ISSN: 2181-3906 2024

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 3 / ISSUE 11 / UIF:8.2 / MODERNSCIENCE.UZ

SHAXS MA'LUMOTLARINI HIMOYA QILISHNING HUQUQIY VA TEXNIK JIHATLARI

Karimjonova Laylo Abdumalik qizi
Toshkent davlat yuridik universiteti.
karimjonovalaylo@gmail.com
Javoxir Eshonqulov
javoxireshonqulov0724@gmail.com
Ilmiy rahbar,
Toshkent davlat yuridik universiteti, Kiber huquq kafedrasi o'qituvchisi.

https://doi.org/10.5281/zenodo.14231936

Annotatsiya. *Bugungi kunda shaxsga oid ma'lumotlar himoyasi har qachongidan ko'ra dolzarbroq hisoblanadi. Yildan yilga shaxsga doir ma'lumotlarning xavfsizligini kuchaytirishga qaratilgan ko'plab chora-tadbirlar olib borilmoqda. Ushbu ilmiy maqolada shaxs ma'lumotlarini himoya qilishning zamonaviy usullari, raqamli muhitda ma'lumotlar xavfsizligini ta'minlash mexanizmlari o'rganildi.*

Kalit so'zlar: *shaxs ma'lumotlar, data protection, personal data, data privacy, keylogger, fishing, soxta identifikatsiya.*

LEGAL AND TECHNICAL ASPECTS OF PERSONAL DATA PROTECTION

Abstract. *Protection of personal data is more relevant today than ever before. Many measures are being taken year after year to strengthen the security of personal data. This scientific article examines modern methods of personal data protection and mechanisms for ensuring data security in the digital environment.*

Keywords*: Personal data, data protection, personal data, data privacy, keylogger, phishing, false identification.*

ЮРИДИЧЕСКИЕ И ТЕХНИЧЕСКИЕ АСПЕКТЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация. *Защита персональных данных сегодня актуальна как всегда. Из года в год принимается множество мер, направленных на усиление безопасности персональных данных. В данной научной статье рассматриваются современные методы защиты персональных данных и механизмы обеспечения безопасности данных в цифровой среде.*

Ключевые слова*: Персональные данные, защита данных, личные данные, конфиденциальность данных, кейлоггер, фишинг, ложная идентификация.*

KIRISH

Hozirgi zamonaviy XXI asrda shaxs ma'lumotlarini himoya qilish dolzarb va muhim ijtimoiy-huquqiy muammoga aylangan. Shaxsga doir ma'lumotlar xavfsizligi - bu individual ma'lumotlarni noqonuniy kirishdan, o'zgartirishdan, tarqatishdan va yo'q qilishdan himoya qilishga yo'naltirilgan chora-tadbirlar majmuasi hisoblanadi.

Bugungi kunda raqamli texnologiyalarning tez sur'atlar bilan rivojlanishi, internet tarmog'ining keng tarqalishi va axborot almashinuvi tezligining oshishi shaxsiy ma'lumotlarning xavfsizligiga yangi xavf-hatar yaratmoqda.

Butun dunyoda 2007-yildan buyon har yili 28-yanvar Xalqaro shaxsga doir ma'lumotlarni himoya qilish kuni (Data Protection Day)[1] sifatida nishonlanadi va ayrim mamlakatlarda u "Maxfiylik kuni" (Data Privacy Day)[2] degan nom bilan ham bayram qilinadi.

Bundan ma'lumki, shaxsga doir ma'lumotlarning himoyasi xalqaro darajada ham muammo sifatida e'tirof etilgan. Ko'rinib turibdiki, axborot texnologiyalari va zamon rivojlanishi bilan birgalikda shaxsga doir ma'lumotlar himoyasi ham yanada dolzarblashib bormoqda.

TADQIQOT MATERIALLARI VA METODOLOGIYASI

Shaxsga doir ma'lumotlar – inson haqidagi har qanday ma'lumotlardan iborat.

Shaxsga doir ma'lumotlar uch turga: umumiy ma'lumotlar, maxsus ma'lumotlar va biometrik ma'lumotlarga bo'linadi.

Umumiy ma'lumotlar qatoriga insonning ism-familiyasi, pasporti va boshqa shaxsiy hujjatlaridagi qaydlar, tug'ilgan sanasi va joyi, e-mail manzili, yashash, o'qish va ishlash joylari, oilaviy, ijtimoiy va mulkiy holati, qayerda ta'lim olgani, qaysi kasb egasi ekanligi, daromadi qanchaligi kabi ma'lumotlar kiradi.

