QO‘QON DAVLAT PEDAGOGIKA INSTITUTI ILMIY XABARLARI
(2025-yil 2-son)

IJTIMOIY FANLAR

SOCIAL STUDIES

YURIDIK HUJJATLARNI HIMOYA QILISHNING XAVFSIZLIK AMALIYOTI

Mavlonov Bahromali Qodirovich
Farg‘ona davlat universiteti
huquq ta’lim kafedrasi o‘qituvchisi
Tel: +99897373604
E-mail: mavlonovbahromaliqodirovich@70gmail.com

Annotatsiya. Yuridik hujjatlarda eng yuqori darajada himoyalanishni talab qiluvchi muhim va maxfiy ma‘lumotlar mavjud. Bugungi raqamli asrda ushbu hujjatlardan ruxsatsiz foydalanish, ularni yo‘qotish yoki o‘zgartirishdan himoya qilish uchun mustahkam xavfsizlik amaliyotlarini amalga oshirish juda muhimdir. Ushbu maqola yuridik hujjatlarni himoya qilish, ularning maxfiyligi va xavfsizligini ta‘minlash bo‘yicha bazi ilg‘or tajribalarni hamda qonuniy hujjatlarni himoya qilishga yordam beradigan bir nechta usullarni o‘rganadi.

Abstract. Legal documents contain sensitive and confidential information that requires the highest level of protection. In today’s digital age, it is essential to implement robust security practices to protect these documents from unauthorized access, loss, or modification. This article explores some best practices for protecting legal documents, ensuring their confidentiality and security, and several techniques that can help protect legal documents.

Абстрактный. Юридические документы содержат конфиденциальную информацию, требующую самого высокого уровня защиты. В современную цифровую эпоху крайне важно внедрять надежные методы безопасности для защиты этих документов от несанкционированного доступа, потери или изменения. В этой статье рассматриваются некоторые передовые методы защиты юридических документов, обеспечения их конфиденциальности и безопасности, а также несколько методов, которые могут помочь защитить юридические документы.

Kalit so‘zlar: yuridik hujjatlar, raqamli imzolar, hujjatni shifrlash, intellektual mulk hujjatlari, raqamli xavfsizlik.

Keywords: legal documents, digital signatures, document encryption, intellectual property documents, digital security.

Ключевые слова: юридические документы, цифровые подписи, шифрование документов, документы интеллектуальной собственности, цифровая безопасность.

