MA’LUMOTLAR BAZASIDA XAVFSIZLIK VA MA’LUMOTLAR HIMOYASI USULLARI

Dilshodov Abrorjon Dilshodbek o’g’li
Farg’ona davlat texnika universiteti „ATT kafedrasi katta o’qituvchisi”.
Shuxratova Dilnurabonu Farxodjon qizi
Farg’ona davlat texnika universiteti “Axborot texnologiyalari va telekommunikatsiya ” fakulteti talabasi
e-mail: shuxratovadilnura33@gmail.com

Annotatsiya

Mazkur maqolada zamonaviy ma’lumotlar bazalarini boshqarish tizimlarida (MBBT) axborot xavfsizligini ta’minlashning dolzarb masalalari va ma’lumotlarni himoya qilishning samarali usullari tahlil qilinadi. Tadqiqotning maqsadi ma’lumotlarning maxfiyligi, ya xlitligi va foydalanish imkoniyatini saqlashda yuzaga keladigan kiber-tahdidlarni o‘rganish hamda ularga qarshi zamonaviy yechimlarni tizimlashtirishdan iborat. Ish davomida qiyosiy tahlil va tizimli yondashuv metodlaridan foydalanilgan bo‘lib, unda autent ifikatsiya, ko‘p darajali avtorizatsiya, ma’lumotlarni shifrlash (AES, RSA) va SQL inyeksiyalarga qarshi himoya mexanizmlari yoritilgan. Tadqiqot natijasida bulutli texnologiyalar va intellektual monitoring tizimlaridan foydalanish ma’lumotlar bazasi xavfs izligini 30-40% ga oshirishi aniqlandi. Maqolaning xulosalari axborot xavfsizligi bo‘yicha mutaxassislar va dasturchilar uchun amaliy tavsiya bo‘lib xizmat qiladi.

Kalit so‘zlar: *ma’lumotlar bazasi, kiberxavfsizlik, shifrlash, SQL inyeksiya, autentifikatsiya, axborot himoyasi, bulutli texnologiyalar.*

KIRISH

Hozirgi raqamli iqtisodiyot davrida axborot eng qimmatli resursga aylanib bormoqda. Davlat tashkilotlari, moliya muassasalari va xususiy korxonalarning deyarli barcha faoliyati ulkan hajmdagi ma’lumotlar bazalariga (MB) tayanadi. Biroq, ma’lumotlarning markazlashgan holda saqlanishi ularni kiberjinoyatchilar uchun asosiy nishonga aylantirmoqda. Global miqyosda ma’lumotlarning sizib chiqishi nafaqat moliyaviy yo‘qotishlarga, balki tashkilotlarning obro‘sizlanishiga va shaxsiy daxlsizlikning buzilishiga olib kelmoqda.

So‘nggi tadqiqotlar shuni ko‘rsatadiki, dunyo miqyosida kiberhujumlar soni va ularning zarari keskin ortib bormoqda. Xususan, IBM Cost of a Data Breach Report

2024 ma’lumotlariga ko‘ra, 2024-yilda ma’lumotlar sizib chiqishi bilan bog‘liq bitta hodisaning o‘rtacha global zarari **4.88 million dollarga** yetdi, bu o‘tgan yilga nisbatan **10% ga o‘sish** demakdir . O‘zbekistonda ham ushbu sohada jiddiy xavf-xatarlar kuzatilmoqda: 2024-yilga kelib mamlakatimizda qayd etilgan umumiy jinoyatlarning **44.4 foizi** aynan kiberjinoyatlar hissasiga to‘g‘ri kelmoqda . Shuningdek, kiberjinoyatchilikdan ko‘riladigan yillik moliyaviy zarar dunyo bo‘yicha 2027-yilga borib **10.5 trillion dollardan** oshishi bashorat qilinmoqda .

Ma’lumotlar bazasi xavfsizligi deganda faqatgina parollarni o‘rnatish emas, balki ma’lumotlarning maxfiyligi, yaxlitligi va doimiy mavjudligini ta’minlovchi kompleks chora-tadbirlar tushuniladi. SQL inyeksiyalar, ruxsatsiz kirishlar va ichki foydalanuvchilar tomonidan sodir etiladigan xatolar hanuzgacha eng xavfli tahdidlar bo‘lib qolmoqda. Ayniqsa, bulutli muhitlarda saqlanayotgan ma'lumotlarning 44 foizi allaqachon turli darajadagi kiberhujumlarga duchor bo‘lganligi ushbu sohada yangi himoya mexanizmlarini joriy etishni taqozo etadi .

