LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 12(2025) / ISSN 3030-3052 Available at www.uznauka.uz

YURIDIK MA'LUMOTLARNING RAQAMLI XAVFSIZLIGI VA KIBERTAHDIDLAR

Musaxonov Asadulloxon To`xtaxo`ja o`g`li
Toshkent davlat yuridik universiteti
Xususiy huquq fakulteti 1- bosqich 3-guruh V patok talabasi
Email:musaxnovasadulloh@gmail.com

***Annotatsiya**: ushbu maqola yuridik tashkilotlar,advakatlik buyrolari,sud organlari va boshqa huquqiy subyektlar faoliyatida raqamli ma'lumotlarni himoya qilishning dolzarbligi tahlil qilinadi. Raqamli tizimlarning kengayishi bilan birga kibertahdidlar, xususan ma'lumotlar o'g'rilash, ruxsatsiz kirish, fishing, zararli dasturlar va ichki xodimlar tomonidan sodir etilishi mumkin bolgan xavflar kuchaygan. Maqola yuridik ma'lumotlar uchun xavfsizligi protokollar, shifrlash mexanizmlari, foydalanuvchi autentifikatsiya va xavfsizlik siyosatining amaliy ahamyatini ko'rsatib beradi.*

Ushbu maqolada yuridik ma'lumotlarning raqamli xavfsizligini ta'minlashning zamonaviy mexanizmlari, kibertahdidlarning turlari va ularning huquqiy jarayonlarga ta'siri chuqur tahlil qilinadi. Raqamli tizimlar keng qo'llanilayotgan hozirgi davrda ma'lumotlar bazalariga ruxsatsiz kirish, kiberhujumlar, fishing, zararli dasturiy vositalar, shaxsga doir ma'lumotlarning sizib chiqishi kabi xavflar keskin oshgani ta'kidlanadi. Maqolada O'zbekiston Respublikasining axborot xavfsizligi bo'yicha amaldagi qonunlari, xalqaro standartlar hamda kiberxavfsizlik strategiyalarining yuridik jarayonlarni himoyalashdagi o'rni yoritiladi. Shuningdek, tashkilotlar uchun texnik, tashkiliy va huquqiy choralarni uyg'un qo'llash, xodimlar malakasini oshirish, kiberhujumlarni erta aniqlash va oldini olish mexanizmlarini kuchaytirish bo'yicha takliflar beriladi.

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 12(2025) / ISSN 3030-3052 Available at www.uznauka.uz

Kalit so`zlar: *Raqamli, xavfsizlik, yuridik, ma'lumotlar, kibertahdidlar, shifrlash, malumotlarni himoya'qlish, fishing, kiberhujumlar, voqealarga, malumotlar, bazasi xavfsizligi, himoya pratakollari, maxfilig, ichki xavflar, tarmoq xavfsizligi,kiberjinoyatlar.*

Kirish:

Raqamlash jarayonida tezlashishi yuridik xizmatlar sohasida ham jiddiy o`zgarishlarga sabab bolmoqda sud hujjatlari, mijozlar ma'lumotlari, shartnomalar, electron dalillr va advakat mijoz yozishmalari endi ko`p hollarada electron shaklda saqlanadi.[1] Bu esa yuridik tashkilotlar oldida muhm vazifani ma`lumotlarning raqamli xavfsizligini ta'minlash masalasini qo`yadi.[2]

Bugungi kunda kiber tahdidlar ko`lami kengayib bormqda. Yuridik sektor cyberjinoyatchilar uchun jozibador yo`nalish hisoblanadi,chunki unda moliyaviy, shaxsiy va maxfiy huquqiy hujjatlar jamlangan. Malumotlar bazasiga ruxsatsiz kirish, fishing orqali parollarni qo`lga kiritish,zararli dasturlar bilan tizimlarni bloklash yoki ma'lumotlarni shirflab tovon talab qlish kabi xurjlar eng ko`p uchraydigan tahdidlardir. Bundan tashqari, ichki xodimlar tomonidan qoida buzarlik yoki beparvolik tufayli yuzaga keladigan xavflar hamda dolzarbligicha qolmoqda.