Transport vositasining davlat raqami, kommunal-turarjoy xo'jaligining hisob raqami kabilar esa shaxsga doir ma'lumot hisoblanmaydi. Chunki ulardan birinchisi – bevosita avtomobilga tegishli bo'lsa, ikkinchisi – uy-joyga taalluqlidir.

Maxsus ma'lumotlar deganda, shaxsning irqiy va milliy mansubligi, siyosiy, diniy va falsafiy qarashlari, sog'ligining holati, intim, ya'ni maishiy hayoti bilan bog'liq ma'lumotlar tushuniladi. Biometrik ma'lumotlar – insonning shaxsini aniqlash imkonini beradigan fiziologik va biologik xususiyatga ega shaxsiy ma'lumotlardir.

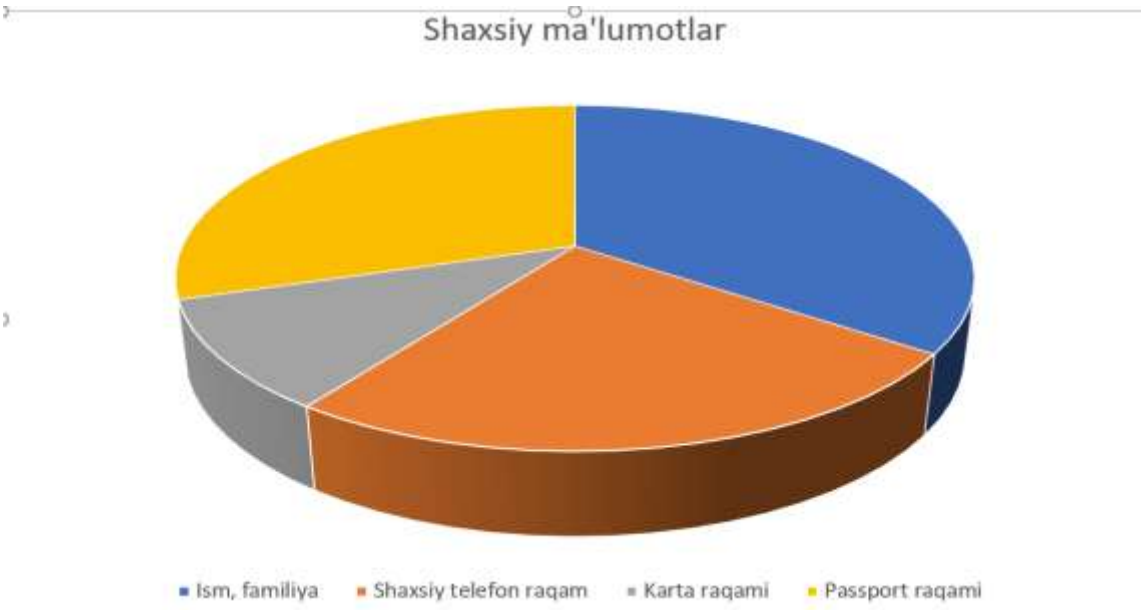
Masalan, shaxsning DNKsi, ovozi, ko'z qorachig'i, barmoq izlari, yuz qiyofasi, bo'yi, vazni bilan bog'liq ma'lumotlar shular jumlasiga kiradi. Hozirgi kunda, yoshlar tomonidan turli xil saytlarga kirish orqali o'z shaxsiy ma'lumotlarini oshkor qilish juda katta muammoga aylanmoqda.

Misol uchun, 2013 – yilda tashkil etilgan "o'lim guruhlari" ya'ni "ko'k kit" o'yini, o'smir yoshdagilardan o'z shaxsiy ma'lumotlarini olish orqali, ularga turli havolalar yuborib ularga "ko'k kit" o'yinini o'ynashni taklif etadi.

Turli xil shartlar beriladi va so'nggida o'zini "qaramonlarcha" o'ldirishni buyuradi, shartni bajarishdan bosh tortsa o'smirning IP manzilini aniqlab, uning uy manzilini bilib oladi va yaqinlarini o'ldirish bilan tadid qiladi. Shaxsning birgina o'z shaxsiy ma'lumotlarini oshkor etishi shunday oqibatlarga olib keladi.