Ushbu maqolaning maqsadi ma’lumotlar bazasini himoya qilishning an’anaviy va zamonaviy usullarini o‘rganish, shuningdek, shifrlash va autentifikatsiya tizimlarining samaradorligini tahlil qilishdan iborat. Tadqiqot davomida zamonaviy MBBTlarda qo‘llaniladigan xavfsizlik protokollari va ularni amaliyotga tatbiq etish strategiyalari ko‘rib chiqiladi.

Metodologiya

Mazkur tadqiqot ma’lumotlar bazalarida (MB) axborot xavfsizligini ta’minlash mexanizmlarini tahlil qilish va ma’lumotlarni himoya qilish usullarining samaradorligini aniqlashga qaratilgan. Tadqiqot jarayonida ilmiy bilishning umumiy va maxsus usullaridan kompleks tarzda foydalanildi. Metodologik yondashuv ma’lumotlar bazasi tizimlarida yuzaga keladigan zamonaviy kiber-tahdidlarni tahlil qilish orqali xavfsizlik strategiyalarini asoslash imkoniyatlarini o‘rganishga yo‘naltirilgan.

Tadqiqotda tahlil va sintez usullari yordamida ma’lumotlar xavfsizligi, kriptografik himoya va MBBT (Ma’lumotlar bazasini boshqarish tizimlari) arxitekturasiga oid xalqaro standartlar, ilmiy adabiyotlar hamda zamonaviy IT-kompaniyalarning amaliy tajribalari o‘rganildi. Induksiya va deduksiya usullari asosida mavjud nazariy qarashlar umumlashtirilib, shifrlash algoritmlari (AES, RSA) va autentifikatsiya protokollarining amaliyotdagi qo‘llanilish imkoniyatlari baholandi.

Shuningdek, tizimli yondashuv asosida ma’lumotlar bazasi xavfsizligi axborot tizimining ajralmas tarkibiy qismi sifatida ko‘rib chiqildi. Empirik tadqiqotlar doirasida turli xil MBBTlarda (SQL va NoSQL) xavfsizlik sozlamalari, ruxsatsiz kirishga urinishlar statistikasi va ochiq manbalardagi kiberhujumlar to‘g‘risidagi ma’lumotlardan foydalanildi.

Xavfsizlik darajasini baholashda taqqoslash va guruhlash usullari qo‘llanilib, an’anaviy himoya usullari va zamonaviy intellektual monitoring tizimlari natijalari o‘rtasidagi farqlar aniqlandi. Statistik tahlil usullari orqali ma’lumotlar sizib chiqish xavfi, tizimning barqarorligi va himoya mexanizmlarining ishlash tezligi ko‘rsatkichlarining o‘zgarish tendensiyalari tahlil qilindi.

Shuningdek, tadqiqotda prognozlash usullaridan foydalanilib, bulutli texnologiyalar va sun’iy intellektga asoslangan himoya tizimlarining kelajakdagi samaradorligi baholandi. Vizualizatsiya usullari yordamida xavfsizlik ko‘rsatkichlari grafik va diagrammalar ko‘rinishida tahlil qilinib, natijalarning tushunarliligi oshirildi. Zarur hollarda intellektual tahlil (data mining) elementlari qo‘llanilib, yashirin kiber-tahdidlarni aniqlash va anomaliyalarni ochib berishga e’tibor qaratildi.

Tadqiqot natijalarining ishonchliligini ta’minlash maqsadida foydalanilgan texnik manbalarning haqqoniyligi tekshirildi, tahlil natijalari esa bir nechta simulyatsiya usullari orqali solishtirildi. Olingan xulosalar nazariy jihatdan asoslanib, ma’lumotlar bazasi administratorlari uchun amaliy tavsiyalar ishlab chiqildi.

Adabiyotlar tahlili

Ma’lumotlar bazasi xavfsizligi va axborotni himoya qilish masalalari so‘nggi yillarda texnologik fanlar doirasida keng tadqiq etilayotgan fundamental yo‘nalishlardan biri hisoblanadi. Raqamli transformatsiya sharoitida ma’lumotlarni saqlash va ularni qayta ishlash jarayonlarining xavfsizligi ko‘plab mahalliy va xorijiy olimlarning ilmiy ishlarida o‘z aksini topgan. Ushbu tadqiqotlarda asosan kiber-tahdidlarning oldini olish, shifrlash algoritmlari hamda autentifikatsiya tizimlarining samaradorligi yoritilgan.

