MEHMONLARNING SHAXSIY MA'LUMOTLARINI MAXFIY SAQLASH VA HIMOYA QILISH: QOIDALAR VA MAS'ULIYAT

Hamroyev Abduqodir Rajabali o'g'li
SamISI "Turizm" kafedrasi o'qituvchisi
Mir-Jafarova Aziza Javoxirovna
SamISI "Servis" fakulteti talabasi
https://doi.org/10.5281/zenodo.19413705

Annotatsiya: Ushbu maqolada mehmonxonalarda mehmonlarning shaxsiy ma'lumotlarini himoya qilish masalalari, ularning turlari, huquqiy asoslari va xavfsizlik choralariga e'tibor qaratiladi. Zamonaviy tahdidlar hamda ularni bartaraf etish yo'llari tahlil qilinadi.

Kalit so'zlar: shaxsiy ma'lumotlar, maxfiylik, GDPR, mehmonxona, kiberxavfsizlik, rozilik, ma'lumotlarni himoya qilish, audit, tahdidlar, xavfsizlik choralar

Abstract: This article focuses on the issues of protecting guests' personal data in hotels, addressing the types of data, the legal framework, and security measures. It also analyzes modern threats and the methods for their mitigation.

Keywords: personal data, privacy, GDPR, hotel, cybersecurity, consent, data protection, audit, threats, security measures

Raqamli asrda mehmonlarning shaxsiy ma'lumotlarini himoya qilish mehmondo'stlik va turizm sanoatining eng muhim vazifalaridan biriga aylandi. Mehmonlar o'zlarining pasport ma'lumotlari, bank kartasi ma'lumotlari, aloqa ma'lumotlari va hatto tibbiy afzalliklarini ishonch bilan ishonib topshiradilar. Bu ma'lumotlar xizmat sifatini yaxshilash, bandlovlarni ta'minlash va mehmon taassurotini yaxshilash uchun juda muhim bo'lsa-da, ularning yetarli darajada himoyalanmaganligi maxfiylik buzilishi, moliyaviy yo'qotishlar va obro'ga putur yetishiga olib kelishi mumkin. Dunyoda ma'lumotlar xavfsizligi bilan bog'liq muammolar kuchayib borar ekan, xalqaro standartlarga rioya qilish har qanday mehmonxona operatorining asosiy vazifasiga aylanmoqda.

Shaxsiy ma'lumotlar tushunchasi

Shaxsga doir ma'lumotlar muayyan shaxsga taalluqli bo'lgan yoki uni bevosita yoxud bilvosita identifikatsiya qilish imkonini beradigan har qanday ma'lumotlardir. Ushbu ma'lumotlar elektron, qog'oz yoki boshqa har qanday moddiy shaklda bo'lishi mumkin. Mehmonlar to'g'risidagi ma'lumotlar quyidagilarga bo'linadi: identifikatsiya ma'lumotlari (F.I.O., tug'ilgan sanasi, pasport raqami, fuqaroligi), aloqa ma'lumotlari (telefon, elektron pochta, ijtimoiy tarmoqlar), moliyaviy ma'lumotlar (bank kartasi ma'lumotlari, to'lovlar tarixi), maxsus yoki nozik ma'lumotlar (sog'liq holati, allergiya, ovqatlanish, nogironlik),

xizmat ma’lumotlari (xona turi, band qilish muddati, maxsus so‘rovlar). Chet ellik mehmonlar uchun pasport ma’lumotlari ko‘pincha qo‘shimcha tekshiruvni talab qiladi.

Maxfiylik darajasi sezgirlik darajasiga qarab o‘zgaradi. Asosiy daraja ism va telefon raqami kabi umumiy ma’lumotlarni o‘z ichiga oladi, ular oddiy rozilik bilan qayta ishlanadi. Maxsus daraja irqiy kelib chiqish, salomatlik holati va shaxsiy hayot haqidagi ma’lumotlarni o‘z ichiga oladi, bu esa aniq rozilik va qo‘shimcha himoya choralarini talab qiladi. Biometrik ma’lumotlar (barmoq izlari, yuzni aniqlash) va genetik ma’lumotlar eng yuqori darajada, chunki ular doimiy va o‘zgarmasdir. Ma’lumotlar operatorlari ma’lumotlarning maxfiyligi va himoyasini ta’minlashlari shart, aks holda qonuniy javobgarlik yuzaga kelishi mumkin.

