

AXBOROT XAVFSIZLIGI VA SHAXSIY MA'LUMOTLAR HIMOYASI**Suyunova Lobar Shuhratovna****Toshkent davlat yuridik universiteti****Ommaviy huquq fakulteti 2-kurs talabasi****e-mail: lobarsuyunova1@gmail.com**<https://doi.org/10.5281/zenodo.21019205>

Annotatsiya: Global miqyosida axborot xavfsizligi va shaxsiy ma'lumotlar himoyasi dolzarb muammoga aylanib ulgurdi. Demak XXI-asrda axborot xavfsizligini va shaxsiy ma'lumotlar daxlsizligini ta'minlash muhim ahamiyat kasb etmoqda. Mazkur maqolada axborot xavfsizligi va shaxsiy ma'lumotlar himoyasining raqamli makonda ahamiyati tahlil qilinadi. Raqamli texnologiyalar rivojlanishi davrida ma'lumotlarni himoya qilish dolzarb masalaga aylangani asoslab beriladi. **Tadqiqot davomida axborot xavfsizligiga tahdid soluvchi omillar, shaxsiy ma'lumotlarning noqonuniy tarqatilishi va ulardan noto'g'ri foydalanish bilan bog'liq muammolar o'rganildi.** Shuningdek, milliy va xalqaro huquqiy mexanizmlar tahlil qilinib, mavjud **kamchiliklar** aniqlanadi. Natijada axborot va shaxsiy ma'lumotlar xavfsizligini ta'minlash bo'yicha huquqiy, tashkiliy va profilaktik takliflar ishlab chiqiladi. Axborot xavfsizligini mustahkamlash fuqarolarning shaxsiy hayoti daxlsizligini ta'minlashga xizmat qiladi.

Kalit so'zlar: axborot xavfsizligi, shaxsiy ma'lumotlar, kiber huquq, ma'lumotlarni himoya qilish, kiberjinoyat, maxfiylik, axborot infratuzilmasi, huquqiy kolliziya, ma'lumotlarni transchegaraviy o'tkazish, xalqaro tajriba.

INFORMATION SECURITY AND PERSONAL DATA PRIVACY**Suyunova Lobar Shuhratovna****2nd-year student, Faculty of Public Law,****Tashkent State University of Law****E-mail: lobarsuyunova1@gmail.com**

Annotation: At the global level, information security and personal data protection have already become urgent issues. Therefore, in the 21st century, ensuring information security and the inviolability of personal data is of great importance. This article analyzes the significance of information security and personal data protection in the digital environment. It substantiates that the protection of data has become a pressing issue in the era of rapidly developing digital technologies. During the research, factors threatening information security, the illegal dissemination of personal data, and problems related to their misuse were examined. In addition, national and international legal mechanisms were analyzed and existing shortcomings were identified. As a result, legal, organizational, and preventive recommendations for ensuring information and personal data security are proposed. The study aims to strengthen information security and ensure the protection of citizens' privacy.

Keywords: information security, personal data, cyber law, data protection, cybercrime, privacy, conflict of laws cross-border data transfer international experience.

ЗАЩИТА ИНФОРМАЦИИ И НЕПРИКОСНОВЕННОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

Суюнова Лобар Шухратовна

Студентка 2 курса факультета публичного права
Ташкентского государственного юридического университета

E-mail: lobarsuyunova1@gmail.com

Аннотация: На глобальном уровне информационная безопасность и защита персональных данных уже стали актуальной проблемой. Следовательно, в XXI веке обеспечение информационной безопасности и неприкосновенности персональных данных приобретает особое значение. В данной статье анализируется значение информационной безопасности и защиты персональных данных в цифровой среде. Обосновывается, что в условиях стремительного развития цифровых технологий защита данных стала насущной задачей. В ходе исследования были изучены факторы, угрожающие информационной безопасности, незаконное распространение персональных данных и проблемы их неправомерного использования. Кроме того, проанализированы национальные и международные правовые механизмы и выявлены существующие недостатки. В результате разработаны правовые, организационные и профилактические рекомендации по обеспечению безопасности информации и персональных данных. Исследование направлено на укрепление информационной безопасности и обеспечение неприкосновенности частной жизни граждан.

