INTERNET OLAMIDA SHAXSIY MA'LUMOTLARNI HIMOYA QILISH

Toxirov Zuxriddin Anvar o'g'li
zuhriddintohirov5@gmail.com
Toshkent davlat yuridik universiteti talabasi
https://doi.org/10.5281/zenodo.20050833

Annotatsiya: Hozirgi rivojlanib borayotgan internet olamida shaxsiy ma'lumotlarga nisbatan tahdidlar kundan kunga ortib bormoqda va buning natijasida odamlar o'z shaxsiy ma'lumotlarini himoya qilishdagi huquqlaridan foydalanishda qiyinchiliklarga duch kelishmoqda. Shuningdek, odamlar internetdan foydalanishda o'z shaxsiy ma'lumotlarini qanday himoya qilish va shaxsiy ma'lumotlarini himoya qilishda qanday huquqlarga ega ekanligini bilishi lozim. Chunki, har qanday shaxs internet olamidagi o'z shaxsiy ma'lumotlarini himoya qilishdagi huquqlari haqida ma'lumotga ega bo'lsa, bu shaxsiy ma'lumotlarga nisbatan tahdidlarni oldini olishga yordam beradi va har bir shaxs o'ziga tegishli bo'lgan har qanday shaxsiy ma'lumotlarini himoya qilishdagi vositalardan foydalanish imkoniyatini vujudga keltiradi. Shu bois ushbu maqolada internet olamida shaxsiy ma'lumotlarni himoya qilishning turlari, shaxsiy ma'lumotlarni himoya qilishdagi davlatlarning roli, odamlarning internet olamidagi o'z shaxsiy ma'lumotlarini himoya qilishda qanday huquqlarga ega ekanligi va internet olamida shaxsiy ma'lumotlarga qilinayotgan tahdidlarni oldini olish maqsadida amalga oshirilayotgan sa'y-harakatlar haqida so'z boradi.

Kalit so'zlar: shaxsiy ma'lumot, ma'lumotlar maxfiyligi, kiberxavfsizlik, kiberjinoyat, texnik himoya, huquqiy himoya, shaxsiy ma'lumotlarni himoya qilishda qonunchilik, unutilish huquqi, shaxsiy ma'lumotlarni himoya qilishda xalqaro hamkorlik.

I.KIRISH

Bugungi raqamli davrda internet hayotimizning ajralmas qismiga aylanib bormoqda va shu bilan birga inson hayotining deyarli barcha jabhalariga muhim ta'sir ko'rsatmoqda. Shuningdek, internet foydalanuvchilari o'zlari haqidagi shaxsiy ma'lumotlarini ixtiyoriy yoki o'zlari bilmagan holda internet tarmoqlarida qoldirishadi. Buning natijasida shaxsiy ma'lumotlarni himoya qilish masalasi yuzaga chiqadi. Chunki, hozirda ko'plab mamlakatlar shaxsiy ma'lumotlarni himoya qilishda noqonuniy ravishda saqalash, yig'ish va tarqatish kabi turli xil kiber tahdidlarga duch kelishmoqda. Ushbu tahdidlarga qarshi davlatlar va yirik kompaniyalar (Google, Apple, Facebook) shaxsiy ma'lumotlarni himoya qilishda turli xil qonuniy va texnologik vositalarni ishlab chiqmoqda. Biroq, internet olamida kiberjinoyatchilikning rivojlanib borishi, shaxsiy ma'lumotlarni himoya qilishdagi mavjud choralarni yetarli darajada samarali ekanligini oqlamaydi. Shuning uchun, rivojlanib borayotgan raqamli dunyoda internet olamida shaxsiy ma'lumotlarni himoya qilish kabi dolzarb masalalar yuzaga chiqadi. Internet olamida shaxsiy ma'lumotlarni himoya qilish mavzusining maqsadi, vazifasi, tadqiqot bo'shlig'i va tadqiqotning ahamiyatiga to'xtalib o'tsak. Internet olamida shaxsiy ma'lumotlarni himoya qilish mavzusining maqsadi hozirgi davrda insonlar tomonidan foydalanib kelinayotgan internet tarmoqlarida ularning shaxsiy ma'lumotlariga bo'lgan huquqlarini ta'minlash, internet va insonlar o'rtasida vujudga keladigan shaxsiy ma'lumotlarga aloqador munosabatlarni tartibga solish, internet olamida shaxsiy ma'lumotlarga nisbatan sodir etilayotgan kiber tahdidlarni tahlil qilish va internet olamida