Kirish

Yuridik hujjatlarni himoya qilish uchun xavfsizlik amaliyotlari bugungi raqamli asrda muhim ahamiyatga ega. Maxfiy ma’lumotlarning onlayn saqlanishi va uzatilishi ortib borayotganligi sababli, tashkilotlar uchun yuridik hujjatlarni ruxsatsiz kirish, yo‘qotish yoki buzishdan himoya qilish uchun mustahkam xavfsizlik choralarini qo‘llash juda muhimdir yuridik hujjatlar xavfsizligini ta’minlashning asosiy amaliyotlaridan biri bu kirishni kuchli nazorat qilishni amalga oshirishdir. Tashkilotlar buni foydalanuvchi rollarini belgilash va ish majburiyatlarini bilish tamoyiliga asoslangan imtiyozlarini berish orqali o‘rnatishlari kerak. Faqat vakolatli xodimlarga kirishni cheklash orqali tashkilotlar ruxsatsiz shaxslarning qonuniy hujjatlarni buzishi yoki o‘g‘irlashi xavfini kamaytirishi mumkin. Kirish nazoratini yanada kuchaytirish uchun tashkilotlar kuchli parol siyosatini qo‘llashlari kerak.[1] Bu xodimlardan murakkab parollardan foydalanishni talab qilish, ularni muntazam ravishda o‘zgartirish va boshqalar bilan baham ko‘rmaslikni o‘z ichiga oladi. Bundan tashqari, ko‘p faktorli autentifikatsiyani amalga oshirish foydalanuvchilardan qonuniy hujjatlarga kirishdan oldin barmoq izi yoki bir martalik parol kabi qo‘shimcha tekshirishni talab qilish orqali qo‘shimcha xavfsizlik darajasini ta’minlashi mumkin. Yuridik hujjatlarni shifrlash xavfsizlikning yana bir muhim amaliyotidir. Shifrlash-bu ma’lumotlarni ruxsatsiz shaxslar tomonidan oson tushunilmaydigan shaklga aylantirish jarayoni hisoblanadi. Shifrlashni amalga oshirish orqali, hatto, hujjat ushlangan yoki ruxsatsiz foydalanilgan bo‘lsa ham, shifrlash kalitisiz u tushunarsiz bo‘ladi. Bu qonuniy hujjatlarning maxfiyligini va ruxsatsiz ko‘rish yoki o‘zgartirishdan himoyalanganligini ta’minlaydi. Doimiy ravishda yuridik hujjatlarning zaxira nusxasi tashkilotlar tomonidan qabul qilinishi kerak bo‘lgan muhim xavfsizlik amaliyotidir.[2] Ma’lumotlarning yo‘qolishi turli sabablarga ko‘ra sodir bo‘lishi mumkin, jumladan qurilmadagi nosozliklar, inson xatosi yoki kiberhujumlar sababli bo‘lishi mumkin. Tashkilotlar saytdan tashqarida yoki bulutli saqlashni ta’minlash uchun muntazam ravishda yuridik hujjatlarning zaxira nusxasini yaratish orqali yo‘qolgan yoki buzilgan hujjatlarni tezda tiklashlari mumkin, bu esa ma’lumotlar yo‘qolishining mumkin bo‘lgan ta’sirini kamaytiradi. Hujjatlarni boshqarishning xavfsiz tizimlarini joriy etish yuridik hujjatlarni himoya qilishda hal qiluvchi ahamiyatga ega. Ushbu tizimlar yuridik hujjatlarni saqlash, tartibga solish va ularga kirish uchun markazlashtirilgan platformani ta’minlaydi, shu bilan birga mustahkam xavfsizlik xususiyatlarini taklif etadi. Bunga hujjatlar versiyasini nazorat qilish, audit yo‘llari va kirish jurnallari kiradi, bu tashkilotlarga hujjatlar faoliyatini kuzatish va yuridik hujjatlarning yaxlitligi va maxfiyligini ta’minlash imkonini beradi. Xodimlarni xavfsizlik bo‘yicha ilg‘or tajribalarga o‘rgatish yuridik hujjatlarni himoya qilishning muhim jihati hisoblanadi. Ko‘pgina xavfsizlik buzilishlari xodimlarning beparvoligi yoki bilimsizligi tufayli sodir bo‘ladi. Xodimlarni shubhali elektron pochta xabarlarini ochmaslik yoki noma’lum havolalarni bosmaslik kabi xavfsizlik amaliyotlarining ahamiyati haqida o‘rgatish fishing hujumlari kabi umumiy xavfsizlik tahdidlarining oldini olishga yordam beradi.[3] Doimiy xavfsizlik auditlari va baholashlari xavfsizlik infratuzilmasidagi zaifliklarni aniqlash uchun juda muhimdir.

Metodologiya

Xavfsizlik amaliyotlarini davriy ko‘rib chiqish va baholashni o‘tkazish tashkilotlarga xavfsizlik choralaridagi har qanday zaif tomonlar yoki bo‘shliqlarni aniqlashga va ularni bartaraf etish uchun tegishli choralarni ko‘rishga yordam beradi. Bunga dasturiy ta‘minot va tizimlarni yangilash, zaifliklarni tuzatish va kerak bo‘lganda qo‘shimcha xavfsizlik nazoratini amalga oshirish kiradi. Xulosa qilib aytganda,yuridik hujjatlarni himoya qilish turli xil xavfsizlik amaliyotlarini qamrab oluvchi kompleks yondashuvni talab qiladi. Kuchli kirish nazorati va shifrlashni amalga oshirishdan tortib hujjatlarning zaxira nusxasini yaratish va xodimlarni xavfsizlik bo‘yicha ilg‘or tajribalarga o‘rgatishgacha tashkilotlar ruxsatsiz kirish, buzish va yuridik hujjatlarni yo‘qotish xavfini kamaytirishi mumkin.[4] Yuridik hujjatlar xavfsizligini birinchi o‘ringa qo‘ygan holda, tashkilotlar yuridik masalalarda muhim bo‘lgan ishonch va maxfiylikni qo‘llab-quvvatlashlari mumkin. Bugungi raqamli asrda yuridik hujjatlarni himoya qilish muhim ahamiyatga ega. Yuridik hujjatlarda maxfiy va shaxsiy ma’lumotlar mavjud bo‘lib, ular buzilgan taqdirda ham jismoniy shaxslar, ham tashkilotlar uchun jiddiy oqibatlarga olib kelishi mumkin.Ushbu hujjatlarning xavfsizligini ta’minlash maxfiylikni himoya qilish, ishonchni saqlash va turli qonuniy majburiyatlarga rioya qilish uchun juda muhimdir. Yuridik hujjatlarni samarali himoya qilish uchun qo‘llanilishi mumkin bo‘lgan bir nechta xavfsizlik amaliyotlari mavjud. Birinchidan, shifrlash ma’lumotlarni tegishli shifrlash kalitisiz o‘qib bo‘lmaydigan formatga aylantiradigan asosiy xavfsizlik chorasidir. Ikkinchidan, kuchli kirish nazoratini amalga oshirish juda muhimdir.[5] Shuningdek, Pdf parol himoyasi bu hujjat va xavfsizlik tizimlarini himoya qilishning eng oddiy va keng tarqalgan usullaridan biridir. Nomidan ko‘rinib turibdiki, bu usul PDF-fayllaringizni himoya qilish uchun parol himoyasidan foydalanadi. Parol tizimi hujjatni to‘liq himoya qila olmasa ham, hujjatingizga noto‘g‘ri kirishni niyat qilgan yomon shaxslar uchun muammolarni murakkablashtiradi. Biroq, parolni himoya qilish usuli o‘zining kamchiliklariga ega. Masalan, sizning parolingiz allaqachon avtorizatsiya qilingan foydalanuvchilarga uzatilishi mumkin, chunki ular ushbu foydalanuvchilarga o‘qilishi mumkin bo‘lgan so‘z formatida yuborilishi kerak. Yuridik hujjatlarni shifrlash orqali, hatto ular noqonuniy ravishda ushlangan yoki ruxsat etilgan bo‘lsa ham, ma’lumotlar xavfsiz bo‘lib qoladi.