Shu sababli yuridik tashkilotlar axborot xavfsizligini kuchaytirish, tizimlarining zaif nuqtalarni aniqlash, muntazam audit o'tkazish kuchli parollar siyosati, ikki bosqichli autentifikatsiya va shifrlash texnalogiyalaridan foydalanish zamon talabi hisoblanadi. Ushbu maqolada aynan shunday xavfsizlik choralari va ularning yuridik ma'lumotlarni himoya qilishdagi ro`li yoritib beriladi.

Asosiy qism:

[1] https://lex.uz/docs/-3098964.
[2] https://lex.uz/ru/docs/-5482934.

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 12(2025) / ISSN 3030-3052 Available at www.uznauka.uz

Raqamli texnologiyalar jadal rivojlanib borayotgan hozirgi davrda yuridik tashkilotlarning faoliyati ham tubdan o‘zgarib bormoqda. Avvallari huquqiy hujjatlar qog‘oz ko‘rinishida yuritilgan bo‘lsa, bugungi kunda shartnomalar, sud hujjatlari, advokat-mijoz yozishmalari, shaxsiy ma’lumotlar, elektron dalillar va xizmat yozishmalari ko‘pincha raqamli shaklda saqlanadi. Raqamli muhitga o‘tish ma’lumot almashinuvini tezlashtirdi, biroq shu bilan birga yuridik ma’lumotlarning xavfsizligi bilan bog‘liq yangi xavf-xatarlarni ham yuzaga keltirdi. Aynan shu sababli yuridik ma’lumotlar uchun raqamli xavfsizlikni ta’minlash hozirgi paytda asosiy masalalardan biridir.

O‘zbekiston Respublikasi yuridik ma’lumotlar xavfsizligini himoya qilish bo‘yicha bir necha asosiy qonunlarga ega.[3] Ulardan eng birinchisi — “Shaxsiy ma’lumotlar to‘g‘risida”gi Qonun bo‘lib, ushbu qonun shaxsiy ma’lumotlarni yig‘ish, saqlash, qayta ishlash va uchinchi shaxsga berish jarayonlarini qat’iy tartibga soladi. Qonun asosida shaxsning roziligisiz uning ma’lumotlarini tarqatish yoki sotish man etiladi. Bu nafaqat jismoniy, balki yuridik tashkilotlarga ham qat’iy talablardan birini belgilaydi. Yuridik ma’lumotlar tarkibida, ko‘pincha mijozlar, sud jarayonidagi ishtirokchilar yoki kompaniyalar haqidagi shaxsiy ma’lumotlar mavjud bo‘lgani sababli, bu qonunning amal qilishi raqamli xavfsizlikning eng muhim bo‘g‘inidir.

Bundan tashqari, “Axborotlashtirish to‘g‘risida”gi Qonun,[4] “Elektron hukumat to‘g‘risida”gi Qonun, “Elektron raqamli imzo to‘g‘risida”gi[5] Qonun va axborot resurslari bilan ishlashga doir boshqa me’yoriy hujjatlar yuridik ma’lumotlar xavfsizligini ta’minlashda muhim o‘rin tutadi. Bu qonunlarda axborot

[3] https://lex.uz/acts/-52268.
[4] https://lex.uz/mact/-83472.
[5] https://lex.uz/docs/-6234904.

