qonunlar kompyuter jinoyatlariga qarshi kurashishda yetarli emas, chunki bu jinoyatlar ko'pincha davlatlararo tusga ega bo'ladi. Shu sababli xalqaro hamkorlik shartdir.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1.1. O'zbekiston Respublikasi Prezidenti Shavkat Mirziyoyevning Shanxay hamkorlik tashkiloti Davlat rahbarlari kengashi majlisidagi "jadallashtirilgan raqamli transformatsiya" yuzasidan nutqi//uzbekistan.org 2024 4-Iyul

1.2. Sh.M.Mirziyoyev.O'zbekiston Respublikasi Konstitusiyasi qabul qilinganining 24 yilligiga bag'ishlangan tantanali marosimdagi "Qonun ustuvorligi va inson manfaatlarini ta'minlash yurt taraqqiyoti va xalq farovonligining garovi"nomli ma'ruzasi // Xalq so'zi. 2016-yil 8-dekabr.

II. Xalqaro hujjatlar

2.1. BMT kiberjinoyatchilikka qarshi ilk global konvensiyasi, 8 avgust 2024

Council of Europe - Convention on Cybercrime (Budapesht konvensiyasi), 2001

2.2. APEC – Working Group Action Plan, 2010–2015

2.3. WSIS – Geneva Declaration of Principles, 2003

2.4. Arab Ligasi – Arab Convention on Combating Information Technology Offences, 2010

2.5. Mustaqil Davlatlar Hamdo'stligi – Agreement on Cooperation in Combating Offences Related to Computer Information, 2001

2.6. World Summit on the Information Society (WSIS). (2003). Geneva Declaration of Principles. Jeneva.

2.7. Council of Europe. (2003). Second Additional Protocol to the Convention on Cybercrime, concerning the enhanced cooperation and disclosure of electronic evidence (CETS No. 224). Strasbourg.

2.8. Singapore. (2018, 31 avgust). Cybersecurity Act 2018 (Act No. 9 of 2018). Singapore Statutes Online.

III. Normativ huquqiy hujjatlar

3.1. O'zbekiston Respublikasining Konstitusiyasi // Qonun hujjatlari ma'lumotlari milliy bazasi, 30.04.2023 y.

3.2. O'zbekiston Respublikasining Jinoyat kodeksi, O'zbekiston Respublikasi Oliy Kengashining Axborotnomasi, 1995-y.

3.3. O'zbekiston Respublikasining ma'muriy javobgarlik to'g'risidagi kodeksi, O'zbekiston Respublikasi Oliy Kengashining Axborotnomasi, 1995-y.

3.4. O'zbekiston Respublikasining "Elektron raqamli imzo to'g'risida" Qonuni, Qonunchilik ma'lumotlari milliy bazasi, 13.10.2022-y.

3.5. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida" Qonuni, Qonunchilik ma'lumotlari milliy bazasi, 16.04.2022-y.

3.6. O'zbekiston Respublikasining "Axborotlashtirish to'g'risida" qonuni, O'zbekiston Respublikasi Oliy Majlisining Axborotnomasi, 2004-y.

3.7. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida" Qonuni, Qonunchilik ma'lumotlari milliy bazasi, 16.04.2022-y.

3.8. O'zbekiston Respublikasining "Reklama to'g'risida" Qonuni, Qonunchilik ma'lumotlari milliy bazasi, 08.06.2022-y.

3.9. O'zbekiston Respublikasining "Shaxsga doir ma'lumotlar to'g'risida" Qonuni, Qonun hujjatlari ma'lumotlari milliy bazasi, 03.07.2019-y.

3.10. O'zbekiston Respublikasining "Axborot erkinligi prinsiplari va kafolatlari to'g'risida" qonuni, O'zbekiston Respublikasi Oliy Majlisining Axborotnomasi, 2003-y.

3.11. O'zbekiston Respublikasi Prezidentining "Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirishga oid qo'shimcha chora-tadbirlar to'g'risida" Qarori, Qonun hujjatlari ma'lumotlari milliy bazasi, 16.09.2019-y.