Natijalar

Ushbu xavfsizlik amaliyotining samaradorligini ta’minlash uchun mustahkam shifrlash algoritmlaridan foydalanish va shifrlash kalitlarini qurilma tokenlari yoki parol bilan himoyalangan serverlar kabi xavfsiz joylarda saqlash muhim. Bunga parol bilan himoyalangan hujjat boshqaruv tizimlari yoki xavfsiz fayl almashish platformalaridan foydalanish orqali erishish mumkin. Bundan tashqari, foydalanuvchilarning kirish huquqlarini muntazam ravishda ko‘rib chiqish va yangilash ruxsatsiz kirish xavfini kamaytiradi. Ko‘rib chiqilishi kerak bo‘lgan yana bir xavfsizlik amaliyoti xavfsiz hujjatlarni saqlash yechimlaridan foydalanishdir. Qulflangan shkaflar yoki seyflar kabi jismoniy xavfsizlik choralariga sarmoya kiritish qonuniy hujjatlarning qog‘oz nusxalarini o‘g‘irlik yoki ruxsatsiz kirishdan himoya qilishi mumkin.

Shunga o‘xshab, ma’lumotlarni shifrlash, muntazam zaxira nusxalari va ishonchli kirishni boshqarish vositalarini birinchi o‘ringa qo‘yadigan xavfsiz bulutli saqlash provayderlaridan foydalanish qonuniy hujjatlarning raqamli nusxalarini himoya qilishni ta’minlaydi.[6] Bundan tashqari, Jismoniy nusxalarni maydalash va raqamli fayllarni xavfsiz yo‘q qilish ma’lumotni qaytarib bo‘lmaydigan qilishning samarali usullaridir. Bundan tashqari, qonuniy hujjatlarni himoya qilish uchun muntazam ma’lumotlarning zaxira nusxalarini yaratish juda muhimdir. Muhim yuridik ma’lumotlarni yo‘qotish xavfini kamaytirish uchun kamida bitta saytdan tashqarida saqlangan bir nechta zaxira nusxalarini saqlash zarur. Bundan tashqari, xodimlarga xavfsizlik bo‘yicha ilg‘or tajribalarni o‘rgatish hujjatlar himoyasini kuchaytirishda muhim ahamiyatga ega. Xodimlarni yuridik hujjatlarni himoya qilish, kuchli parollarni o‘rnatish, fishingga urinishlarni aniqlash va xavfsizlikka potentsial tahdidlarni tan olish muhimligini o‘rgatish xavfsizlikni buzish ehtimolini sezilarli darajada kamaytirishi mumkin. Nihoyat, muntazam ravishda xavfsizlik auditi va baholashlarini o‘tkazish zaifliklarni aniqlashga va hujjatlar himoyasini yaxshilashga yordam beradi. Maxfiy yuridik hujjatlarni himoya qilish nafaqat maxfiylik va ishonchni saqlab qoladi, balki qonuniy talablar va majburiyatlarga rioya qilishni ham ta’minlaydi.