shaxsiy ma’lumotlarni himoya qilishga doir muhim muammolarga yechib izlashdan iborat. Ushbu mavzuning vazifalari quyidagilardan iborat: internet olamida shaxsiy ma’lumotlarni himoya qilishga oid amalga oshirilayotgan harakatlarni va shaxsiy ma’lumotlarga tahdid soluvchi xavf-xatarlarni tahlil qilish, shaxsiy ma’lumotlarni himoya qilish usullarini o’rganish, internet olamida shaxsiy ma’lumotlarni himoya qilishda xalqaro va milliy darajadagi qonunchiliklarni tahlil qilish va shaxsiy ma’lumotlarni himoya qilish bo’yicha samarali vositalarni tavsiya qilish. Hozirgi kunga kelib internet olamida shaxsiy ma’lumotlarni himoya qilish borasida turli xil ilmiy va amaliy tadqiqotlar olib borilgan bo’lsada, ushbu yo’nalishdagi kiber tahdidlarning rivojlanib borishi tufayli shaxsiy ma’lumotlarni himoya qilishdagi chora-tadbirlar o’z kuchini yuqotib bormoqda. Shuningdek, internet olamidagi shaxsiy ma’lumotlarni himoya qilishga oid izlanishlar yetarlicha o’rganilmagan. Shu bois, ushbu maqolaning tadqiqoti raqamli davrda samarali vositalar yordamida shaxsiy ma’lumotlarni himoya qilishning zamonaviy usullarini taklif qilishga qaratilgan.

II.METODLAR

Mazkur maqolada, internet olamida insonlarning shaxsiy ma’lumotlarini himoya qilishdagi bir qancha tushunchalarni (shaxsiy ma’lumotlar, ma’lumotlar maxfiyligi) tahlil qilish bilan birga, internet olamida insonlarning shaxsiy ma’luotlarini himoya qilishning texnik va huquqiy himoyasining turlari, shaxsiy ma’lumotlarni himoya qilishda davlatlarning roli, insonlar internet tarmoqlardagi o’z shaxsiy ma’lumotlarini himoya qilishda qanday huquqlarga ega ekanligi va internet olamida shaxsiy ma’lumotlarga nisbatan sodir etilayotgan tahdidlarga qarshi qanday harakatlar olib borilayotganligi haqida ma’lumot berib o’tiladi. Shuningdek, ushbu tadqiqot davomida quyidagi masalalar tahlil qilindi: qanday ma’lumotlar shaxsiy ma’lumot hisoblanadi, ma’lumotlar maxfiyligi, shaxsiy ma’lumotlarni boshqarish huquqi, internet olamida shaxsiy ma’lumotlarni himoya qilishda unutilish huquqi nima ekanligi, shaxsiy ma’lumotlarga nisbatan sodir etiladigan tahdidlar, shaxsiy ma’lumotlarni himoya qilishda texnik va huquqiy himoya choralari, kiberjinoyat va kiberxavfsizlik tushunchalari, internet olamidagi shaxsiy ma’lumotlarni himoya qilishda davlatlarning roli va xalqaro hamkorlik. Ushbu tadqiqotning manbasi sifatida, internet olamida shaxsiy ma’lumotlarni himoya qilishga oid ilmiy maqolalar, adabiyotlar, shaxsiy ma’lumotlarni himoya qilishda olib borilayotgan sa’y-harakatlar haqida hisobotlar, kiberjinoyat va kiberxavfsizlikka oid statistik ma’lumotlar, internet olamida shaxsiy ma’lumotlarni himoya qilishda davlatlarning olib borayotgan harakatlariga oid hisobotlar va statistik ma’lumotlar, davlatlar va davlatlar o’rtasidagi xalqaro hamkorlik orqali internet olamida insonlarning shaxsiy ma’lumotlarini himoya qilishga oid ishlab chiqgan samarali vositalari va qonun hujjatlari. Tahlil usuli, internet olamida shaxsiy ma’lumotlarni himoya qilishning texnik va huquqiy himoya choralarini tahlil qilish, shaxsiy ma’lumotlarni himoya qilishda insonlarning huquqlari va ular bilishi kerak bo’lgan ko’nikmalarni tadqiq qilish, internet tarmoqlardagi shaxsiy ma’lumotlarga nisbatan sodir etilayotgan tahdidlarni va ularning oqibatlarini o’rganish, kiberjinoyat va kiberxavfsizlikka oid statistik ma’lumotlardan foydalanish, internet olamida shaxsiy ma’lumotlarni himoya qilishda davlatlarning roli va xalqaro hamkorlikning ta’sirlarini tahlil qilish kabi metodlardan foydalaniladi.

