

KATTA MA'LUMOTLAR VA SHAXSIY MA'LUMOTLAR XAFSIZLIGINI TA'MINLASH

*Toshkent irrigatsiya va qishloq xo'jaligini mexanizatsiyalash muhandislari instituti,
Milliy tadqiqot universiteti, "Texnologik jarayonlarni avtomatlashtirish va boshqarish"
kafedrasi "Axborot tizimlari va texnologiyalari" bakalavr ta'lim yo'nalishi talabasi*

Mamatqulov Mirvoxid Mirzoxid o'g'li

*Toshkent irrigatsiya va qishloq xo'jaligini mexanizatsiyalash muhandislari instituti,
Milliy tadqiqot universiteti, "Raqamli texnologiyalar va sun'iy intellekt" kafedrasi
bakalavr ta'lim yo'nalishi talabasi*

Najmiddinov Ahliddin Sirojiddin o'g'li

Anotatsiya: Ushbu maqolada hozirda ko'plab sohalarga kirib borgan katta hajmdagi va shaxsiy ma'lumotlar xavfsizligi tavsiflanadi, ularda ishlatiladigan katta hajmdagi ma'lumotlar va texnologiyalarning axborot xavfsizligi muammolari muhokama qilinadi, turli sohalarda qo'llaniladigan katta hajmdagi ma'lumotlar, xavfsizlik mexanizmini ta'minlaydi. Ushbu muammolarni hal qilish, shuningdek, qo'shimcha tavsiyalar beradi.

Kalit so'zlar: Katta ma'lumotlar, Shaxsiy ma'lumotlar, xavfsizlik, kiberxavfsizlik, axborot xavfsizligi, standartlashtirish.

Annotation: This article describes the security of big data and personal data, which has now penetrated many industries, discusses the information security problems of big data and technologies used in them, big data used in various fields, provides a security mechanism . solutions to these problems, as well as provide additional recommendations.

Key words: Big data, Personal data, security, cyber security, information security, standardization.

Аннотация: В данной статье описывается безопасность крупномасштабных и персональных данных, которая в настоящее время проникла во многие отрасли, обсуждаются проблемы информационной безопасности крупномасштабных данных и используемых в них технологий, а также приводится механизм

безопасности крупномасштабных данных, используемых в различных отраслях. .
пути решения данных проблем, а также дать дополнительные рекомендации.

Ключевые слова: Большие данные, Персональные данные, безопасность, кибербезопасность, информационная безопасность, стандартизация.

Axborot xavfsizligi (inglizcha: Information Security, shuningdek, inglizcha: InfoSec) — axborotni ruxsatsiz kirish, foydalanish, oshkor qilish, buzish, o‘zgartirish, tadqiq qilish, yozib olish yoki yo‘q qilishning oldini olish amaliyotidir. Ushbu universal kontseptsiya ma’lumotlar qanday shaklda bo‘lishidan qat’iy nazar (masalan, elektron yoki, jismoniy) amal qiladi. Axborot xavfsizligini ta’minlashning asosiy maqsadi ma’lumotlarning konfidensialligi, yaxlitligi va mavjudligini muvozanatli, qo‘llashning maqsadga muvofiqligini hisobga olgan holda va tashkilot faoliyatiga hech qanday zarar yetkazmasdan himoya qilishdir. Bunga, birinchi navbatda, asosiy vositalar va nomoddiy aktivlar, tahdid manbalari, zaifliklar, potensial ta’sirlar va mavjud xavflarni boshqarish imkoniyatlarini aniqlaydigan ko‘p bosqichli xavflarni boshqarish jarayoni orqali erishiladi. Bu jarayon xavflarni boshqarish rejasining samaradorligini baholash bilan birga olib boriladi.