Yirik kompaniyalardan shaxsga doir ma'lumotlarning olib chiqib ketilishi, o'tgan va bugungi asr uchun ham yot emas. Tadqiqotlarga ko'ra, 100 kishidan so'rovnoma o'tkizilganda shuni bilib oldikki, ular asosan internet saytlariga kirayotganda yoki turli xil pullik va bepul programmalardan foydalanayotganda, asosan ism va familiyasidan tashqari o'z raqami va karta raqamini ham kiritishlarini aytishdi.

[1] https://privacy.web.cern.ch/news/news/did-you-know-28-january-data-protection-day (So, now you know why on the 28th January, many organisations, national authorities, private companies and other actors organise activities to raise awareness about the importance of data protection and to promote best practices.)
[2] https://en.wikipedia.org/wiki/Data_Privacy_Day (Data Privacy Day (known in Europe as Data Protection Day))



Bundan ko‘rinib turibdiki, ulardan 78 tasi o‘z ism familiyasini, 56 tasi o‘z shaxsiy telefon raqamini , 23 tasi karta raqamini va 67 tasi passport raqamini kiritishlari aniqlandi. Ko‘rinib turibdiki, shaxslarning o‘zi avvalo shaxsga oid ma’lumotlarini o‘zlari , bilmasdan va ba’zan bilib oshkor qilishadi.

TADQIQOT NATIJALARI

O‘zbekiston Respublikasining shaxsga doir ma’lumotlar haqidagi qonuni fuqarolarning shaxsiy ma’lumotlarini himoya qilishga qaratilgan muhim hujjatdir. Ushbu qonun davlatga shaxsiy ma’lumotlarning maxfiyligini va xavfsizligini ta’minlash kafolatini beradi. “Shaxsga doir ma’lumotlar to‘g‘risida”gi O‘zbekiston Respublikasining Qonuni[3], 5 – bobi “Shaxsga doir ma’lumotlarni himoya qilish” haqida bo‘lsa, unda asosiy e’tiborni shaxs ma’lumotlarining yaxlitligini saqlashga qaratadi va mulkdor yoki operatorlarga qo‘yiladigan talablarni belgilaydi.

Ularning asosiy vazifasi shaxsning o‘z hayotiga aralashuvdan himoyalanish huquqini ta’minlash, ma’lumotlarning maxfiyligiga rioya etish va qonunga xilof ishlov berishning oldini olishdan iboratdir. Xususan, qonun shaxsga doir ma’lumotlarni oshkor etish va tarqatishga qat’iy cheklov qo‘yadi. Subyektning roziligisiz hech qanday ma’lumot uchinchi shaxslarga berilishi mumkin emas. Shu bilan birga, ba’zi hollarda, aholini axborot bilan ta’minlash maqsadida va subyektning yozma roziligi bilan ayrim shaxsiy ma’lumotlarni ochiq manbalariga kiritish mumkin.

Shaxsga doir ma’lumotlarga turli xil hujumlar haqida gaplashamiz.

Fishing - elektron aldamchilik bo‘lib, foydalanuvchilarni soxta veb-sayt yoki xabarlar orqali shaxsiy ma’lumotlarini berish uchun aldashdir. Bunday hujumlarda hakerlar foydalanuvchilarni aldash orqali ularning shaxsiy ma’lumotlarini o‘g‘irlaydilar. Fishing hujumlari eng keng tarqalgan ijtimoiy muhandislik sxemalaridan biridir. Bunga odamlarni aldab o‘z ma’lumotlarini bo‘lishishga mo‘ljallangan e-pochta xabarlari, SMS, ijtimoiy media yoki chat orqali yuborilgan xabarlar kiradi va firibgarlar bu ma’lumotlardan jiddiyroq jinoyatlar sodir etish uchun foydalanadilar.Shuningdek, zararli havola yoki biriktirmalar orqali qurilmalarda zarali dastur o‘rnatish ham fishingning bir turi hisoblanadi.

[3] O'zbekiston Respublikasining "Shaxsga doir ma'lumotlar to'g'risida"gi Qonuni. 02.07.2019-yildagi O'RQ-547-son.