III.NATIJALAR

Tadqiqot natijasiga keladigan bo'lsak, bugungi raqamli davrda har bir inson o'z ehtiyojlariga ko'ra internet tarmoqlaridan foydalanib keladi. Ammo, insonlar internet tarmoqlaridan foydalangan payt internet tarmog'idagi saytlar tomonidan foydalanuvchining ma'lumotlari saqlanib qolinishi ehtimoli yuzaga keladi. Buning natijasida, foydalanuvchining shaxsiy ma'lumotlari boshqa insonlarga ma'lumot egasining roziligisiz o'tishi mumkin va ushbu holatda foydalanuvchining shaxsiy ma'lumotlariga nisbatan huquqlari buzilishi mumkin. Ushbu holatda qanday ma'lumotlar shaxsiy ma'lumotlar ekanligini bilishimiz lozim.

"Shaxsiy ma'lumotlar" bu identifikatsiya qilingan yoki aniqlanishi mumkin bo'lgan jismoniy shaxsga tegishli har qanday ma'lumotni anglatadi (ma'lumotlar subyekti); identifikatsiya qilinadigan jismoniy shaxs to'g'ridan-to'g'ri yoki bilvosita, xususan identifikatorga, masalan, ism, identifikatsiya raqami, joylashuv ma'lumotlari, onlayn identifikator yoki ushbu jismoniy shaxsning jismoniy, fiziologik, genetik, aqliy, iqtisodiy, madaniy yoki ijtimoiy identifikatoriga xos bo'lgan bir yoki bir nechta omillarga murojaat qilish orqali aniqlanishi mumkin bo'lgan shaxsdir;(General Data Protection Regulation, 2018, Article 4).

"Ma'lumotlar maxfiyligi" bu insonlarning shaxsiy yoxud muhim ma'lumotlarini ko'rish uchun ruxsat etilmagan shaxslar yoki tizimlar tomonidan ko'rilishi, o'g'irlanishi va oshkor etilishidan himoyalanganligini anglatadi. Shuningdek, ushbu tushunchaning boshqa ma'nosi ham mavjud, ya'ni, internetdagi ma'lumotlarga faqat ma'lumot egasi tomonidan ruxsat etilgan shaxslar va tizimlarning kirishi mumkinligi tushuniladi.

Ma'lumotlar maxfiyligi bo'yicha muammolar:

Internetdan foydalanish jarayonida foydalanuvchilar ko'plab shaxsiy ma'lumotlarini oshkor qilishadi. Bular orasida ism, manzil, elektron pochta, telefon raqami, hatto moliyaviy ma'lumotlar, tibbiy yozuvlar va geolokatsiya ma'lumotlari ham bo'lishi mumkin. Bu ma'lumotlar ko'pincha onlayn xaridlar, ijtimoiy tarmoqlar, mobil ilovalar va veb-brauzerlar orqali yig'iladi.

Internet olamida shaxsiy ma'lumotlarni himoya qilishda xavotirga sabab bo'ladigan holatlardan ba'zilari quyidagilar:

- **Roziliksiz ma'lumot yig'ish:** Ko'plab veb-saytlar foydalanuvchining aniq roziligisiz shaxsiy ma'lumotlarini to'playdi.
- **Ma'lumotlarni uchinchi shaxslarga uzatish:** Tashkilotlar to'plangan ma'lumotlarni boshqa kompaniyalarga sotishi yoki almashishi mumkin.
- **Ma'lumotlar xavfsizligining buzilishi:** Xakerlik yoki texnik nosozliklar natijasida foydalanuvchining maxfiy ma'lumotlari oshkor bo'lishi mumkin.
- **Kuzatuv va profil tuzish:** Onlayn faoliyatni kuzatish orqali kompaniyalar foydalanuvchilarning shaxsiy profillarini yaratishadi, bu esa maxfiylikni buzadi. (Winnie Chung and John Paynter, 2002).

Kiberjinoyat- bu kompyuter, kompyuter tarmog'i yoki tarmoqqa ulangan qurilmaga qaratilgan yoki undan foydalanadigan jinoiy faoliyat. Aksariyat kiberjinoyatlar pul ishlashni xohlaydigan kiberjinoyatchilar yoki xakerlar tomonidan sodir etiladi. Biroq, ba'zida kiber jinoyatlar foydadan tashqari boshqa sabablarga ko'ra kompyuterlar yoki tarmoqlarga zarar yetkazishni maqsad qiladi. Bu siyosiy yoki shaxsiy bo'lishi mumkin. **Kiberjinoyatlarning o'sishining turli sabablari quyidagilar hisoblanadi.** Samarali xavfsizlik choralari va

yechimlarining yo'qligi kiberjinoyatchilar uchun oson nishon bo'lgan zaif qurilmalarning keng doirasini taqdim etadi. Kiberjinoyatchilar va xakerlik guruhlarining eng keng tarqalgan motivatsiyasi, bugungi kunda aksariyat hujumlar undan foyda olishga qaratilgan.(Cyber Talents,2025). 2025-yil fevral holatiga koʻra, dunyo boʻylab 5,56 milliard kishi internet foydalanuvchisi boʻlgan, bu butun dunyo aholisining 67,9 foizini tashkil qiladi.(Statista, 2025). Kiberjinoyatlar xilma-xil boʻlib, huquqbuzarlik xususiyatiga koʻra turlarga boʻlinishi mumkin.