Muhokama qismi

Yuridik hujjatlarni mustahkam himoya qilish tizimini joriy etish, muntazam ravishda fayllarning zaxira nusxasini yaratish, kirishni boshqarish vositalarini joriy etish, maxfiy ma’lumotlarni shifrlash, jismoniy xavfsizlikni ta’minlash, xodimlarni o‘qitish va muntazam xavfsizlik tekshiruvlarini o‘tkazish bularning barchasi xavfsizlik bo‘yicha muhim amaliyotlardir. Shuningdek, O‘zbekiston Respublikasining ‘‘Kiberxavfsizlik to‘g‘risida’’gi Qonunida ham kiberxavfsizlik sohasida ishlab chiqiladigan normativ-huquqiy hujjatlarni va texnik jihatdan tartibga solish sohasidagi normativ hujjatlarni vakolatli davlat organi bilan kelishishi kerakligi belgilab qo‘yildi.[7] Ushbu chora-tadbirlarni amalga oshirish orqali yuridik mutaxassislar, davlat organi xodimlari yuridik hujjatlarning maxfiyligi, yaxlitligi va mavjudligini himoya qilishlari pirovardida o‘z mijozlarining manfaatlarini himoya qilishlari va ularning professional obro‘sini saqlab qolishlari mumkin. Ushbu texnologiya rivojlangan davrda yuridik hujjatlarni himoya qilish eng muhim ahamiyatga ega. Yuridik hujjatlar mijozning muhim ma‘lumotlaridan tortib, maxfiy sud hujjatlarigacha himoya qilinishi kerak bo‘lgan shaxsiy ma’lumotlarni o‘z ichiga oladi. Tegishli xavfsizlik amaliyoti bo‘lmasa, yuridik mutaxassislar va ularning mijozlari o‘z ma’lumotlarining noto‘g‘ri qo‘llarga tushishi va halokatli oqibatlarga olib kelishi mumkin.yuridik hujjatlarni himoya qilishning asosiy xavfsizlik amaliyotlaridan biri bu kuchli parollar va kirishni boshqarish vositalarini joriy qilishdir. Parollar murakkab bo‘lishi kerak, ular katta va kichik harflar, raqamlar va maxsus belgilar kombinatsiyasidan iborat bo‘lishi kerak.[8]

Elektron tizim orqali taqdim etilgan idoraviy normativ-huquqiy hujjatni huquqiy ekspertizadan o‘tkazish natijasida unda texnik ko‘rinishdagi, shu jumladan hujjat mazmunining o‘zgarishiga olib kelmaydigan xatoliklar mavjudligi aniqlangan taqdirda, mazkur xatoliklar

O‘zbekiston Respublikasi Adliya vazirligi tomonidan elektron tizim orqali bartaraf etilishi mumkin. Bunda, idoraviy normativ-huquqiy hujjatda aniqlangan texnik ko‘rinishdagi, shu jumladan mazmun o‘zgarishiga olib kelmaydigan xatoliklar hujjatni qabul qilgan organ (organlar) birinchi rahbari tomonidan imzolangan tegishli xatga asosan bartaraf etiladi. [9] Parollarni muntazam ravishda o‘zgartirish va bir nechta hisoblar uchun bir xil paroldan foydalanishdan qochish tavsiya etiladi. Bu, ayniqsa hujjatlar raqamli shaklda saqlangan yoki uzatilganda, qo‘shimcha himoya qatlamini qo‘shadi.yuridik hujjatlarni shifrlash orqali, hatto ular noto‘g‘ri qo‘llarga tushib qolsa ham, kontent xavfsiz bo‘lib qoladi va ruxsatsiz shaxslarga kira olmaydi. Doimiy ma’lumotlarning zaxira nusxalari ham yuridik hujjatlarni himoya qilish uchun muhim xavfsizlik amaliyotidir. Birmingemdagi Alabama universiteti tomonidan tuzilgan ma’lumotlarga ko‘ra, so‘rovda qatnashgan yuridik tashkilotlarning 80 foizi o‘zlarining eng katta xavfsizlik xavflari foydalanuvchilardan kelib chiqishini aytadi. Har qanday o‘zgarishlarni muvaffaqiyatli qo‘llashdan oldin xodimlarni muhim ma’lumotlar bilan to‘g‘ri ishlashga o‘rgatish kerak.[10] Yuridik mutaxassislar o‘z hujjatlarining ma’lumotlar yo‘qolishi, masalan, qurilmadagi nosozlik yoki kiberhujum kabi hodisalarda mavjudligini ta’minlash uchun muntazam ravishda zaxira nusxasini yaratishlari kerak. Zaxira nusxalari xavfsiz serverlarda, bulutli saqlash platformalarida yoki tashqi disklarda saqlanishi mumkin. Yangilangan zaxira nusxalarini saqlab, yuridik mutaxassislar o‘zlarining muhim yuridik hujjatlarini tezda tiklashlari va har qanday ma’lumotlar yo‘qolishining ta’sirini kamaytirishlari mumkin. Ko‘p faktorli autentifikatsiyani (MFA) amalga oshirish huquqshunoslar e’tiborga olishlari kerak bo‘lgan yana bir xavfsizlik amaliyotidir. Bundan tashqari, yuridik hujjatlarning jismoniy nusxalarini himoya qilish ham bir xil darajada muhimdir. Yuridik mutaxassislar jismoniy hujjatlarni qulflangan shkaflar yoki kirish imkoniyati cheklangan xonalarda saqlanishini ta’minlashi kerak. Bundan tashqari, jismoniy hujjatlar bilan to‘g‘ri ishlash va yo‘q qilish uchun protokollarni o‘rnatish juda muhimdir.