Ushbu faoliyatni standartlashtirish maqsadida ilmiy va kasbiy hamjamiyatlar texnik axborot xavfsizligi choralari, yuridik javobgarlik, shuningdek, foydalanuvchi va ma’murlarni tayyorlash standartlari sohasida asosiy metodologiya, siyosat va tarmoq standartlarini ishlab chiqishga qaratilgan doimiy hamkorlik asosida ish olib boradi. Ushbu standartlashtirishga asosan ma’lumotlarga kirish, qayta ishlash, saqlash va uzatishni tartibga soluvchi keng ko‘lamli qonunlar va qoidalar ta’sir ko‘rsatadi. Biroq, tashkilotda agar doimiy takomillashtirish madaniyati to‘g‘ri shakllantirilmagan bo‘lsa, har qanday standartlar va metodologiyalarni joriy etish yuzaki ta’sir ko‘rsatishi mumkin.

Katta hajmli ma'lumotlar xavfsizligini ta'minlash.

Katta ma'lumotlarni himoya qilish yuqori qiymatli va turli xil maqsad bo'lishdan tashqari, noyob muammolar bilan birga keladi. Bu Big Data xavfsizligi an'anaviy ma'lumotlar xavfsizligidan tubdan farq qilmaydi. Katta ma'lumotlar xavfsizligi muammolari asosiy farqlar emas, balki qo'shimcha farqlar tufayli yuzaga keladi. Big Data

muhitlari va an'anaviy ma'lumotlar muhitlari o'rtasidagi farqlar quyidagilarni o'z ichiga oladi:

Katta ma'lumotlarni tahlil qilish uchun to'plangan, jamlangan va tahlil qilingan ma'lumotlar;

Katta ma'lumotlarni saqlash va joylashtirish uchun ishlatiladigan infratuzilma; Strukturalanmagan va yarimstrukturalangan katta ma'lumotlarni tahlil qilish uchun qo'llaniladigan texnologiyalar.

Asosiy ustuvorlik katta hajmdagi ma'lumotlar tezligini taklif qilish bo'lganligi sababli, xavfsizlik ko'pincha e'tiborga olinadigan oxirgi element bo'lishi mumkin, ya'ni asosan saqlanadigan va uzatiladigan ma'lumotlarning o'ziga xos tasnifi mavjud emasligi sababli. Turli texnologiyalarning integratsiyasi xavfsizlikning yangi muammolarini keltirib chiqaradi, ular odatda texnologiyaga xos muammolarga bo'lingan holda to'g'ri hal qilinishi kerak. Katta ma'lumotlar tizimlari muhim infratuzilmalarni qo'llab-quvvatlash, xavfsizlik ham talabga aylanadi. Katta ma'lumotlar tizimlari murakkab bo'lganligi sababli, xizmatlarning foydalanuvchanligini va uzluksizligini ta'minlash uchun xavfsizlik yondashuvi yaxlit bo'lishi kerak.

Xavfsizlik muammolarini tushunish uchun katta hajmli ma'lumotlardan foydalanish misollariga amal qilishga va tegishli holatlarni o'rganish kerak. Quyida 3 ta tegishli amaliy tadqiqotlarni tahlil qilindi va aniqlangan xavfsizlik muammolarini tavsiflandi. Ushbu foydalanish holatlarini tanlash mezonlari to'plangan ma'lumotlardan ko'proq qiymatni ta'minlaydigan ushbu sektorlarda Katta ma'lumotlarning yetukligi hisoblanadi. Shuni hisobga olish kerakki, Katta ma'lumotlar nisbatan yangi tushuncha bo'lganligi sababli, jamiyat xavfsizlik kabi muayyan masalalar bo'yicha yechimlarni aniqlashning dastlabki bosqichida. Quyida 1-jadvalda ushbu foydalanish holatlari uchun xavfsizlik tahlilini keltirildi:

Kibermakon global axborotkommunikasiya infratuzilmasida markaziy o'ringa chiqqani sababli hozir ijtimoiy tarmoqlarda ma'lumotlar xavfsizligi dunyo bo'ylab korporasiyalar va hukumatlar uchun asosiy vazifaga aylandi. Hamma joyda mavjud bo'lgan, bir-biriga bog'langan va internetga oson kirish imkonini beruvchi texnologiyalar kundalik hayotda chuqur ahamiyat kasb etmoqda. Natijada ijtimoiy, iqtisodiy va siyosiy

aloqalar uchun kibermakonga tobora ko‘proq bog‘lanib boryapmiz. Internet sog‘liqni saqlash, oziq-ovqat va suv, moliya, axborotkommunikasiya texnologiyalari, jamoat xavfsizligi, energetika va kommunal xizmatlar, ishlab chiqarish, transport kabi muhim infratuzilma tarmoqlari va xizmatlari uchun qulay platformani taqdim etib kelayotir.