Xakerlik - bu ruxsatsiz shaxslarning kompyuter tizimlari, tarmoqlari yoki ma'lumotlariga kirishi orqali zarar yetkazishga qaratilgan noqonuniy faoliyatdir. Ushbu harakatlar natijasida maxfiy ma'lumotlar oʻgʻirlanishi, tizimlarning ishdan chiqishi yoki shaxsiy hayot daxlsizligining buzilishi mumkin. Xakerlar tizimga kirish uchun fishing elektron xatlari, zararli dasturlar (malware) va dasturiy ta'minotdagi zaifliklardan foydalanadilar. Ularning maqsadlari turlicha boʻlishi mumkin: moliyaviy foyda, sanoat yoki siyosiy josuslik. Eng koʻp uchraydigan xakerlik usullariga, xizmat koʻrsatishni rad etish (DDoS) hujumlari va "man-in-the-middle" (oʻrtadagi vositachi) hujumlari kiradi.

Shaxsni oʻgʻirlash - bu boshqa bir shaxsning shaxsiy ma'lumotlarini firibgarlik yoki boshqa jinoyatlarda foydalanish maqsadida oʻzlashtirishdir. Ushbu holat jabrlanuvchiga moliyaviy zarar, obroʻsiga putur yetishi, ruhiy bosim va hatto huquqiy muammolarni keltirib chiqarishi mumkin. Kiberjinoyatchilar bu ma'lumotlarni fishing xabarlari, ma'lumotlar bazasining buzilishi yoki zararli dasturlar orqali qoʻlga kiritadilar. Shaxsiy ma'lumotga ega boʻlgan jinoyatchi uning yordamida kredit olish, bank hisoblarini ochish yoki jabrlanuvchining nomidan noqonuniy harakatlar qilish imkoniyatiga ega boʻladi. Bu holat, bir qancha yirik korxonalarga ham katta moliyaviy va uning imijiga zarar yetkazishi mumkin.

Fishing - bu internet foydalanuvchilarini oʻz ixtiyori bilan maxfiy ma'lumotlarni (masalan, parollar yoki bank rekvizitlari) taqdim etishga chalgʻitish maqsadida ishlab chiqilgan firibgarlik usulidir. Jinoyatchilar koʻpincha oʻzlarini ishonchli tashkilot vakili sifatida koʻrsatib, yolgʻon elektron xatlar yoki soxta veb-saytlar orqali foydalanuvchilarni aldashadi. Fishingdan himoyalanish uchun foydalanuvchilar elektron xabarlarning manbasini diqqat bilan tekshirishi, noma'lum havolalarni bosmasligi va qurilmalarda kiberxavfsizlik dasturlarini muntazam yangilab turishi zarur.

Onlayn firibgarlik - bu internet orqali shaxslar yoki tashkilotlarni aldash orqali moliyaviy foyda yoki muhim ma'lumotlarni qo'lga kiritib olishga qaratilgan kiberjinoyatdir. Bunga investitsiya firibgarliklari, fishing orqali ma'lumot yigʻish, va soxta onlayn savdo platformalari kiradi. Ushbu firibgarliklar koʻpincha ishonchli koʻrinishga ega boʻlib, foydalanuvchilarning moliyaviy operatsiyalarini amalga oshirishiga yoki maxfiy ma'lumotlarini oshkor qilishiga sabab boʻladi. Bunday holatlardan himoyalanish uchun foydalanuvchilar elektron xatlarning haqiqatligini tekshirishi, veb-saytlarning ishonchliligini baholashi, va bank hisoblaridagi har qanday oʻzgarishlarni doimiy ravishda nazorat qilib borishi lozim.