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 12(2025) / ISSN 3030-3052 Available at www.uznauka.uz

tizimlariga qo‘yiladigan texnik talablar, ma’lumotlarni qayta ishlash tamoyillari, shifrlash va autentifikatsiya usullari, ruxsatsiz kirishdan himoya qilish mexanizmlari aniq belgilangan. Mazkur huquqiy hujjatlar orqali yuridik tashkilotlarda raqamli xavfsizlik faqat tavsiya emas, balki majburiy talablardan biriga aylangan

Kibertahdidlar turining kengayib borishi yuridik ma’lumotlarni yanada himoyasiz qoldirmoqda. Eng ko‘p uchraydigan xurujlardan biri — fishing bo‘lib, u soxta elektron xabarlar yoki havolalar orqali foydalanuvchi parolini qo‘lga kiritishni maqsad qiladi. Yuridik tashkilotlarda xodimlar ko‘pincha pochta orqali ko‘p miqdorda hujjatlar bilan ishlaydiganligi sababli fishing xatlari sezilmay qolishi mumkin. Bunday hujum natijasida butun ma’lumotlar bazasiga ruxsatsiz kirish imkoni paydo bo‘ladi

Yana bir keng tarqalgan xuruj turi — ransomware. Bu zararli dasturlar tizimdagi barcha fayllarni shifrlab qo‘yadi va ularni tiklash uchun tovon puli talab qiladi. Sud materiallari, mijozlar arxivlari yoki korporativ shartnomalar singari muhim ma’lumotlar shifrlab qo‘yilganida, yuridik tashkilotning faoliyati butunlay to‘xtab qolishi mumkin. Shuningdek, DDoS hujumlar[6], tarmoqga noqonuniy kirish, ma’lumotlarni yashirincha o‘zgartirish, ichki xodimlarning noto‘g‘ri harakatlari ham eng xavfli tahdidlardan hisoblanadi. Ichki xodimlar tomonidan sodir etiladigan xavflar ko‘pincha beparvolik yoki mas’uliyatsizlik oqibatida yuzaga keladi. Masalan, xodimning kuchsiz parol ishlatishi, himoyalanmagan USB qurilmadan foydalanishi yoki ma’lumotlarni shaxsiy qurilmalarida saqlashi katta xavf tug‘diradi.

[6] https://uz.wikipedia.org/wiki/DoS_hujum.

Issue - 12(2025) / ISSN 3030-3052 Available at www.uznauka.uz

Shu sababli yuridik tashkilotlar o‘z tizimlarida texnik himoya choralarini joriy etishi shart. Bularning eng muhimi — shifrlash texnologiyalari. Shifrlash ma’lumotlarni ruxsatsiz shaxslar tomonidan o‘qilmasligi uchun ularni kodlaydi.[7] Ayniqsa advokat-mijoz yozishmalarida shifrlangan kanal (masalan, VPN, TLS) orqali ma’lumot almashish zarur.Avtentifikatsiya tizimida ikki bosqichli tasdiqlash (2FA) qo‘llanilishi kerak. Bu foydalanuvchidan nafaqat parol, balki qo‘shimcha tasdiqlash — SMS-kod, mobil ilovadagi token yoki biometrik ma’lumotni kiritishni talab qiladi. Bu tizim ruxsatsiz kirishning oldini olishda eng samarali vositalardan biridir.

Foydalanuvchi huquqlarini boshqarish ham muhim o‘rin tutadi. Har bir xodim faqat o‘z vazifasi bilan bog‘liq bo‘lgan ma’lumotlargina kira olishi kerak. Bu “eng kam ruxsat” tamoyili deb ataladi. Masalan, kotibiyat bo‘limidagi xodimga mijozlarning moliyaviy hujjatlari yoki ichki shartnomalar bazasiga kirish huquqi berilmasligi kerak.Ma’lumotlarni zaxiralash (backup) ham raqamli xavfsizlikning zarur qismidir. Zaxira nusxalar alohida, himoyalangan serverda saqlanishi va muntazam yangilanib borishi shart. Aks holda ransomware yoki tizim ishdan chiqqanida barcha ma’lumotlar butunlay yo‘qolib ketishi mumkin.