Xulosa

Yuridik hujjatlarni himoya qilish maxfiy ma’lumotlarning yaxlitligini ta’minlash uchun juda muhimdir. Shuningdek, hujjatlarni xavfsiz saqlash, kuchli parol himoyasi, shifrlash, kirishni nazorat qilish choralari va muntazam xavfsizlik tekshiruvlarini amalga oshirish orqali siz ruxsatsiz kirish xavfini sezilarli darajada kamaytirishingiz va yuridik hujjatlaringiz xavfsizligini ta’minlashingiz mumkin. Hujjat xavfsizligini birinchi o‘ringa qo‘yish orqali siz o‘z mijozlaringiz va manfaatdor tomonlaringizga ishonchni oshirishingiz, shu bilan birga qonuniy va me’yoriy talablarga rioya qilishingiz mumkin. Eskirgan yoki keraksiz yuridik hujjatlarni maydalash yoki xavfsiz tarzda yo‘q qilish ruxsatsiz shaxslarning maxfiy ma’lumotlarni olishiga to‘sqinlik qilishi mumkin. Umuman olganda shuni aytish mumkinki, yuridik hujjatlarni himoya qilish huquqshunoslar uchun ustuvor vazifa bo‘lishi kerak. Kuchli parollar va kirishni boshqarish vositalari, shifrlash, muntazam ma’lumotlarni zaxiralash, ko‘p faktorli autentifikatsiya va jismoniy hujjatlar xavfsizligi protokollari kabi xavfsizlik

amaliyotlarini qo‘llash orqali yuridik mutaxassislar ruxsatsiz kirish xavfini sezilarli darajada kamaytirishi va ularning yuridik hujjatlaridagi maxfiy ma’lumotlarini himoya qilishi mumkin.

FOYDALANILGAN MANBALAR:

1. O‘zbekiston Respublikasining ‘‘Kiberxavfsizlik to‘g‘risida’’gi 15.04.2022- yildagi 764-sonli Qonuni;

2. Legal Aid Agency – Information Security Handling Personal Data and Documents Data Security Guidance November 2020;

3. Best Practices for Establishing Security Requirements for Business Documents https://www.perivan.com/resources/blog/best-practices-for-establishing-security-requirements-for-business-documents/;

4. Ensuring the Security of Legal Documents: Tools and Techniques https://leaksid.com/security-of-legal-documents/;

5. The Importance of Document Security in Legal Practices | Di Lauri & Hewitt Law Group https://dilaurilaw.com/the-importance-of-document-security-in-legal-practices/;

6. O‘zbekiston Respublikasi adliya vazirining 2014-yil 28-fevraldagi Idoraviy normativ-huquqiy hujjatlarni tayyorlash va qabul qilish Qoidalari;

7. Seven Easy Ways to Improve Legal Document Security - Legal IT Professionals https://www.legalitprofessionals.com/legal-it-columns/65-guest-columns/12160-seven-easy-ways-to-improve-legal-document-security;

8. PDF And Document Security Systems: Protect, Track, And Secure PDFs https://www.inkit.com/blog/document-security-systems;

9. PDF & document security: How to protect and track documents securely (2022);

10. Five Ways to Secure Documents and Protect Private Information in the Workplace https://documentmedia.com/article-3089-5-Ways-to-Secure-Documents-and-Protect-Private-Information.html.