Zararli dasturiy ta'minot (malware) hujumlari - bu kompyuter tizimlariga zarar yetkazish, ma'lumotlarni oʻgʻirlash yoki ularning ish faoliyatini buzish maqsadida ishlab chiqilgan zararli dasturlardan foydalanishdir. Malware turlariga viruslar, qurtlar (worms), toʻlov dasturlari (ransomware), josuslik dasturlari (spyware) va reklama dasturlari (adware) kiradi. Bunday hujumlar koʻpincha dasturiy ta'minotdagi zaifliklar yoki foydalanuvchilarni aldash orqali, ya'ni ijtimoiy muhandislik (social engineering) usullari orqali amalga oshiriladi.

Natijada moliyaviy yo‘qotishlar, obro‘ga putur yetishi va jismoniy shaxslar hamda tashkilotlar uchun huquqiy oqibatlar yuzaga kelishi mumkin. Zararli dasturlarning xavfini kamaytirish uchun quyidagi choralarning ahamiyati katta: operatsion tizim va dasturlarni muntazam yangilab borish, kuchli va murakkab parollarni qo‘llash, ishonchli antivirus dasturlaridan foydalanish.

Xizmat ko‘rsatishni rad etish (Denial of Service - DoS) hujumlari - bu ma'lum bir server, tarmoq yoki veb-saytga ortiqcha trafik yuborish orqali uning normal faoliyatini izdan chiqarishga qaratilgan kiberhujum turidir. Buning natijasida xizmat sekinlashadi, to‘liq ishlamay qoladi yoki foydalanuvchilar uchun mavjud bo‘lmay qoladi. Ushbu hujumlar odatda buzilish keltirib chiqarish, qasos olish, moliyaviy manfaat olish yoki raqobatchilarga zarar yetkazish maqsadida amalga oshiriladi. Ayniqsa, internet orqali xizmat ko‘rsatadigan korxonalar bunday hujumlarga nisbatan juda zaif hisoblanadi. Xizmatning to‘xtashi ularning moliyaviy yo‘qotishlariga, mijozlar ishonchini yo‘qotishiga va brend obro‘sining pasayishiga olib kelishi mumkin. Xizmat ko‘rsatishni rad etish (Denial of Service - DoS) hujumlaridan himoyalanish uchun xavfsizlik devorlari (firewall), kiber hujamlarni aniqlash va oldini olish tizimlari kabi zararni kamaytirish strategiyalaridan foydalansih juda muhimdir. Shuningdek, tashkilotlar kiberxavfsizlik bo‘yicha muntazam tayyorgarlik mashg‘ulotlarini o‘tkazib, favqulodda holatlarga tayyor turishlari zarur.(DataGuard, 2024). **Cybersecurity Ventures kompaniyasining 2024-yilgi hisobotiga ko‘ra, 2025-yilga kelib ransomware hujumlari oqibatida yetkazilgan global zarar 20 milliard AQSh dollaridan oshishi kutilmoqda.** Bu ko‘rsatkich atiga bir necha yil avvalgi 5 milliard dollarlik zararga nisbatan keskin o‘sishdir. Statistik ma’lumotlarga ko‘ra, sog‘liqni saqlash, ta’lim va ishlab chiqarish kabi sohalar eng ko‘p nishonga olinadigan tarmoqlar hisoblanadi. Global statistik ma’lumotlar shuni ko‘rsatadiki, shaxsiy ma’lumotlarni o‘g‘irlash eng keng tarqalgan kiberjinoyatlardan biri bo‘lib, har yili millionlab insonlar o‘zlarining shaxsiy ma’lumotlaridan mahrum bo‘lmoqdalar. Fishing (firibgarlik orqali ma’lumot yig‘ish) hujumlari ham vaqt o‘tishi bilan ancha murakkab shaklga ega bo‘lib bordi. Dastlab oddiy firibgarlik sifatida boshlangan bu usul hozirda ilg‘or ijtimoiy muhandislik texnikalari va aniq maqsadli hujumlarni o‘z ichiga olmoqda. 2023-yilda butun dunyo bo‘ylab 1,5 milliondan ortiq fishing bilan bog‘liq hodisalar qayd etilgan. Bu esa fishing hujumlarini eng keng tarqalgan kiberjinoyatlardan biri sifatida ko‘rsatmoqda.(GO-Globe,2025).