Aksariyat fishing hujumlari qonuniy ko‘rinishdagi va odatda siz ishonadigan manbadan (masalan, davlat tashkiloti, bank yoki ijtimoiy media xizmatidan) kelgan umumiy ommaviy xabarlar orqali amalga oshiriladi. Shu bilan birga, ma’lum shaxslar yoki guruhlarga qaratilgan fishing hujumlari ham mavjud va g‘araz niyatli odamlar o‘z vositalarini yanada takomillashtirib va yanada makkor hiyla yo‘llarini topib boradilar.[4] Ular soxta elektron pochta, SMS yoki veb-saytlar orqali shaxsiy ma’lumotlarni, bank ma’lumotlarini va parollarni o‘g‘irlashga harakat qiladilar. 2022-yilda dunyo bo‘yicha 300,000 dan ortiq phishing hodisasi qayd etilgan. Har 39 soniyada 1 ta phishing hujumi sodir bo‘lmoqda.

Kompaniyalarga yetkaziladigan zarar yillik 12 mlrd dollardan oshgan[5]. Fishingning eng keng tarqalgan turlari, Email Fishing, SMS Fishing (Smishing),Voice Fishing (Vishing),Web Fishing va Clone Fishing deb ataladi. Shunday ekan, turli xil raqamlardan kelgan qo‘ng‘iroqlarni qabul qilish yoki begonalarga o‘z shaxsiy ma’lumotlaringizni oshkor etish shunday holatlarga olib kelishi mumkin.

Soxta identifikatsiya kiberjinoyatlarning eng xavfli va ko‘p tarqalgan turlaridan biridir.

Ushbu jarayon moddiy va ma’naviy ziyon yetkazishga qaratilgan murakkab psixologik va texnik manipulyatsiya hisoblanadi. Hakerlar odatda identifikatsiyani qoplashning bir necha asosiy usullaridan foydalanadilar. Ular birinchi navbatda, individual shaxsning shaxsiy ma’lumotlarini to‘plashga harakat qiladilar. Buning uchun ijtimoiy tarmoqlar, ochiq axborot bazalari va boshqa manbalardan foydalanadilar. Eng xavfli tomoni shundaki, soxta identifikatsiya faqat virtual muhit bilan cheklanmaydi. Ayrim hollarda bu real moliyaviy operatsiyalar, yuridik dokumentlar va hatto jinoyat sodir etishgacha borib yetishi mumkin.

Keylogger dasturlar – 2005-yilda Florida shtatidagi bir ishbilarmon Bank of Americani bankdagi hisob raqamidan 90.000 XNUMX AQSh dollarini o‘g‘irlab ketganidan keyin sudga berdi. Tekshiruv davomida tadbirkorning kompyuterida yuqorida aytib o‘tilgan Backdoor Coreflood virusi yuqtirilganligi aniqlandi. Sizning bank operatsiyalaringizni Internet orqali amalga oshirganingiz sababli, kiberjinoyatchilar sizning barcha maxfiy ma’lumotlaringizni olishdi.[6] Bu kabi zararli dasturlarning eng xavfli va introspektiv turlaridan biri hisoblanadi. Ushbu dastur foydalanuvchi kompyuterida yoki smartfonida maxfiy ravishda o‘rnatiladi va uning barcha kiritilayotgan ma’lumotlarini qo‘lga kiritadi. Keylogger dasturlar kompyuter tugmachalar bosilishini kuzatuvchi maxsus dasturiy ta’minotdir. Ular foydalanuvchi kiritayotgan har bir belgini, parolni, chat yozishmalarini, bank ma’lumotlarini va boshqa maxfiy informatsiyalarni to‘g‘ridan-to‘g‘ri hakerning server yoki elektron pochta manziliga uzatib boradi. Keylogger dasturlarning asosiy maqsadi shaxsiy ma’lumotlarni o‘g‘irlash. Ularning o‘rnatilish usullari turlicha. Ba’zi hollarda hakerlar maxsus dasturlarni elektron pochta havolalari, USB-fleshkalar, ochiq Wi-Fi tarmoqlari orqali tarqatadilar. Ba’zida esa ular kompyuter tizimining zaif tomonlaridan foydalanib, keylogger dasturlarni yashirin ravishda o‘rnatib qo‘yadilar. Keylogger dasturlarning eng xavfli tomoni shundaki, ular tizimda juda ko‘p vaqt saqlanishi va foydalanuvchi bilmasdan ishlashi mumkin. Ba’zi dasturlar operatsion tizimga shu qadar chuqur kirib boradi-ki, antivirus dasturlari ham ularni aniqlashda qiyinchilik chekadi.