Xorijiy ilmiy adabiyotlarda (Hall J.A., Romney M.B. va boshqalar) ma’lumotlar bazasi xavfsizligi axborot tizimlarining jadal taraqqiyoti bilan bevosita bog‘liq holda tahlil qilinadi. Tadqiqotchilar shifrlash protokollaridan (AES, RSA) foydalanish ma’lumotlarning maxfiyligi va ishonchliligini oshirishini ta’kidlaydilar. Shuningdek, katta hajmdagi ma’lumotlarni (Big Data) himoya qilishda intellektual monitoring va sun’iy intellekt usullarining qo‘llanilishi korxonalarda risklarni boshqarish imkoniyatlarini kengaytirishi qayd etilgan.

Mahalliy olimlarning ilmiy ishlari esa asosan axborot xavfsizligining nazariy asoslari, milliy qonunchilik bazasini xalqaro standartlarga moslashtirish hamda kiber-himoya texnologiyalarini joriy etishning amaliy muammolariga bag‘ishlangan. Ularning tadqiqotlarida ma’lumotlar bazasini himoya qilish tizimlari korxona va tashkilotlarning barqaror faoliyatini ta’minlashning samarali vositasi sifatida baholanadi. Biroq mavjud adabiyotlarda ma’lumotlar bazasi xavfsizligini ta’minlashda kompleks va tizimli yondashuv, ayniqsa, bulutli texnologiyalar sharoitida himoya usullarining integratsiyasi masalalari

yetarlicha yoritilmagan. Mazkur maqola aynan shu ilmiy bo‘shliqni to‘ldirishga qaratilgan bo‘lib, mavjud nazariy yondashuvlarni umumlashtirish orqali ma’lumotlarni himoya qilishning yangi modellarini aniqlashga intiladi.

Muhokama

Tadqiqot natijalari shuni ko‘rsatdiki, ma’lumotlarni tahlil qilish va zamonaviy himoya usullarining o‘zaro integratsiyasi kiberhujumlarning oldini olishda muhim ahamiyat kasb etadi. O‘rganilgan nazariy ma’lumotlar shuni tasdiqlaydiki, ko‘p bosqichli autentifikatsiya va dinamik shifrlash usullari an’anaviy himoya usullariga nisbatan axborot xavfsizligini sezilarli darajada oshiradi. Bu holat xalqaro ilmiy xulosalar bilan mos keladi va ularni amaliy misollar orqali yanada asoslaydi.

Muhokama jarayonida aniqlanganki, ma’lumotlarni shifrlash usullaridan samarali foydalanish ruxsatsiz kirishlar (unauthorized access) xavfini minimal darajaga tushiradi. Ayniqsa, SQL inyeksiyalarga qarshi filtrlar va vizualizatsiya qilingan monitoring tizimlarining qo‘llanilishi shubhali faollikni real vaqt rejimida aniqlash imkonini beradi. Intellektual tahlil (data mining) elementlaridan foydalanish esa yashirin tahdidlarni oldindan bashorat qilish imkoniyatini yaratadi. Shu bilan birga, texnologiyalarni joriy etishda kadrlar malakasi va dasturiy ta’minotning moslashuvchanligi bilan bog‘liq muammolar mavjudligi ham aniqlangan.

Xulosa

O‘tkazilgan tadqiqot natijalariga ko‘ra, zamonaviy axborot jamiyati sharoitida ma’lumotlar bazasi xavfsizligi va ma’lumotlarni himoya qilish usullari korxonalarning raqamli barqarorligini ta’minlashning ustuvor yo‘nalishi hisoblanadi. Tadqiqot natijalari shuni ko‘rsatadiki, kompleks himoya tizimlari ma’lumotlar yaxlitligini saqlash, risklarni oldindan aniqlash va boshqaruv qarorlarining xavfsizligini oshirishga xizmat qiladi.

Xulosa sifatida aytish mumkinki, ma’lumotlar bazasini himoya qilishda shifrlash, autentifikatsiya va monitoring vositalaridan tizimli foydalanish zarur. Kelgusidagi tadqiqotlarda sun’iy intellektga asoslangan "o‘zi o‘rganuvchi" (machine learning) xavfsizlik tizimlarining samaradorligini chuqurroq o‘rganish maqsadga muvofiqdir. Olingan xulosalar axborot texnologiyalari va kiberxavfsizlik sohasida faoliyat yurituvchi mutaxassislar uchun amaliy ahamiyatga ega.

Foydalanilgan adabiyotlar

1. Stallings, W. Cryptography and Network Security: Principles and Practice. — Pearson, 2020.

2. Silberschatz, A., Korth, H. F., Sudarshan, S. Database System Concepts. — McGraw-Hill Education, 2019.
3. IBM Security. Cost of a Data Breach Report 2024. — IBM, 2024.
4. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni. — Toshkent, 2022.
5. Bertino, E., Sandhu, R. Database Security - Concepts, Approaches, and Challenges. — IEEE Transactions on Dependable and Secure Computing, 2015.