Axborot tizimlarida shaxsiy ma'lumotlarni himoya qilish usullari

J.O.Jumamuratov, TATU Nukus filiali talabasi

Bugungi kunda informatsiya texnologiyalari tez rivojlanib, ko'plab sohalarga o'z ta'sirini o'tkazmoqda. Shu sababli, shaxsiy ma'lumotlarning xavfsizligi va maxfiyligini ta'minlash masalasi yanada dolzarb bo'lib qoldi. Har kuni turli xil tizimlarda millionlab shaxsiy ma'lumotlar yig'iladi, saqlanadi va uzatiladi. Bu ma'lumotlar o'z ichiga ism, familiya, manzil, telefon raqamlari, elektron pochta manzillari, kredit karta ma'lumotlari va boshqa shaxsiy axborotlarni oladi. Ushbu ma'lumotlarning xavfsizligini ta'minlash uchun turli xil texnologik chora-tadbirlar va strategiyalar qo'llaniladi. Bu chora-tadbirlar orasida shifrlash, autentifikatsiya, kirishni boshqarish, ma'lumotlarni zaxiralash, va boshqalar mavjud. Har bir usulning o'ziga xos afzalliklari va cheklovlari bor bo'lib, ularni birgalikda qo'llash orqali maksimal himoya darajasiga erishish mumkin. Ushbu maqolada informatsiya tizimlarida shaxsiy ma'lumotlarni himoya qilishning asosiy usullari, shuningdek, bu usullarning ahamiyati va ularni amalga oshirish yo'llari ko'rib chiqiladi. Shaxsiy ma'lumotlarni himoya qilish nafaqat huquqiy majburiyat, balki foydalanuvchilarning ishonchini qozonish va ularni saqlab qolish uchun ham muhimdir.

Texnik Himoya Usullari

Shifrlash shaxsiy ma'lumotlarni himoya qilishning eng asosiy va keng qo'llaniladigan usullaridan biridir. Shifrlash texnologiyasi ma'lumotlarni o'qilmaydigan shaklga aylantiradi, faqat maxsus kalit yordamida qayta o'qilishi mumkin. Bu usul orqali ma'lumotlar internet orqali uzatilganda yoki saqlanganda ularga ruxsatsiz kirishning oldi olinadi. AES (Advanced Encryption Standard) va RSA (Rivest-Shamir-Adleman) kabi shifrlash algoritmlari ko'plab tizimlarda qo'llaniladi.

Ikki faktorli autentifikatsiya (2FA) foydalanuvchilarni identifikatsiyalashda qo'shimcha xavfsizlik qatlamini ta'minlaydi. Bu usulda foydalanuvchi, odatda, parol kiritganidan keyin qo'shimcha ravishda bir martalik kod yoki biometrik

identifikatsiya orqali tasdiqlanadi. Bu usul hisoblar va tizimlarga ruxsatsiz kirishni qiyinlashtiradi.

Firevallar va antivirus dasturlari tarmoq va kompyuter tizimlarini zararli dasturlardan va hujumlardan himoya qiladi. Firevallar tarmoq trafigini nazorat qiladi va zararli trafiga ruxsat bermaydi. Antivirus dasturlari esa zararli dasturlarni aniqlash va yo'q qilishga yordam beradi. Bu vositalar ma'lumotlarni ruxsatsiz kirishdan himoya qilishda muhim rol o'ynaydi.

Ma'lumotlarni zaxiralash shaxsiy ma'lumotlarni himoya qilishning muhim jihatlaridan biridir. Ma'lumotlarni muntazam ravishda zaxiralash orqali ularni yo'qotish xavfidan saqlanish mumkin. Zaxiralashning bulutli saqlash (cloud storage) xizmatlari yordamida amalga oshirilishi ma'lumotlarning xavfsizligini oshiradi va ularga kirishni yanada osonlashtiradi.

Kirishni Boshqarish va Autentifikatsiya

Kirishni boshqarish tizimlari shaxsiy ma'lumotlarga faqatgina ruxsat etilgan foydalanuvchilar kirishini ta'minlaydi. Bu tizimlar foydalanuvchi rollari va ruxsatlarini boshqaradi. Har bir foydalanuvchiga o'z vazifasiga mos ravishda kirish huquqlari beriladi, bu esa ma'lumotlarning himoyasini kuchaytiradi.

Biometrik autentifikatsiya usullari, masalan, barmoq izi, yuz tanish va ko'z qovog'i skanerlash kabi texnologiyalar shaxsiy ma'lumotlarni himoya qilishda yuqori darajadagi xavfsizlikni ta'minlaydi. Bu usullar foydalanuvchini identifikatsiyalashda aniq va ishonchli bo'lib, parol va boshqa an'anaviy usullardan ko'ra xavfsizroqdir.

Ma'lumotlarni anonimlashtirish va psevdonimlashtirish shaxsiy ma'lumotlarni himoya qilishning samarali usullaridir. Anonimlashtirish orqali ma'lumotlar shaxsni identifikatsiyalash imkoniyatini yo'qotadi, bu esa ma'lumotlarning maxfiyligini ta'minlaydi. Psevdonimlashtirish esa shaxsiy ma'lumotlarni maxsus identifikatorlar yordamida almashtirib, ularni xavfsiz saqlashni ta'minlaydi.

Ta'lim va Huquqiy Choralar

Shaxsiy ma'lumotlarni himoya qilish faqat texnik choralardan iborat emas. Foydalanuvchilar va xodimlarni o'qitish va xabardor qilish ham muhim ahamiyatga ega. Xodimlar ma'lumotlarni xavfsiz saqlash va ishlatish qoidalari bilan tanish

bo'lishlari kerak. Xavfsizlik bo'yicha muntazam treninglar o'tkazish va xabardorlik kampaniyalarini tashkil etish ma'lumotlarning himoyasini kuchaytiradi.

Shaxsiy ma'lumotlarni himoya qilishda qonun va me'yoriy talablar ham muhim o'rin tutadi. Ko'plab mamlakatlarda shaxsiy ma'lumotlarni himoya qilish bo'yicha qonunlar mavjud. Masalan, Yevropa Ittifoqida GDPR (General Data Protection Regulation) qoidalari amal qiladi. Ushbu qoidalarga rioya qilish va ularga muvofiq ravishda ma'lumotlarni himoya qilish choralari ko'rilishi zarur.

Xulosa

Informatsiya tizimlarida shaxsiy ma'lumotlarni himoya qilish ko'plab texnologiyalar va usullarni talab etadi. Shifrlash, ikki faktorli autentifikatsiya, firevallar, antivirus dasturlari, ma'lumotlarni zaxiralash, kirishni boshqarish, biometrik autentifikatsiya, anonimlashtirish va psevdonimlashtirish, o'qitish va xabardorlik, shuningdek, qonun va me'yoriy talablar shaxsiy ma'lumotlarni himoya qilishning asosiy usullaridir. Ushbu choralarning kompleks qo'llanilishi shaxsiy ma'lumotlarni ruxsatsiz kirishdan va zararli hujumlardan himoya qilishda muhim rol o'ynaydi.

Foydalanilgan adabiyotlar ro'yxati

1. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons.

2. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.

3. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson.

4. Garfinkel, S., & Spafford, G. (2002). Practical UNIX and Internet Security. O'Reilly Media.

5. Schneier, B. (2013). Two-Factor Authentication: Why It's More Important Than Ever. IEEE Security & Privacy, 11(1), 93-96.