[4] https://cyber-star.org/uz/cs-articles/how-to-recognize-phishing-attacks-uz/ (Fishing nima?)
[5] Cybersecurity and Privacy Law Report 2022. IBM Security Research // www.ibm.com/security/reports
[6] https://citeia.com/uz/texnologiyadagi-innovatsiyalar/keylogger-nima (Birinchi Keylogger qachon paydo bo'ldi?)

Biometrik xavfsizlik mexanizmlarini takomillashtirish orqali foydalanuvchi identifikatsiyasini yanada ishonchli qilish uchun ko‘z qorachig‘i, barmoq izi, ovoz va yuz tanish kabi biometrik texnologiyalardan keng foydalanish kerak. Ushbu yondashuvlar soxta identifikatsiya risklarini sezilarli darajada pasaytirishi mumkin. Keylogger dasturlar uchun esa, kompyuter tizimlarni o‘zini-o‘zi himoya qiluvchi va zarar yetkazuvchi dasturlarni darhol aniqlaydigan “immun tizim”ga o‘xshash dasturlarni ishlab chiqish lozim.

MUHOKAMA

Bugungi kunda turli xil ijtimoiy tarmoqlarda (Telegram, Facebook, Instagramm) har xil programmalar havolalari kelib turibdi. Ularning deyarli barchasi hakerlar tomonidan tashkil etilgan bo‘lib, shaxsiy ma’lumotlaringizga kirish uchun “tuzoq” sifatida qo‘yilgan bo‘ladi. Bunday “tuzoq”larga tushib qolmaslik uchun huquqiy ong va huquqiy madaniyatni rivojlantirish, atrofingizdagi jamiyatda sodir bo‘layotgan kiberhujumlardan boxabar bo‘lishingiz kerak.

Davlat tomonidan olib borilayotgan profilatika nazorat haftaliklari, seminar va turli xil treninglar, qabul qilinayotgan qonunlar shaxslarning shaxsiy ma’lumotlariga nisnatan sodir etilishi mumkin bo‘lgan ko‘plab kiberhujumlar uchun to‘siq vazifasini bajarmoqda. Kiberfiribgarlar ma’lum harakatlarni amalga oshirish yoki ishonuvchan shaxslarning shaxsiy ma’lumotlarini qo‘lga kiritish uchun psixologik manipulyatsiya — ijtimoiy fikrni boshqarish uslubidan foydalanishadi.

Ho‘sh qanday qilib bunga chek qo‘ysa bo‘ladi? Avvalo, noma’lum manbalardan kelgan xabar va havolalarga ishonch bilan yondashmaslik kerak, shaxsiy ma’lumotlaringizni saqlashingiz va hech kimga bermaslik kerak. Kuchli himoyalangan va murakkab parollardan foydalanish zarur, bir xil parollardan qochish kerak. Ikki bosqichli identifikatsiya tizimidan foydalanish esa shaxsiy hisob uchun qo‘shimcha himoya bo‘ladi.

General Data Protection Regulation (GDPR)[7]- Yevropa Ittifoqi tomonidan 2018 yilda qabul qilingan shaxsiy ma’lumotlarni himoya qilish bo‘yicha eng muhim qonunchilik hujjati hisoblanadi. Ushbu qonun jimsoniy va yuridik shaxslarning ma’lumotlarini ishlov berish jarayonlariga qat’iy tartib o‘rnatadi. Ushbu qonunchilik hujjatining asosiy maqsadi, fuqarolarning shaxsiy ma’lumotlarini himoya qilish, ma’lumotlarni ishlov berishda ochiqlik va shaffoflikni ta’minlash va kompaniyalar tomonidan ma’lumotlardan noto‘g‘ri foydalanishning oldini olish hisoblanadi. GDPR nafaqat Yevropa davlatlariga, balki butun dunyo kompaniyalariga ta’sir qiladi va ularni o‘z ma’lumotlar siyosatini qayta ko‘rib chiqishga majbur etadi.

Shaxsiy ma’lumotlarni saqlash masalasi bugungi raqamli davrdagi eng dolzarb muammolardan biri bo‘lib, CCPA (California Consumer Privacy Act)[8] 2018 yilda qabul qilingan va 2020 yilda kuchga kirgan ushbu qonun AQSh Kaliforniya shtatida fuqarolarning shaxsiy ma’lumotlarini himoya qilishga qaratilgan. CCPA kompaniyalarni ma’lumotlarni ochiq va shaffof ishlov berishga, fuqarolarning shaxsiy ma’lumotlar ustidan nazoratini kuchaytrishga va ma’lumotlarni noto‘g‘ri ishlov berishga chek qo‘yishga yo‘naltirilgan. Qonun buzilgan taqdirda kompaniyalarga 100 dollardan 750 dollargacha, ayrim hollarda bir marta buzilganda 7,500 dollargacha jarima qo‘llanilishi mumkin.