Ключевые слова: информационная безопасность, персональные данные, киберправо, защита данных, киберпреступность, конфиденциальность, трансграничная передача данных, международный опыт, правовая коллизия.

Kirish: XXI-asrda axborot xavfsizligi va shaxsiy ma'lumotlarni himoya qilish global muammoga aylanib ulgurdi. Har bir shaxs kun davomida onlayn xizmatlar, onlayn platformalar, ijtimoiy tarmoqlar hamda raqamli texnologiyalardan foydalanadi. Bu esa internetni strategik resurs sifatida muhim ahamiyat kasb etishiga olib keldi. Biroq bu phishing, DDoS, Brute Force, SQL Injection, Identity Theft kabi kiberjinoatlarning avj olishiga sharoit yaratib berdi. Shuningdek, 2025-yilda Hindistonda 265 milliondan ortiq kiberhujum qayd etildi¹. 2024-yilda **Eron bank tizimlariga (IRLeaks guruhi orqali) katta kiberhujumlar amalga oshirildi**, unda 20 ta bank tizimi zararlandi va millionlab mijozlarning ma'lumotlari o'g'irlandi yoki sotuvga chiqarildi². Bu shuni ko'rsatadiki ko'pgina davlatlarda hali axborot xavfsizligi, shaxsiy ma'lumotlar himoyasini kiberhujumlardan to'liq himoyalash uchun muayyan mexanizmlar yetarli darajada ishlab chiqilmagan. Demak, raqamli texnologiyalarni kiberhujumlardan himoya qilish mexanizmlarini yaratish lozim. Raqamli texnologiyalar barcha sohalarga kirib bormoqda jumladan sog'liqni saqlash, ta'lim, biznes, davlat xizmatlari, moliya, soliq. Raqamli transformatsiya jarayonida yangi kelajak kasblari SSM, data scientist, cloud engineer, prompt engineer va boshqalar paydo bo'ldi. Natijada ko'pgina ijtimoiy munosabatlar, shaxsiy ma'lumotlar raqamli muhitga ko'chmoqda. Shu

¹ <https://timesofindia.indiatimes.com/technology/tech-news/india-records-265-million-cyber-attacks-in-2025-report/articleshow/125772984.cms>

² <https://www.justice.gov/archives/opa/pr/three-irgc-cyber-actors-indicted-hack-and-leak-operation-designed-influence-2024-us>

sababli ham kiberjinoyatlar soni ortib bormoqda. Bu jarayonda kiberxavfsizlik sohasining ustuvor vazifasi axborot xavfsizligi va shaxsiy ma'lumotlar daxlsizligini ta'minlashdir.

METODOLOGIYA

Tadqiqot olib borish usullari: qiyosiy-huquqiy tahlil orqali dastlab shaxsga doir ma'lumotlar himoyasi hamda axborot xavfsizligi sohasida milliy va xalqaro qonunchilik tahlil qilindi. Shuningdek, xalqaro va milliy qonunchilikning o'xshash va farqli jihatlari solishtirilib, ikkala tomonning ham yutuqlari va kamchiliklari muhokama qilindi. Shuningdek, xalqaro huquqiy keyslar orqali huquqiy bo'shliqlar muhokama qilindi. Mantiqiy va normativ-huquqiy tahlil asosida xalqaro manbalardan foydalangan holda kiberjinoyatlar muhokama va tahlil qilindi. Xalqaro miqyosdagi kiberjinoyatlarning va tahdidlarning ko'lami va xavfi batafsil yoritib berildi.