Ma’lumotlarni himoya qilishning huquqiy asoslari

Milliy qonunchilik shaxsiy ma’lumotlarni himoya qilishni nazarda tutsa-da, jahon standartlari, xususan, Yevropa Ittifoqining ma’lumotlarni himoya qilish bo‘yicha umumiy reglamenti (GDPR) butun dunyo bo‘ylab mehmonxonalar uchun eng muhim ko‘rsatma bo‘lib xizmat qiladi. GDPR 2018-yilda kuchga kirdi. Yevropa fuqarolarining ma’lumotlarini qayta ishlaydigan har qanday biznesga (joylashuvidan qat’i nazar) tatbiq qilinadi. Uning asosiy tamoyillari:

-ma’lumotlarni qayta ishlashning qonuniyligi, adolatliligi va shaffofligi - ma’lumotlar qonuniy, halol va ochiq tarzda yig‘ilib, qanday ishlatilayotgani mijozga tushuntiriladi;

-maqsadning cheklanganligi - ma’lumotlar faqat aniq belgilangan maqsad uchun yig‘iladi va boshqa maqsadda ishlatilmaydi;

-ma’lumotlarni minimallashtirish - faqat zarur bo‘lgan ma’lumotlar olinadi, ortiqcha ma’lumot yig‘ilmaydi;

-aniqlik - ma’lumotlar to‘g‘ri va doimo yangilanib turishi kerak;

-saqlash vaqtining cheklanganligi - ma’lumotlar faqat kerakli muddat davomida saqlanadi;

-yaxlitlik va maxfiylik - ma’lumotlar himoyalangan bo‘lishi va begona shaxslarga oshkor qilinmasligi kerak;

-javobgarlik - ma’lumotlarni qayta ishlovchi tashkilot barcha qoidalarga amal qilishi va buning uchun javob berishi shart.

GDPR mehmonxonalar uchun: mehmonlardan aniq, erkin rozilik olish, maxfiylik siyosatini ochiq va tushunarli tarzda taqdim etish, mehmonlarning huquqlarini ta’minlash – ma’lumotlarga kirish, tuzatish, o‘chirish, qayta ishlashga qarshi chiqish va ma’lumotlarni boshqa operatorga ko‘chirish huquqi bo‘yicha aniq talablarni qo‘yadi. Ma’lumotlar buzilishi aniqlanganda 72 soat ichida nazorat

organlariga xabar berish majburiy hisoblanib, agar xavf yuqori bo‘lsa, mehmonlarga ham bildiriladi. Xavfsizlik choralari yetarli bo‘lmagan taqdirda, jarimalar global aylanmaning 4 foizigacha yoki 20 million yevrogacha yetishi mumkin. Ko‘plab xalqaro mehmonxona zanjirlari GDPR talablarini O‘zbekistonda ham qo‘llaydi.

Bundan tashqari, Kaliforniya iste’molchilar maxfiyligi qonuni (CCPA/CPRA), Braziliya LGPD va Xitoy PIPL kabi global qonunlar ham shaxsiy ma’lumotlar himoyasini kuchaytirib, mehmonxonalarni shaffoflik va mas’uliyatga undamoqda. Bu qonunlar operatorlarni ma’lumotlar bazasini ro‘yxatdan o‘tkazish, ma’lumotlar xavfsizligiga mas’ul shaxs tayinlash va muntazam auditni yo‘lga qo‘yishga majburlaydi.

Mehmon ma’lumotlarini yig‘ish va qayta ishlash

Mehmonxonalarda mijozlarga oid ma’lumotlar odatda onlayn bron qilish, telefon orqali buyurtma berish, check-in jarayoni hamda xizmat ko‘rsatish davomida yig‘iladi. Ushbu ma’lumotlar mijozga sifatli xizmat ko‘rsatish va bronlash jarayonini to‘g‘ri tashkil etish uchun zarur hisoblanadi. Majburiy ma’lumotlarga pasport rekvizitlari, aloqa uchun telefon yoki elektron pochta manzili hamda to‘lovga oid ma’lumotlar kiradi. Bundan tashqari, ayrim hollarda mijozning qulayligini ta’minlash maqsadida uning tibbiy ehtiyojlari yoki ovqatlanish talablari kabi qo‘shimcha ma’lumotlar ham ixtiyoriy ravishda olinishi mumkin.