Huquqiy jihatdan qaraganda, O‘zbekistonda raqamli xavfsizlik bo‘yicha majburiyatlar tobora kuchayib bormoqda. Davlat organlari va ko‘plab yuridik shaxslar uchun axborot tizimlarining zaifliklarini muntazam aniqlash, axborot xavfsizligi bo‘yicha mas’ul xodimlar tayinlash va maxsus protokollarga amal qilish talab qilinmoqda. Bu esa yuridik ma’lumotlar xavfsizligini faqat texnik masala emas, balki to‘liq huquqiy majburiyat sifatida qarash zarurligini ko‘rsatadi.Yuridik tashkilotlar kibertahdidlardan himoyalanish uchun nafaqat texnik vositalar, balki

[7] https://lex.uz/docs/-4396419.

tashkiliy choralarni ham qo‘llashi lozim. Xodimlarni muntazam ravishda axborot xavfsizligi bo‘yicha o‘qitish, ularga fishing xatlarni aniqlashni o‘rgatish, xavfsizlik siyosati bo‘yicha qat’iy qoidalar joriy etish zarur. Ichki nazorat tizimi, jurnal yuritish, hujjat aylanishi bo‘yicha monitoring ham muhim ahamiyatga ega.[8]

Raqamli xavfsizlikning yuridik sohada yanada mustahkamlanishi uchun xalqaro standart va normalarga moslashuv ham muhim o‘rin tutadi. Bugungi kunda ko‘plab davlatlar va yirik tashkilotlar ISO/IEC 27001 axborot xavfsizligi boshqaruv standartini qo‘llashmoqda[9]. Ushbu standart ma’lumotlarni tasniflash, xavflarni aholash, xavfsizlik siyosatini ishlab chiqish, texnik himoya choralarini tartibga solish va doimiy monitoringni o‘z ichiga oladi. Yuridik tashkilotlar ham ushbu standartga mos ishlash orqali o‘z ma’lumotlarini xalqaro talablar asosida himoya qila oladi.Shuningdek, yuridik tashkilotlar faoliyatida GDPR (General Data Protection Regulation) kabi xalqaro qoidalar ham dolzarblik kasb etadi, ayniqsa chet ellik mijozlar bilan ishlaganda. Ushbu reglament shaxsiy ma’lumotlarni minimal miqdorda yig‘ish, aniq maqsadga yo‘naltirish va foydalanuvchining ma’lumotlarini o‘chirish huquqi kabi tamoyillarni belgilaydi.[10] Garchi GDPR O‘zbekistonda majburiy bo‘lmasa-da, xalqaro aloqalar kuchayib borar ekan, yuridik sohaga uning talablariga moslashish zarur bo‘lmoqda.

Raqamli xavfsizlikning yana bir muhim yo‘nalishi — kiberhujumlarga tayyorgarlik va voqealarga javob berish tizimidir. Har qanday tashkilot yo kiberhujumni butunlay to‘xtata olmaydi, yo bo‘lmasa uni to‘liq oldindan bilib bo‘lmaydi. Shu sababli “zero-trust” (nol ishonch) modeli qo‘llanilmoqda. Bu modelga ko‘ra, hatto ichki tarmoq foydalanuvchilari ham avtomatik tarzda

[8] https://lex.uz/docs/-6166539.
[9] https://lex.uz/docs/-4390513.
[10] https://lex.uz/acts/-5482934.

Issue - 12(2025) / ISSN 3030-3052 Available at www.uznauka.uz

ishonchli deb hisoblanmaydi. Har bir amal, har bir kirish urinishida autentifikatsiya talab qilinadi. Bu usul ayniqsa yuridik ma'lumotlar kabi maxfiy axborot bilan ishlaganda juda samarali.Kibertahdidlar kuchayishi yuridik javobgarlik masalasini ham o'rtaga qo'yadi. Ma'lumotlarni himoya qilish bo'yicha belgilangan talablarga rioya qilinmasa, tashkilotlar intizomiy, ma'muriy yoki fuqaroviy javobgarlikka tortilishi mumkin. Ba'zi holatlarda, masalan, ma'lumotlarning ommaga sizib chiqishi oqibatida mijozlar manfaatiga zarar yetkazilsa, qurbonlar tomonidan sudga murojaatlar ham ko'payishi mumkin. Bu esa yuridik tashkilotlar uchun reputatsion yo'qotishlarni yanada kuchaytiradi