[7] General Data Protection Regulation (GDPR) 2016/679, European Union, 2018.
[8] California Consumer Privacy Act (CCPA), California Civil Code Section 1798.100-1798.199, 2018.

Shunday jarimalar natijasida, shaxslarning ma’lumotlariga qilinadigan kiberhujumlar kamaymoqda. Rivojlangan davlatlarda qo‘llanilayotgan yangi himoya dasturlaridan , rivojlanayotgan mamlakatlar andoza olishi va o‘xshash himoya usullarini ishlab chiqishi lozim.

XULOSA

Xulosa qilib aytganda, shaxsiy ma’lumotlarni saqlash bugungi davrdagi eng dolzarb va murakkab masalalardan biridir. Tadqiqot natijalari shuni ko‘rsatadiki, zamonaviy texnologiyalarning rivojlanishi bilan birga shaxsga doir ma’lumotlarning xavfsizligiga tahdidlar ham ortib bormoqda. Shaxsiy ma’lumotlarni himoya qilishning bir necha muhim yo‘nalishlari mavjud.

Birinchidan, qonuniy mexanizmlar - GDPR, CCPA kabi xalqaro hujjat va aktlar fuqarolarning shaxsiy malumotlar ustidan nazoratini kuchaytiradi. Ikkinchidan, texnologik yechimlar - biometrik identifikatsiya, ikki bosqichli autentifikatsiya tizimlaridan foydalanish ma’lumotlar xavfsizligini oshiradi. Kiberhujumlarning eng asosiy turlari - phishing, soxta identifikatsiya va keylogger dasturlar bo‘lib, ular shaxslarning ma’lumotlarini o‘g‘irlash va unga ziyon yetkazishga qaratilgan. Bunday hujumlardan saqlanish uchun fuqarolarning huquqiy ongi va madaniyatini oshirish, oddiy parollar va ochiq manbalardan ehtiyot bo‘lish zarur.

O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni shaxsiy ma’lumotlarni himoya qilishning huquqiy asosini yaratadi. Kelgusida bunday qonunlarni yanada takomillashtirish, xalqaro standartlarga muvofiqlashtirish va texnologik yechimlarni joriy etish asosiy masala bo‘lib qolmoqda.

REFERENCES

1. O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni. 02.07.2019-yildagi O‘RQ-547-son.
2. https://privacy.web.cern.ch/news/news/did-you-know-28-january-data-protection-day (So, now you know why on the 28th January, many organisations, national authorities, private companies and other actors organise activities to raise awareness about the importance of data protection and to promote best practices.)
3. https://en.wikipedia.org/wiki/Data_Privacy_Day (Data Privacy Day (known in Europe as Data Protection Day))
4. https://cyber-star.org/uz/cs-articles/how-to-recognize-phishing-attacks-uz/ (Fishing nima?)
5. https://citeia.com/uz/texnologiyadagi-innovatsiyalar/keylogger-nima (Birinchi Keylogger qachon paydo bo‘ldi?)
6. General Data Protection Regulation (GDPR) 2016/679, European Union, 2018.
7. California Consumer Privacy Act (CCPA), California Civil Code Section 1798.100-1798.199, 2018.
8. Cybersecurity and Privacy Law Report 2022. IBM Security Research // www.ibm.com/security/reports
9. Eshonqulov, Javoxir. "SUV RESURSLARINI MUHOFAZA QILISH YO‘LIDAGI O‘ZBEKISTON RESPUBLIKASI QONUNCHILIK TAHLILI." *Центральноазиатский журнал образования и инноваций* 2.11 Part 3 (2023): 47-52.

10. Javokhir Eshonkulov “Legal Foundations for the Application of Artificial Intelligence Technologies in the Sports Industry” American Journal of Education and Evaluation Studies Том 1, No.7, 2024/10/4, 240-247
11. Usmonova Sabina, Javoxir Eshonqulov “Huquqiy risklarni baholashda big datatexnologiyasidan foydalanish” ISSN:2181-39062024 International scientific journal«MODERNSCIENCEAND RESEARCH»VOLUME 3/ ISSUE 11/ UIF:8.2 / MODERNSCIENCE.UZ