Rozilik olish asosiy talab hisoblanadi. Rozilik yozma yoki elektron shaklda berilishi kerak va u aniq, erkin berilgan va yaxshi xabardor qilingan bo‘lishi kerak. Mehmonxona maxfiylik siyosatini taqdim etishi va mehmonni o‘z huquqlari haqida xabardor qilishi shart. Rozilik bermasa, faqat shartnomani bajarish yoki qonun talabi bo‘yicha ma’lumot yig‘iladi. Foydalanish faqat xizmat ko‘rsatish, hisob-kitob qilish va qonuniy majburiyatlarni bajarish bilan cheklanadi. Marketing maqsadlari uchun alohida rozilik talab qilinadi. Ma’lumotlar anonimlashtirilgandan keyin statistik maqsadlarda ishlatilishi mumkin.

Ma’lumotlarni saqlash va himoyalashning samarali usullari quyidagilardan iborat:

-Texnik himoya choralari - ma’lumotlar bazasi kuchli shifrlash (AES-256) orqali himoyalanadi, ikki bosqichli autentifikatsiya joriy etiladi, xavfsizlik devorlari va antivirus dasturlari ishlatiladi, tizim muntazam yangilanadi hamda zaifliklar skanerlanadi. Bulutli xizmatlardan foydalanishda mahalliy yoki xavfsiz serverlarga ustuvorlik berish tavsiya etiladi.

-Tashkiliy chora-tadbirlar - kirish faqat vakolatli xodimlar bilan cheklanishi kerak, audit jurnallari yuritiladi va ma'lumotlarni saqlash siyosati belgilanadi - masalan, mehmon ketgandan so'ng hisob-kitob uchun kerakli ma'lumotlar saqlanadi, so'ngra o'chiriladi. Yangi tizimlar yaratishda "dizayn asosida himoya" tamoyili qo'llanilishi lozim, ya'ni xavfsizlik tizimning boshidanoq integratsiya qilinadi.

-Jismoniy xavfsizlik - qog'oz hujjatlar seyflarda saqlanadi, kirish cheklangan bo'ladi va CCTV orqali nazorat amalga oshiriladi. Mehmonxona mulkini boshqarish tizimi dasturiy ta'minoti ma'lumotlarni markazlashtirilgan tarzda himoya qilishga yordam beradi.

-Xodimlarning mas'uliyati - barcha xodimlar maxfiylik qoidalari bilan tanishtiriladi va maxfiylik shartnomasi (NDA) imzolaydi. Har bir xodim faqat o'z vazifasiga muvofiq kerakli ma'lumotlarga kirish huquqiga ega. Parollarni ochiq saqlash, uchinchi shaxsga berish yoki beparvolik ma'lumotlarning sizib chiqishiga olib keladi va jarima, ishdan bo'shatish yoki jinoyat ishi bilan javobgarlikka sabab bo'ladi.

-O'quv va monitoring - xodimlar uchun muntazam treninglar, phishing testlari va ichki auditlar o'tkazilishi zarur. Ular kiberxavfsizlik asoslarini puxta o'rganishi, kuchli parol yaratish, shubhali havolalarni ochmaslik va boshqa xavfsizlik choralari shart. Rahbariyat mas'uliyatni aniq taqsimlaydi, operator umumiy javobgar bo'lsa, xodimlar o'z harakatlari uchun shaxsiy javob beradi.

Xavflar va tahdidlar

Asosiy xavflar kiberhujumlar bo'lib, ularga zararli dasturlar, firibgarlik xabarlari,

ma'lumotlar bazasiga hujum va internetga ulangan qurilmalardagi zaifliklar kiradi. Mehmonxonalarda to'lov tizimlari, mehmonlar uchun Wi-Fi va front-ofis ish tizimlari eng zaif bo'lgan joylardir.

Ichki tahdidlar xodimlarning beparvoligi yoki ichki firibgarlik tufayli yuzaga keladi. Ma'lumotlarning ko'pchiligi inson xatosidan oshkor bo'ladi. Tashqi tahdidlar esa uchinchi shaxs xizmat ko'rsatuvchilari yoki zaif infratuzilmadan keladi.

Haqiqiy misollar bu xavflarni aniq ko'rsatadi. 2024 yilda Omni Hotels & Resorts kiberhujumga uchrab, bron qilish, to'lov tizimlari va elektron xona kalitlari uzoq vaqt ishlamay qoldi, bu esa mehmonlar uchun katta noqulaylik tug'dirdi. Shu yili Otelier mehmonxona boshqaruv platformasining buzilishi natijasida Marriott, Hilton va Hyatt mehmonlarining 437 ming elektron pochta manzili, ism-familiya, manzil, telefon va ba'zi hollarda to'lov ma'lumotlari oshkor

bo‘ldi. 2025 yilda Pyramid Global Hospitality zararli dastur hujumiga uchradi, bu esa mehmon va xodim ma’lumotlarining katta qismini xavf ostiga qo‘ydi. Bunday hodisalar millionlab dollar zarar keltirishi va mehmonlar ishonchini yo‘qotishiga olib keladi.