Raqamli xavfsizlikning muhim qismi — ma'lumotlarning hayotiy siklini boshqarishdir. Ma'lumotlar o'z vaqtida arxivlanishi, ortiqcha nusxalar o'chirib borilishi, yaroqsiz yoki muddati o'tgan ma'lumotlar maxsus tartibda yo'q qilinishi lozim. Ma'lumotlarni yillar davomida keraksiz holda saqlash ularni extimoldagi hujumlar uchun oson nishonga aylantiradi. Yuridik tashkilotlar ma'lumotlarni saqlash muddati bo'yicha ichki normativlarni ishlab chiqishi zarur. Bundan tashqari, yuridik sohada raqamli etik qoidalar ham tobora ahamiyat kasb etmoqda. Advokatlar, yuristlar va sud xodimlari elektron tizimlar bilan ishlaganda mijozlar huquqlarini hurmat qilishi, ularning roziligisiz ma'lumotlarni ko'chirib olmasligi, tarqatmasligi va shaxsiy fayllardan foydalanmasligi kerak. Raqamli etikaga xilof harakatlar, hatto texnik jihatdan hech qanday zarar yetkazmasa ham, huquqiy va intizomiy jazoga sabab bo'lishi mumkin.[11]Yuridik tashkilotlar ko'plab hollarda tashqi IT-xizmat ko'rsatuvchi kompaniyalardan foydalanadi. Bu esa outsourcing xavfsizligi masalasini dolzarb qiladi. Tashqi kompaniya ma'lumotlarga cheklangan

[11] https://parliament.gov.uz/articles/2211.

Issue - 12(2025) / ISSN 3030-3052 Available at www.uznauka.uz

darajada kirishi, shartnoma asosida maxfiylikni ta’minlashi, barcha xavfsizlik talablariga rioya qilishi shart. Shartnomalarda ma’lumotlarni himoya qilish, javobgarlik, audit o‘tkazish huquqi va kiberhujum sodir bo‘lganda choralar bo‘yicha alohida bandlar bo‘lishi lozim.

Kelgusida yuridik sohada sun’iy intellekt, neyrotarmoqlar va avtomatik hujjatlashtirish tizimlari yanada keng qo‘llanilishi kutilmoqda. Bu texnologiyalar tezlik va qulaylikni oshirgan holda, yangi xavf turini ham yuzaga chiqaradi — algoritmik tahdidlar. Sun’iy intellektga asoslangan tizimlarga noto‘g‘ri ma’lumot kiritish yoki ularni manipulyatsiya qilish yuridik qarorlar sifatiga bevosita ta’sir ko‘rsatishi mumkin. Shu sababli kelajakda sun’iy intellekt bilan ishlaydigan yuridik tizimlar uchun alohida xavfsizlik standartlari ishlab chiqilishi ehtimol.Umuman olganda, yuridik ma’lumotlarning raqamli xavfsizligi tobora murakkablashib borayotgan jarayondir. Tashkilotlar texnik vositalar, huquqiy talablar, xalqaro standartlar va xodimlarning bilimini uyg‘unlashtirib, kompleks yondashuv asosida ishlagan taqdirdagina kibertahdidlar bilan muvaffaqiyatli kurasha oladi.

Xulosa:

Raqamli texnologiyalar jadal rivojlanib borayotgan hozirgi davrda yuridik ma’lumotlarning xavfsizligini ta’minlash davlat boshqaruvi, sud-huquq tizimi va xususiy sektor faoliyatining ajralmas qismiga aylandi. Ma’lumotlar elektron shaklga o‘tayotgani, sud jarayonlarining raqamlashtirilishi, davlat xizmatlarining onlayn ko‘rinishda ko‘payishi yuridik axborotning qiymatini keskin oshirdi. Shu bilan birga, kiberjinoyatlar, ma’lumotlar sizib chiqishi, ruxsatsiz kirish, shaxsiy identifikatsiya ma’lumotlarining o‘g‘irlanishi kabi xavf-xatarlar ham mutanosib ravishda kuchayib bormoqda. Bu jarayon yuridik ma’lumotlarning ishonchli

Issue - 12(2025) / ISSN 3030-3052 Available at www.uznauka.uz

himoyasini nafaqat texnik, balki normativ-huquqiy darajada ta’minlash zarurligini ko‘rsatadi.