MUHOKAMA VA TADQIQOT NATIJALARI

Aksariyat hollarda axborot xavfsizligiga quyidagi omillar; texnik, huquqiy, inson omillari, raqamli texnologiya yoki raqamli platformalarning xavfsizligining zaifligi hamda ijtimoiy omillar sabab bo'ladi. **Texnik omillar** - odatda raqamli muhitda foydalanuvchilar qo'ygan parollarning zaifligi, takroriyligi va ikki bosqichli autentifikatsiyaning yo'qligi sabab bo'ladi. **Huquqiy omillar** - muayyan davlat yurisdiksiyasi ostidagi hududda raqamli muhit va axborot infratuzilmasini tartibga soladigan qonunchilik hujjatlarining yo'qligi sabab bo'ladi. Natijada bu sohada keskin tartibsizliklar va kiberjinoyatlar soni ortishi kuzatiladi. **Inson omillarida** - muayyan hududdagi fuqarolarning shaxsiy ma'lumotlarini himoya qilish bo'yicha, ijtimoiy tarmoqlardan foydalanishda savodxonlik darajasi yahshi bo'ladi, davlat yuridiksiyasi ostida kiber huquq sohasida kerakli qonunlar ishlab chiqilgan va amaliyotga tadbiiq etilgan bo'ladi. Biroq jinoyatchilar tomonidan sun'iy ravishda hakerlik, viruslar tarqatish kabi yo'llar bilan kiberhujumlar sodir qilinadi. Kiberjinoyatchilikni amalga oshirishda eng ko'p qo'llanadigan kiberhujumlar: phishing, DDoS, ransomware, deepfake, botnet zararli dasturlar, SQL Injection, parollarni buzish hisoblanadi.

Quyida O'zbekistonda eng keng tarqalgan kiberhujumlarni tahlil qilamiz. **Phishing hujumlari** kiberjinoyatchilar tomonidan eng ko'p ishlatiladigan bo'lib, bu hujumlar foydalanuvchilarni aldashga asoslangan soxta sms, soxta elektron pochta, ijtimoiy tarmoqlardagi soxta profillardan xabarlar va haqiqiydek ko'rinadigan web-sitelardan foydalangan holda amalga oshiriladi. O'zbekistonda phishing hujumlari asosan bank karta ma'lumotlari, onlayn to'lov tizimlari (click, pay me), shaxsiy identifikatsiya ma'lumotlari (passport raqami, login va parollar) o'g'irlashga qaratilgan. Misol uchun foydalanuvchilarga mahalliy banklar yoki to'lov tizimlari nomidan yuborilgan soxta xabarlar orqali ularni maxsus yaratilgan veb-saytlarga yo'naltirib, login va parollarini kiritishlari talab qilinadi³. Bunday hujumlarning muvaffaqiyati ko'pincha foydalanuvchilarning raqamli savodxonligi pastligi, kiberxavfsizlik bo'yicha bilim yetishmasligi va ijtimoiy muhandislik usullarining murakkabligi bilan bog'liq. Interpol ma'lumotlariga ko'ra, dunyo bo'ylab har kuni 1,5 milliondan ortiq phishing xabarlar tarqatiladi va O'zbekistonda bu xabarlar katta qismi mahalliy foydalanuvchilarga, xususan, bank xizmatlaridan faol foydalanuvchilarga yo'naltiriladi. 2024-yilda O'zbekistonda phishing hujumlari natijasida fuqarolarning taxminan 15 million dollarlik mablag'i o'g'irlandi, bu esa muammoning jiddiyligini ko'rsatadi⁴. Ransomware – zararli dastur bo'lib kompyuterdagi fayllarga kirishni bloklab yoki shifrlab qo'yadi. Natijada, shaxs kompyuteridagi fayllarga kira olmaydi, virus esa undan tovon puli talab qiladi. Shu sababli, ransomware so'zi ingliz tilida tovon puli degan ma'noni anglatadi. **DDoS hujumi** - bu tizimga, serverga juda ham ko'p so'rov yuborish natijasida uni qotirish va