Kiberxavfsizlik - bu qurilmalar va xizmatlarni xakerlar, spamerlar hamda boshqa zararli raqamli jinoyatchilar tomonidan amalga oshiriladigan elektron hujumlardan himoya qilishni o‘z ichiga oluvchi fan sohasi hisoblanadi. Zamonaviy raqamli muhitda kiberxavfsizlikni e’tibordan chetda qoldirish mumkin emas. Birgina xavfsizlik buzilishi millionlab insonlarning shaxsiy ma’lumotlari oshkor bo‘lishiga olib kelishi mumkin. Bunday hodisalar nafaqat korxonalar uchun jiddiy moliyaviy yo‘qotishlarga, balki mijozlar ishonchini yo‘qotishga ham sabab bo‘ladi. (Karin Kelley, 2025). Kiberxavfsizlik bugungi kunda nafaqat ommaviy axborot vositalarining sarlavhalarida, balki siyosatchilar, sanoat rahbarlari, akademiklar va keng jamoatchilik e’tiborida ham dolzarb mavzuga aylangan. Ushbu xavfli vaziyatda hech kim va hech nima to‘liq himoyalangan deb hisoblanmaydi. Global raqamli infratuzilmalar, korxonalar, davlat muassasalari va hatto oddiy foydalanuvchilar ham kiberhujumlar nishoniga aylanishi mumkin. Shuning uchun ham kiberxavfsizlik masalalari bugungi axborot asrida eng muhim

ustuvor yo‘nalishlardan biriga aylangan.(Dan Jerker B.Svantesson,Christopher Kuner,Fred H. Cate,Orla Lynskey and Christopher Millard,2017).

(Nchumbeni Yanthan, 2023).

Shaxsiy ma’lumotlarni samarali texnik himoya usullari quyidagilar :

Internet olamida shaxsiy ma’lumotlarni himoya qilish har bir foydalanuvchi uchun dolzarb va mas’uliyatli vazifadir. Olib borilgan tahlillar shuni ko‘rsatadiki, texnologik vositalardan xavfsiz foydalanish, xususan, HTTPS protokolidan foydalanish orqali ma’lumotlarni shifrlash, shaxsiy axborotni uchinchi tomonlardan himoyalashda samarali usullardan biri hisoblanadi. Shubhali havolalardan ehtiyot bo‘lish, ijtimoiy tarmoqlarda shaxsiy ma’lumotlarni oshkor etmaslik, va umumiy Wi-Fi tarmoqlaridan foydalanganda ehtiyot choralarini ko‘rish, shaxsiy ma’lumot xavfsizligini ta’minlashda muhim ahamiyatga ega. Ayniqsa, VPN texnologiyasidan foydalanish ochiq tarmoqlarda ma’lumotlar himoyasini sezilarli darajada kuchaytiradi. Mobil xavfsizlik, internet foydalanuvchilar mobil ilovalarni faqat rasmiy manbalardan yuklab olishlari va har bir ilovaning ruxsatlari va shartlarini e’tibor bilan ko‘rib chiqishlari lozim. Dasturiy ta’minotni muntazam ravishda yangilab borish, qurilma va ilovalardagi zaifliklarni bartaraf etishga yordam beradi va yangi xavflardan himoya qilishda muhim rol o‘ynaydi.(Yazid Yusuf, 2024).

Har bir davlat o‘zining ichki qonunlariga ega bo‘lsada, bu sohada xalqaro qonunchilik va huquqiy me’yorlar muhim rol o‘ynaydi.

Umumiy Ma’lumotlarni Himoya Qilish Reglamenti (GDPR) – bu dunyodagi eng qat’iy maxfiylik va xavfsizlik qonuni hisoblanadi. Ushbu qonun, Yevropa Ittifoqi (EU) tomonidan ishlab chiqilgan va qabul qilingan bo‘lsa-da, u YI hududidagi odamlarga tegishli ma’lumotlarni oluvchi yoki yig‘uvchi har qanday tashkilotga, u qayerda joylashganidan qat’i nazar, majburiyatlar yuklaydi. Reglament 2018-yil 25-maydan kuchga kirgan. GDPR maxfiylik va

xavfsizlik standartlarini buzganlarga nisbatan og‘ir jarimalarni belgilaydi, bu jarimalar bir necha million yevroga yetishi mumkin. GDPR orqali Yevropa, odamlar shaxsiy ma’lumotlarini bulutli xizmatlarga tobora ko‘proq ishonib topshirayotgan va ma’lumot buzilishlari kundalik hodisaga aylangan bir vaqtda, ma’lumotlar maxfiyligi va xavfsizligi bo‘yicha qat’iy ishtirokini namoyon qilmoqda.(Ben Wolford, 2020).

Yevropa Kengashining “Kiberjinoyatchilik to‘g‘risidagi Konvensiya” (Budapesht, 2001-yil 23-noyabr) - kompyuter axboroti sohasida milliy miqyosda amalga oshiriladigan chora-tadbirlarni qayd etdi; kiberjinoyatlarning turlari va ularni sodir etganlik uchun jazo turlarini belgilab berdi; tezkor-qidiruv harakatlarining ayrim protsessual xususiyatlarini, tergov jarayonida ma’lumotlarning saqlanishini aniqladi; bu boradagi xalqaro hamkorlik va o‘zaro yordamning umumiy tamoyillarini taklif qildi. Budapesht Konvensiyasi ishtirokchilarining har biri ushbu hujjat qoidalarida ko‘zda tutilgan vakolatlar va tartiblarni belgilash uchun zarur bo‘lgan milliy qonunchilikni ishlab chiqadi va boshqa choralarni ko‘radi deb, tavsiya etgan. (R.R.Shakurov,M.M.Vohidov, 2022).