3.12. O'zbekiston Respublikasi Prezidentining "Raqamli iqtisodiyot va elektron hukumatni keng joriy etish chora-tadbirlari to'g'risida" Qarori, Qonun hujjatlari ma'lumotlari milliy bazasi, 29.04.2020-y.

3.13. O'zbekiston Respublikasi Prezidentining "Raqamli iqtisodiyot va elektron hukumatni keng joriy etish chora-tadbirlari to'g'risida" Qarori, Qonun hujjatlari ma'lumotlari milliy bazasi, 29.04.2020-y

3.14. O'zbekiston Respublikasi Prezidentining "Raqamli O'zbekiston — 2030" strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to'g'risida Farmoni, Qonun hujjatlari ma'lumotlari milliy bazasi, 06.10.2020-y.

IV. Maxsus adabiyotlar

- 4.1. Kiber huquq – huquq sohasi sifatida: risola / tuzuvchilar R.R.Shakurov, M.M.Vohidov. – Toshkent: O'zbekiston Respublikasi Adliya vazirligi qoshidagi.
- 4.2. Gulyamov S. "Kiber huquq: nazariy va amaliy masalalar", Toshkent, 2023-yil
- 4.3. S.S.Niyozova – Kiberjinoyatchilik, o'quv qo'llanma. TDYU nashriyoti, 2024.
- 4.4. Yuristlar malakasini oshirish markazi, 2022 Islombek Abdixakimov Kiber huquq kafedrası o'qituvchisi, Toshkent davlat yuridik universiteti, Raqamli iqtisodiyotda - Raqamli jinoyatlar maqolasi. Elita.uz
- 4.5. P.B.Olim o'g'li - Kiber jinoyatchilikka qarshi immunitet hosil qilish masalalari
- 4.6. Кибербезопасность и информационная безопасность Демаркация правовых категорий. Баландин А.Ю.
- 4.7. Защита в цифровую эпоху: значение и важность страхования от киберпреступности. Ш.Абдуллаев
- 4.8. Brenner, S. W. (2010). Cybercrime: Criminal threats from cyberspace. Santa Barbara.
- 4.9. Простосердов М.А. Экошические преступления, совершаемые киберпространстве, и меры противодействия
- 4.10. Salaev N.S., Ro'ziev R.N. Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar. Monografiya., – T.: TDYU, 2018.
- 4.11. Geist, M. A. Law, Privacy and the Internet. - Ottawa: University of Ottawa, 2020
- 4.12. Edwards, L. Cyberlaw: The Intersection of Technology and Law. Newcastle: Newcastle University Press, 2020
- 4.13. Mitnick, K. D., & Simon, W. L. (2002). The Art of Deception: Controlling the Human Element of Security. Indianapolis: Wiley Publishing
- V. Internet veb-saytlari
- 5.1 <https://www.lex.uz/>
- 5.2 <https://cyberleninka.ru/>
- 5.3 <https://forbiddenstories.org/>
- 5.4 <https://kun.uz/>
- 5.5 <https://stat.uz/uz/>
- 5.6. <https://daryo.uz/2022/06/16/songgi-3yilda-kiberjinoyatlar-soni-bir-necha-baravarga-oshib-ketdi-iiv>
- 5.7. <https://csec.uz/uz/news/maqolalar/2022-yil-uchun-asosiy-kiberxavfsizlik-tahdidlari-bashorati>
- 5.8 <https://xabar.uz/uz/post/ozbekistonda-kiberxavfsizlik-strat>
- 5.9 <https://www.gazeta.uz/oz/2022/08/06/kiberxavfsizlik>
- 5.10 <https://e-gov.uz/news/ozbekistonda-kiberxavfsizlik-boyicha-2021-yilgi-hisobot-taqdim-etildi-298>

5.11 <https://infocom.uz/articles/kiberhujumlarga-qarshi-kurash-strategiyalari>

5.12 <https://www.smartnation.gov.sg/>