Hozir ijtimoiy tarmoqlarga kirish uchun internet tizimidan eng ko‘p foydalanilayotgani hammaga ma‘lum. Ushbu tarmoqlar bir qancha qulaylik va afzalliklarga ega bo‘lsada, kamdan-kam foydalanuvchilar tarmoqqa joylashtirayotgan ma‘lumotlari qanchalik himoyalangani haqida o‘ylaydi. Haqiqatan, dunyo bo‘ylab har daqiqada millionlab insonlar shunga o‘xshash tizimlarga shaxsiy ma‘lumotlarini, jumladan, ism-familiyasi, tug‘ilgan sanasi, suratlariyu kundalik hayotiga oid turli lavhalarni joylamoqda. Biroq har doim ham ushbu ma‘lumotlarning xavfsizligi ta‘minlanmaydi. Hatto ba‘zan huquqiy jihatdan ma‘lumotlar xavfsizligini ta‘minlash kimning majburiyati ekanini aniqlab olish ham mushkul vazifa.

Qator izlanishlar natijasi shuni ko‘rsatadiki, jinoyatchilar ijtimoiy tarmoqlarda ko‘proq vaqt o‘tkazmoqda. Chunki endi jinoyat, jumladan, o‘g‘rilik qilmoqchi bo‘lgan shaxs “o‘lja”si haqidagi barcha ma‘lumotni ijtimoiy tarmoqlardan olishi mumkin. Boisi, ijtimoiy tarmoq foydalanuvchilarining ba‘zilari ushbu dasturlarning o‘zida belgilab qo‘yilgan ma‘lumotlar xavfsizligini ta‘minlashga xizmat qiluvchi sozlamalardan ham foydalanmaydi.

Odamlar ijtimoiy tarmoqlarda baham ko‘radigan katta hajmdagi ma‘lumotlar ishonchli qarindosh va do‘stlar doirasidan tashqaridagilarni ham jalb qiladi. Shunisi qiziqki, ko‘pchilik ijtimoiy tarmoqlarda hattoki hayotda umuman tanimaydigan, ko‘rmagan shaxslarning ham sahifalariga a‘zo bo‘lgan. Vaholanki, foydalanuvchilar ijtimoiy tarmoqlarda qayerga borgani, nimalar bilan mashg‘ulligi, hatto maosh olgani va qandaydir katta xaridlarni amalga oshirgani kabi shaxsiy ma‘lumotlarni ham joylamoqda. Buning barchasi ushbu ma‘lumotlar asosida jinoyat sodir qilish yoki ushbu shaxslarning huquqlarini poymol qiluvchi harakatlarni amalga oshirish imkonini yaratmoqda. Shunday qilib, spam-botlar, reklama kompaniyalari, bundan ham yomoni, kiberjinoyatchilar shaxsiy ma‘lumotlarga qiziqish bildirishi mumkin. Biroq ijtimoiy media maxfiylikini himoya qilish uchun tegishli choralar ko‘rish imkoniyati ham bor.

Foydalanilgan adabiyotlar ro'yxati:

1.https://uz.m.wikipedia.org/wiki/Axborot_xavfsizligi

2.<https://cyberleninka.ru/article/n/katta-hajmli-ma-lumotlarda-axborot-xavfsizligi-muammolari>

3.<https://yuz.uz/uz/news/shaxsga-doir-malumotlar-xavfsizligi-ijtimoiy-tarmoqlarda-ham-taminlanishi--shart>

4.<https://advice.uz/oz/document/2116>

5.<https://taschkent.diplo.de/uz-uz/-/1444718>