O’zbekiston Respublikasining Shaxsga doir ma’lumotlar to’g’risida“gi Qonuni - ushbu qonunning amal qilishi doirasi shaxsga doir ma’lumotlarga ishlov berish va ularni himoya qilish chog‘ida qo‘llaniladigan ishlov berish vositalaridan, shu jumladan axborot texnologiyalaridan qat’i nazar yuzaga keladigan munosabatlarga nisbatan tatbiq etiladi va maqsadi shaxsga doir ma’lumotlar sohasidagi munosabatlarni tartibga solishdan iborat. **“Unutilish huquqi”** — bu shaxsning shaxsiy ma’lumotlari tashkilot yoki xizmat ko‘rsatuvchi tomonidan saqlanayotgan bo‘lsa, uni shaxsning iltimosiga binoan o‘chirib tashlash talabini qo‘yish huquqidir. Bu huquq, Yevropa Ittifoqining Umumiy Ma’lumotlarni Himoya Qilish Reglamenti (GDPR) asosida berilgan bo‘lib, Yevropa Ittifoqi (EU)dagi shaxslarning shaxsiy ma’lumotlarini himoya qiladi. Biroq, internet olamida har doim ham foydalanuvchilar o’z ma’lumotlarini o’chirib tashlay olmasligi mumkin.(Cloudflare,2025).

IV. MUHOKAMA

Hozirgi raqamli davrda har bir inson o’z ehtiyojidan kelib chiqgan holda internet tarmoqlaridan foydalanadi. Ammo, internetdan foydalanish jarayonida turli xil internet tarmoqlar va veb-saytlar tomonidan foydalanuvchining shaxsiy ma’lumotlarini yig’ilishi va boshqa shaxslarga uzatish holatlari yuzaga keladi. Bu esa ushbu ma’lumotlarning egasi roziligisiz uchinchi shaxslarga o’tishiga olib kelishi mumkin. Natijada, internet foydalanuvchining shaxsiy hayoti va ma’lumotlariga doir huquqlari buzilishiga olib keladi. Shuning uchun qanday ma’lumotlar shaxsiy ma’lumot hisoblanishini bilib olishimiz lozim. 2025-yil boshida dunyo bo‘yicha jami 5,56 milliard kishi internetdan foydalangan, bu esa jahondagi umumiy aholi sonining 67,9 foiziga tengdir.(DataReportal, 2025). Ushbu statistikadan kelib chiqib shuni aytishimiz kerakki, internet foydalanuvchilarning shaxsiy ma’lumotlari va ularning internetdan foydalanishdagi huquqlarining himoyasiga alohida e’tibor qaratish lozim. Internet olamida shaxsiy ma’lumotlarni himoya qilishda huquqiy himoya chorasi, ya’ni, internet foydalanuvchisi o’zi yashaydigan mamlakatning qonunchiligi asosida yoki xalqaro normalarga binoan internet tarmoqlaridagi shaxsiy ma’lumotlarini himoya qilishga oid huquqlari himoya qilinishi belgilab o’tiladi. Huquqiy himoya chorasi asosan qonunchilikda va xalqaro normalarda belgilab qo’yiladi. Internet olamida shaxsiy ma’lumotlarni himoya qilishda yana bir asosiy omil bu internet foydalanuvchisi o’z shaxsiy

ma'lumotlarini himoya qilishda texnik va huquqiy himoya choralarini bilishi,shuningdek, shaxsiy ma'lumotlarini himoya qilishdagi huquqlari haqida bilimga ega bo'lganligi hisoblanadi. Shu sababli, har bir foydalanuvchi internetdagi o'z shaxsiy ma'lumotlari saqlanib qolinishini oldini olishi yoki internet tarmoqlaridan foydalanish jarayonida har bir foydalanayotgan tarmoqlarining talablari va shartlarini diqqat bilan o'qib chiqib keyin rozilik bildirishi bir qancha internetdagi kiber tahdidlarni oldini olishga yordam beradi.