³ <http://www.wosjournals.com/index.php/shokh/article/view/7134/7515>

⁴ file:///C:/Users/user/Downloads/pcadmin.+2_5258270826326680580.pdf

vaqtincha ishdan chiqarish hisoblanadi. Misol uchun 2016-yil **21-oktyabr** kuni Dyn serverlariga katta **Distributed Denial of Service attack** hujumi amalga oshirildi. Bu hujum natijasida ko'plab mashhur internet xizmatlari vaqtincha ishlamay qoldi. Olimlarning aytishicha o'sha vaqtda hujum paytida **100 mingdan ortiq zararlangan qurilmalar** serverga zararli trafik yuborgan va DNS tizimi vaqtincha ishlamay qolgan⁵. Shu sababli, ko'p olimlar tomonidan XXI-asr raqamlashgan ma'lumotlar asri deb baholanadi. Eng ko'p axborot xavfsizligi va shaxsiy ma'lumotlar himoyasiga oid jinoyatlar raqamli muhitda sodir bo'lmoqda.

Raqamli ma'lumotlarni himoya qilish mexanizmlari. O'zbekiston Respublikasi va xalqaro qonunchilik tahlili: xalqaro maydonda raqamli ma'lumotlar noqonuniy tarqatilishi hollari uchrab turadi. Misol uchun AQSH da 2020-yilning yanvar oyida New-York Times Clearview AI startapi bilan bog'liq shov-shuvli xabarni e'lon qildi. Ma'lum bo'lishicha Clearview AI kompaniyasi Facebook, You-tube, Venmo kabi ko'plab ochiq veb-sitelardan foydalanuvchilarning 3 milliarddan ortiq fotosuratlarini ularning roziligisiz “skrapping” (avtomotlashtirilgan yig'ish) usuli orqali yig'ib olgan va ulkan biometric ma'lumotlar bazasini yaratgan. Bu ulkan ma'lumotlar bazasini esa politsiyaga sotgan⁶. Biometrik ma'lumotlarni yig'ish va qayta ishlash faqat aniq rozilik asosida amalga oshirilishi shart. Shaxsiy ma'lumotlarning politsiyaga sotilishi davlatning fuqarolarining hayotiga ortiqcha aralashuvini anglatadi. Axloqiy va huquqiy muammolarni keltirib chiqaradi. Ushbu xodisa shaxsga doir ma'lumotlar sohasida aniq va qat'iy talabga ega bo'lgan, chegaralar belgilangan fuqarolarning huquqlarini himoya qilish mexanizmi va qonunchilik ishlab chiqilishi zarurligini ko'rsatadi.

Xalqaro miqyosda kiber huquq sohasida axborot daxlsizligi va maxfiylik siyosatining asosiy tayanchi – GDPR (General Data Protection Regulation) ya'ni Yevropa Ittifoqining “Ma'lumotlarni himoya qilishning umumiy reglamenti” hisoblanadi. GDPR – xalqaro miqyosda ancha obro'li hujjat bo'lib, ushbu sohada global standart hisoblanadi. Buning asosiy sababi esa mukammal ishlangan huquqiy hujjat XXI-asrda shaxsga doir ma'lumotlar subyektlariga keng imkoniyatlar va daxlsizlik huquqini taqdim etadi. Ma'lumotlardan foydalanuvchi tashkilotlarga esa qat'iy majburiyatlar yuklaydi. Shu sababli ko'p davlatlar GDPR modeli asosida o'z qonunchiligini takomillashtirmoqda. Shu jumladan O'zbekiston ham Shaxsga doir ma'lumotlar to'g'risidagi qonunini ushbu model asosida ishlab chiqqan. Shaxsga doir ma'lumotlar to'g'risidagi qonun 2019-yilda qabul qilingan bo'lib, uning qo'llanilish sohasi shaxsiy ma'lumotlarni yig'ish, saqlash, uzatish, qayta ishlash sohasidagi ijtimoiy munosabatlarni tartibga solish hisoblanadi. Shuningdek, kiber huquq sohasida O'zbekiston qonunchiligining asosiy tayanchi sifatida xizmat qiladi.