Muammolar va ularning yechimlari

Amaliy muammolar. Katta hajmdagi ma’lumotlarni boshqarish, xodimlarning malakasining yetarli emasligi, texnik infratuzilmaning zaifligi va ma’lumotlarni chegaralararo uzatish xavfi. Onlayn bron qilish platformalari va uchinchi tomon xizmatlari qo‘shimcha zaifliklar yaratadi.

Taklif etilayotkan yechimlar. Ma’lumotlarni muntazam audit qilish va inventarizatsiya o‘tkazish, tizimlarni xavfsizlik nuqtai nazaridan sinovdan o‘tkazish (penetratsiya testi va zaifliklarni tekshirish), ma’lumotlar buzilgan taqdirda tezkor javob berish rejasi (72 soat ichida javob berish) tayyorlash kabilarni tavsiya etish mumkin. Xodimlar uchun majburiy treninglar o‘tkazish, mehmonlarga ochiq maxfiylik siyosati taqdim etish va rozilik (consent) mexanizmlarini joriy etish zarur. Shuningdek, sug‘urta va mas’uliyatni aniq taqsimlash muhim hisoblanadi. Yangi tizimlarni yaratishda “Privacy by Design” tamoyilini qo‘llash kelajakdagi xavflarni kamaytirishga yordam beradi.

Xulosa

Mehmonlarning shaxsiy ma’lumotlari maxfiyligini ta’minlash va ularni himoya qilish zamonaviy mehmondo‘stlik sohasining eng muhim talablaridan biridir. Xalqaro standartlar, xususan, GDPRning qat’iy qoidalari mehmonxona operatorlarini huquqiy, texnik va tashkiliy choralarni to‘liq amalga oshirishga undaydi. Rozilik olish, zaruriy minimal ma’lumotlarni yig‘ish, kuchli shifrlash usullaridan foydalanish, xodimlar malakasini muntazam oshirib borish va auditlar o‘tkazish - shaxsiy ma’lumotlarni himoya qilishning asosiy vositalaridir.

Foydalanilgan adabiyotlar ro‘yxati:

1. O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni (O‘RQ-547-son, 02.07.2019 y.). Lex.uz rasmiy portali. https://lex.uz/docs/-4396419

2. GDPR asosiy talablari va mehmondo‘stlik sohasiga qo‘llanilishi bo‘yicha qo‘llanma. “GDPR for Hotels: A step-by-step guide”. Infosys BPM, 2025. https://www.infosysbpm.com/blogs/travel-hospitality/gdpr-for-hotels-step-by-step-guide.html

3. “What are the legal requirements for hotel data protection and privacy”. International Hospitality Institute. https://www.internationalhospitalityinstitute.com/ articles/what-are-the-legal-requirements-for-hotel-data-protection-and-privacy

4. Omni Hotels & Resorts kiberhujumi (2024). Help Net Security va CSO Online hisobotlari, 2024–2025.
5. Marriott International (Starwood) data breach (2014–2018 va keyingi holatlar). FTC (AQSh Federal Savdo Komissiyasi) rasmiy bayonoti, 9 oktyabr 2024 y. https://www.ftc.gov/news-events/news/press-releases/2024/10/ftc-takes-action-against-marriott-starwood-over-multiple-data-breaches
6. MGM Resorts International kiberhujumlari (2019 va 2023 yillar). Rasmiy hisobotlar va class-action da'volar tahlillari, 2025 yilgi settlement ma'lumotlari.
7. California Consumer Privacy Act (CCPA/CPRA). Kaliforniya shtati qonunchiligi (2018 va keyingi o'zgartirishlar). Mehmondo'stlik sohasiga qo'llanilishi bo'yicha tahlillar: https://www.internationalhospitalityinstitute.com/articles/what-are-the-legal-requirements-for-hotel-data-protection-and-privacy
8. "Data Privacy in Hospitality: Building Trust, Avoiding Breaches". DailyPoint va boshqa sanoat nashrlari, 2024–2025.