Tahlil shuni ko‘rsatadiki, kibertahdidlar ko‘p qirrali bo‘lib, ularning asosiy qismi sun’iy intellektdan foydalangan holda yaratilayotgan murakkab hujumlar, zararli dasturlar, fishing hujumlari, ma’lumotlar bazasini buzish va davlat yoki xususiy tashkilotlarga qarshi maqsadli kiberhujumlardir. Shu sababli, yuridik ma’lumotlar bilan ishlovchi muassasalar kuchli texnik himoya, ikki bosqichli autentifikatsiya, shifrlash, zaxiralash va muntazam audit kabi choralarni joriy etishi zarur. Bunda inson omili – xodimlarning xabardorlik darajasi, xavfsizlik bo‘yicha ichki tartiblar va kiberhujumlarga qarshi tezkor reaksiya mexanizmlari muhim rol o‘ynaydi.O‘zbekiston va xalqaro huquqiy me’yorlar tahlili shuni ko‘rsatadiki, raqamli xavfsizlikni mustahkamlash bo‘yicha aniq standartlar va majburiyatlar mavjud. “Axborotlashtirish to‘g‘risida”gi Qonun, “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun, kiberxavfsizlik bo‘yicha milliy strategiyalar tashkilotlarning ma’lumotlarni himoya qilish bo‘yicha majburiyatlarini belgilab beradi.[12] Xalqaro miqyosda esa GDPR, ISO/IEC 27001, Budapest Konvensiyasi kabi hujjatlar asosiy mezon sifatida qo‘llaniladi.

Umuman olganda, yuridik ma’lumotlarning raqamli xavfsizligini ta’minlash keng ko‘lamli va uzluksiz jarayondir. Texnik vositalarni yangilash, qonunchilikni takomillashtirish, xodimlarni o‘qitish, xalqaro standartlarni tatbiq etish va raqamli madaniyatni kuchaytirish orqali kibertahdidlarning salbiy oqibatlarini sezilarli darajada kamaytirish mumkin. Yuridik axborotning ishonchli himoyasi sud adolati, davlat boshqaruvi, biznes faoliyati va fuqarolarning huquqlarini ta’minlashning muhim omillaridan biri bo‘lib qolaveradi.

[12] https://lex.uz/docs/-83472.

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 12(2025) / ISSN 3030-3052 Available at www.uznauka.uz

FOYDALANILGAN ADABIYOTLAR:

1 O‘zbekiston Respublikasi, “Shaxsiy ma’lumotlar to‘g‘risida”gi Qonun, Toshkent, 2[1] https://parliament.gov.uz/articles/2211.

2. O‘zbekiston Respublikasi, “Axborotlashtirish to‘g‘risida”gi Qonun, Toshkent, 2019. [1] https://lex.uz/acts/-5482934.

3. O‘zbekiston Respublikasi, “Elektron hukumat to‘g‘risida”gi Qonun, Toshkent, 2018.: https://lex.uz/docs/-83472.

4. ISO/IEC 27001:2013, Information security management systems – Requirements, International Organization for Standardization.: https://lex.uz/docs/-4390513.

5. European Union, General Data Protection Regulation (GDPR), 2018.: https://lex.uz/docs/-6234904

6. Budapest Convention on Cybercrime, Council of Europe, 2001.

7. Dentons, Uzbekistan Tightens Cybersecurity Obligations for Organizations, 2025.

8. Inlibrary.uz, “Shaxsiy ma’lumotlarni himoya qilish va kiberxavfsizlik”, 2023

9. Scientific-jl.com, Cybersecurity in Legal Sector: Analysis and Recommendations.