Raqamli muhitning eng zamonaviy institutlaridan biri bu GDPR ning 17-moddasiga asosan “Right to be forgotten” ya'ni unutilish huquqidir. Ushbu huquq 2014-yilda Yevropa Ittifoqi Adliya sudining “Google Spain” ishi bo'yicha shakllantirilgan⁷. Unga ko'ra foydalanuvchi shaxsiy qidiruv tizimlaridan (google yoki yandex) o'zi haqidagi haqiqatga to'g'ri kelmaydigan, eskirgan, noaniq ma'lumotlarni o'chirib tashlashni talab qilish huquqiga ega. O'zbekiston qonunchiligida, Shaxsga doir ma'lumotlar to'g'risidagi qonunda **unutilish huquqi** to'g'ridan-to'g'ri keltirilmagan. Biroq uning 30-moddasida shaxs o'zi haqidagi ma'lumotlari noaniq yoki to'liq bo'lmagan holatlarda ma'lumotlariga ishlov berishni vaqtinchalik to'xtatib turishni talab qilish huquqiga ega.

⁵ <https://www.csidb.net/csldb/incidents/83c278be-382b-4a32-a922-b5a64c4d2e58/>

⁶ <https://arstechnica.com/tech-policy/2020/02/facebook-youtube-order-clearview-to-stop-scrapping-them-for-faces-to-match/>

⁷ <https://www.loc.gov/item/global-legal-monitor/2014-05-21/court-of-justice-of-the-european-union-decision-upholds-right-to-have-personal-data-erased>

Shuningdek 17-moddada fuqaro shaxsiy ma'lumotlaridan ko'zlangan maqsadga erishilganda yoki roziligini chaqirib olganda ularni yo'q qilishni talab qilishi mumkin.

Biroq shaxsiy ma'lumotlar xavfsizligiga tahdid soluvchi dolzarb omillardan biri Big Data hisoblanadi. Hozirgi kunda biz foydalanayotgan ko'pgina ijtimoiy tarmoqlar va veb-sitetlar bizning shaxsiy ma'lumotlarimizni qayta ishlash va qulaylik yaratish maqsadida olishadi. Shuningdek, ular ma'lumotlarni qayta ishlash jarayonida depersonalized (shaxssizlantiriladi) qilinadi. Biroq huquqiy muammo shundaki, Big Data ya'ni shaxssizlantirilgan ma'lumotlarni qaytadan de-anonimizatsiya texnologiyalari orqali muayyan bir shaxs bilan bog'lash mumkin. Aynan shaxssizlantirilgan ma'lumotlarni de-anonimizatsiya qilish orqali muayyan bir shaxs bilan bog'lash imkoniyati maxfiylik siyosatiga ziddir. Shaxsiy ma'lumotlar himoyasiga katta tahdid deb baholanadi. Bundan tashqari bu usul Shaxsga doir ma'lumotlar to'g'risidagi qonun normalarini ham amalda chetlab o'tadi. Chunki hali O'zbekiston qonunchiligida Big Data'ga egalik qilish huquqi ya'ni Data Ownership to'liq tartibga solinmagan.

QONUNCHILIKKA TAKLIFLAR

1. Right to be forgotten ya'ni unutilish huquqini kiber huquq sohasida O'zbekiston qonunchiligiga to'g'ridan-to'g'ri kiritish. Shaxsga doir ma'lumotlar to'g'risidagi qonunda uning o'rnini to'ldiruvchi moddalar bo'lishiga qaramasdan, unutilish huquqining o'rnini to'ldira olmaydi. Shu sababli ham ushbu huquq to'g'ridan-to'g'ri kiritilishi zarur.

2. Big Data va Data ownership (ma'lumotlarga egalik qilish huquqini tartibga solish) institutini tartibga soluvchi qonunchilik hujjatlarini takomillashtirish. Ushbu institutni tartibga solmaslik dolzarb muammolarni keltirib chiqaradi. Chunki O'zbekiston Respublikasi fuqarolarining aksariyati foydalanadigan Instagram, Facebook, Telegram, Twitter kabi ijtimoiy tarmoqlarning ma'lumot bazalari davlat hududida joylashmagan. Shu sababli ham ushbu soha dolzarb, muammoli va nazoratsiz hisoblanadi.