V. XULOSA

Yuqorida internet olamida shaxsiy ma'lumotlarni himoya qilishda turli xil texnik va huquqiy mexanizmlarni tahlil qilganimizdan so'ng, quyidagi umumiy xulosaga kelishimiz mumkin. Bugungi kunda raqamli davr tez sur'atda rivojlanib bormoqda. Shu bois, har bir internet foydalanuvchisi internetdagi turli xil veb-saytlardan va tarmoqlardan foydalanishda internetdan xavfsiz foydalanishga oid bilim va ko'nikmalarni bilishi lozim. Chunki, har bir internet foydalanuvchisi internetdan xavfsiz foydalanishdagi bilim va ko'nikmalarni o'zida shakllantirsa, internet tarmoqlardagi bir qancha kiber tahdidlarni oldini olishga ko'maklashadi. Shu sababli, har bir internet foydalanuvchilar internet tarmoqlaridan foydalanish jarayonida turli xil xavfsiz himoya choralari haqida bilimga ega bo'lishlari kerak. Ushbu maqolada, internetda shaxsiy ma'lumotlarni himoya qilishning ahamiyati, mavjud kiber tahdidlar, turli kiberjinoyatlar va ularga qarshi kurashish usullari tahlil qilindi. Internet xavfsizlik madaniyatini shakllantirish, internet foydalanuvchilarining huquqiy va texnik savodxonligini oshirish, shuningdek, shaxsiy ma'lumotlar va axborot xavfsizligi bo'yicha xalqaro hamkorlikni kuchaytirish orqali shaxsiy ma'lumotlarni himoya qilish darajasini oshirish mumkin. Shu bilan birga, har bir inson internet olamida shaxsiy ma'lumotlarni himoya qilish, ya'ni, kiberxavfsizlik sohasidagi muhim bo'lgan yangiliklar va axborotlardan xabardor bo'lib borishi va internet tarmoqlaridan foydalanishda xavfsizlik choralari haqida kerakli ma'lumotlar va bilimlarni o'rganib borishi lozim.

Adabiyotlar, References, Литературы:

1. General Data Protection Regulation (GDPR), 2018. https://gdpr-info.eu/
2. Winnie Chung and John Paynter."Privacy Issues on the Internet.'' *The University of Auckland, New Zealand,* 2002.
3. Cyber Talents. "What is Cyber Crime? Types, Examples, and Prevention.'' *Cyber Talents.* Accessed April 3, 2025. https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention
4. Statista. "Internet usage worldwide – statistics & facts." *Statista.* Accessed April 3, 2025. https://www.statista.com/topics/1145/internet-usage-worldwide/
5. DataGuard. "What is cyber crime ? ." *DataGuard.* Accessed April 3, 2025. https://www.dataguard.com/blog/what-is-a-cyber-crime/
6. Cyber Security News. "Cybercrime Index." *Cyber Security News.* Accessed April 3, 2025. https://cybersecuritynews.com/cybercrime-index-ranks/
7. GO-Globe. "Cyber Crime Statistics and Trends." *GO-Globe.* Accessed April 3, 2025. https://www.go-globe.com/cyber-crime-statistics-and-trends-infographic/
8. SimpliLearn. "What is Cyber Security l Types, Importance and Threats." *SimpliLearn.* Accessed April 3, 2025. https://www.simplilearn.com/tutorials/cyber-security-tutorial/

9. Dr. Christopher Kuner, Dan Jerker B. Svantesson, Fred H. Cate, Orla Lynskey and Christopher Millard. "The rise of cybersecurity and its impact on data protection." *in International Data Privacy Law,* 2017. https://www.researchgate.net/publication/
10. SprintZeal. "Cyber Attack Statistics and Trends to Know in 2024." *SprintZeal.* Accessed April 5, 2025. https://www.sprintzeal.com/blog/cyber-attack-statistics-and-trends
11. Dr. Yazid Yusuf. "Safe Ways to Protect Your Personal Data on the Internet." *Telkom University.* Accessed April 5, 2025. https://bif.telkomuniversity.ac.id/
12. Gdpr.eu. "What is GDPR, the EU's new data protection law?." *Gdpr.eu.* Accessed April 5, 2025. https://gdpr.eu/what-is-gdpr/
13. *Kiber huquq – huquq sohasi sifatida: risola /* tuzuvchilar R.R.Shakurov, M.M.Vohidov. – Toshkent: O'zbekiston Respublikasi Adliya vazirligi qoshidagi Yuristlar malakasini oshirish markazi, 2022.
14. Cloudflare. "What is the right to be forgotten." *Cloudflare.* Accessed April 5, 2025. https://www.cloudflare.com/learning/privacy/right-to-be-forgotten/
15. DataReportal. "Digital Around The World." *DataReportal.* Accessed April 5, 2025. https://datareportal.com/global-digital-overview