3. **Aholining huquqiy savodxonligini takomillashtiruvchi institutlarni rivojlantirish. Raqamli savodxonlikni aholi o'rtasida oshirish mexanizmlarini shakllantirish.** Hozirgi kunda aksariyat fuqarolarning raqamli savodxonligi qoniqarli darajada emas. Shu sababli ham maktablarda 1-sinf dan raqamli savodxonlikni oshiruvchi va shaxsiy ma'lumotlar himoyasini o'rgatuvchi to'garaklar bosqichma-bosqich ishlab chiqilishi lozim. Natijada biz maktablardan raqamli savodxon va raqamli XXI-asr talablariga javob bera oladigan avlodni tarbiyalaymiz.

4. **Axborot xavfsizligi va shaxsga doir ma'lumotlar himoyasi bo'yicha xalqaro hamkorlikni rivojlantirish va muayyan davlatlar o'rtasida amal qiladigan umumiy standartlarni ishlab chiqish.** Rivojlangan davlatlar bilan xalqaro hamkorlik bizga keng imkoniyatlar yaratadi. Jumladan: axborot xavfsizligi va shaxsiy ma'lumotlar himoyasida xalqaro tajribani chuqur o'rganish, almashish va kiber huquq sohasida kadrlarni rivojlantirishga yordam beradi. Ular bilan birgalikda umumiy standartlar va me'yorlarni ishlab chiqish esa axborotlarni transchegaraviy o'tkazishda huquqiy kolliziyalar kelib chiqishini oldini oladi.

Ushbu tashabbuslarni milliy qonunchilik va amaliyotga kiritish raqamli axborot asrida ma'lumotlar xavfsizligi sohasida shaxslarning huquqlarini himoya qilishga keng imkoniyatlar yaratadi. Shuningdek, milliy qonunchiligimizni yana bir pog'ona ko'tarib, xalqaro standartlarga moslashtiradi.

XULOSA

XXI-asrda shaxsiy ma'lumotlar va axborot xavfsizligi global muammoga aylanib ulgurdi. Shuningdek, raqamli texnologiyalarning rivojlanishi ijtimoiy munosabatlarning raqamlashishiga olib keldi. Natijada phishing, DDoS, ransomware, identity theft kabi kiberjinoyatlar soni keskin

oshmoqda. Bu esa avvalo raqamli texnologiyalardan foydalanuvchilar o'rtasida raqamli savodxonlikni oshirish, milliy qonunchiligimizni takomillashtirish va fuqarolarning huquqlarini himoya qilishning yangi mexanizmlarini ishlab chiqishni talab qiladi. O'zbekistonda kiberhuquq sohasida qonunchilik shakllantirilgan bo'lsada, Big Data, sun'iy intellekt, Data ownership kabilar yetarli darajada tartibga solinmagan. Xalqaro tajriba va GDPR shaxsiy ma'lumotlar himoyasida fuqarolarning huquqlarini himoya qiluvchi qat'iy talablar, aniq mexanizmlar, samarali nazorat tizimi va kafolatlar muhim ahamiyat kasb etishini ko'rsatadi.

Adabiyotlar, References, Литературы:

1. Kiber huquq (Matn): o'quv qo'llanma / Abdihakimov Islombek Bahodir o'g'li. – T.: TDYU nashriyoti, 2025 – 218-b
2. <https://timesofindia.indiatimes.com/technology/tech-news/india-records-265-million-cyber-attacks-in-2025-report/articleshow/125772984.cms>
3. <https://www.justice.gov/archives/opa/pr/three-irgc-cyber-actors-indicted-hack-and-leak-operation-designed-influence-2024-us>
4. <https://www.csidb.net/csldb/incidents/83c278be-382b-4a32-a922-b5a64c4d2e58/>
5. <https://arstechnica.com/tech-policy/2020/02/facebook-youtube-order-clearview-to-stop-scraping-them-for-faces-to-match/>
6. <https://arstechnica.com/tech-policy/2020/02/facebook-youtube-order-clearview-to-stop-scraping-them-for-faces-to-match/>
7. <https://www.loc.gov/item/global-legal-monitor/2014-05-21/court-of-justice-of-the-european-union-decision-upholds-right-to-have-personal-data-erased>