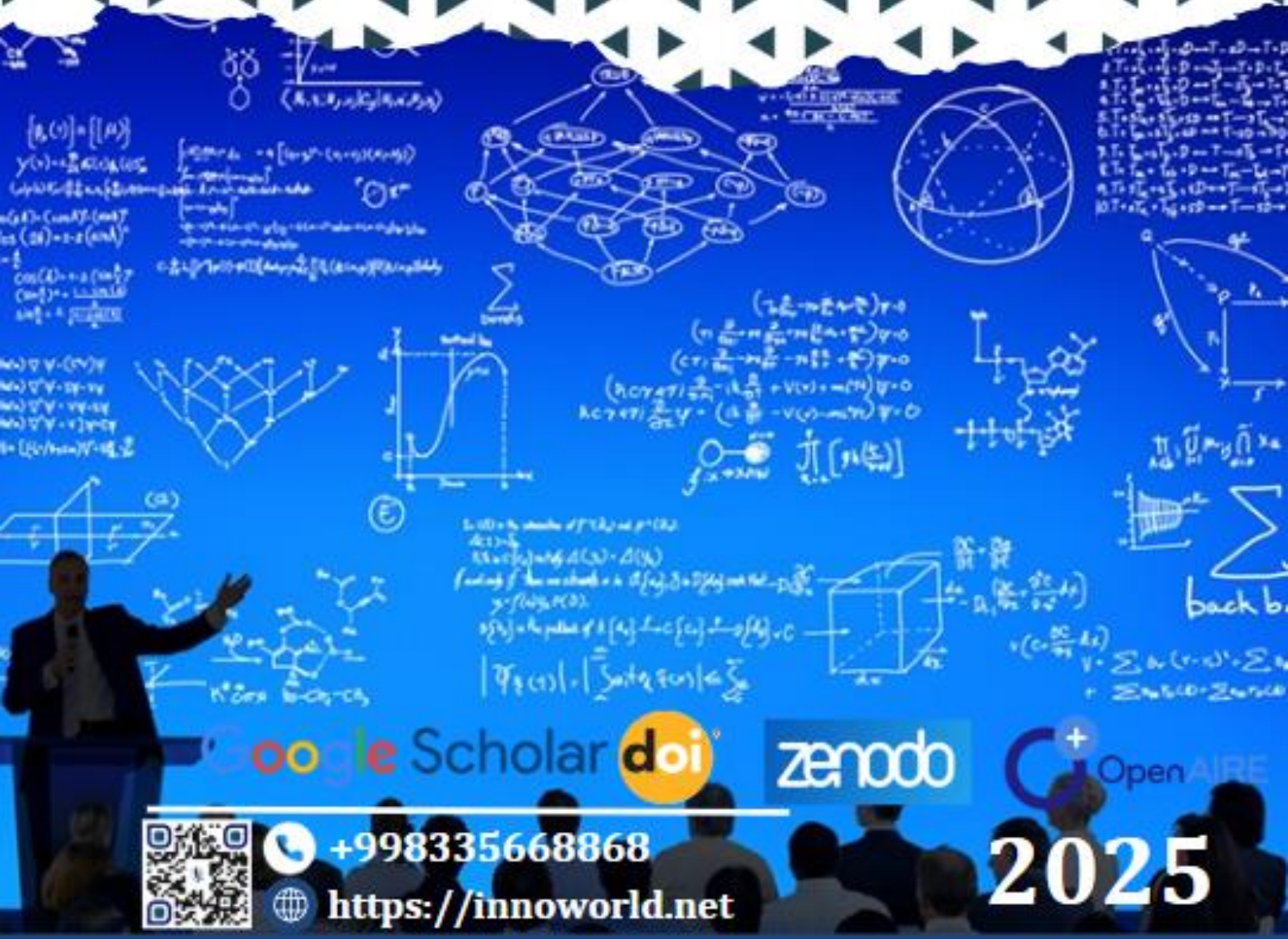
INNOVATIVE WORLD
Ilmiy tadqiqotlar markazi

ZAMONAVIY ILM-FAN VA TA'LIM: MUAMMO VA YECHIMLAR

ILMIY-AMALIY KONFERENSIYA



+998335668868
https://innoworld.net
2025

«INNOVATIVE WORLD» ILMIY TADQIQOTLARNI QO'LLAB-QUVVATLASH MARKAZI

«ZAMONAVIY ILM-FAN VA TADQIQOTLAR: MUAMMO VA YECHIMLAR» NOMLI 2025-YIL № 5-SONLI ILMIY, MASOFAVIY, ONLAYN KONFERENSIYASI

ILMIY-ONLAYN KONFERENSIYA TO'PLAMI
СБОРНИК НАУЧНЫХ-ОНЛАЙН КОНФЕРЕНЦИЙ
SCIENTIFIC-ONLINE CONFERENCE COLLECTION

www.innoworld.net
O'ZBEKISTON-2025

Ma'lumotlar bazasida xavfsizlik va himoya mexanizmlari.

Dumanov Ulug'bek
Axborot texnologiyalari va telekommunikatsiya fakulteti
Axborot xavfsizligi yo'nalishi 641-24AX guruh 2-bosqich talabasi
+998940626131, Ulugbekdumanov4@gmail.com
Pulatova Gulxayo
Farg'ona Davlat Texnika Universiteti

Annotatsiya: Mazkur maqolada ma'lumotlar bazalarida axborot xavfsizligini ta'minlash masalalari va ularni amalga oshirishda qo'llaniladigan zamonaviy himoya mexanizmlari yoritilgan. Axborot tizimlarida saqlanayotgan ma'lumotlarning hajmi va ahamiyati ortib borishi bilan birga, ularga bo'lgan tahdidlar ham murakkablashib bormoqda. Maqolada ma'lumotlar bazalariga nisbatan asosiy tahdidlar, autentifikatsiya va avtorizatsiya mexanizmlari, kriptografik himoya usullari, audit va monitoring tizimlari hamda zaxira nusxalash jarayonlari ilmiy-nazariy jihatdan tahlil qilinadi. Tadqiqot natijalari ma'lumotlar bazasi xavfsizligini ta'minlashda kompleks yondashuv zarurligini ko'rsatadi.

Kalit so'zlar: ma'lumotlar bazasi, axborot xavfsizligi, kiberxavfsizlik, autentifikatsiya, avtorizatsiya, shifrlash, kriptografiya, audit, monitoring, zaxira nusxa, ma'lumotlar yaxlitligi, maxfiylik, mavjudlik, ruxsatsiz kirish, xavfsizlik siyosati, foydalanuvchi huquqlari, SQL-inyeksiya, xavfsizlik modeli, axborot tizimi, himoya mexanizmlari.

Kirish: Bugungi kunda axborot texnologiyalarining jadal rivojlanishi natijasida ma'lumotlar bazalari deyarli barcha sohalarda asosiy axborot resursi sifatida xizmat qilmoqda. Bank tizimlari, davlat axborot resurslari, sog'liqni saqlash, ta'lim va sanoat korxonalarida katta hajmdagi muhim ma'lumotlar aynan ma'lumotlar bazalarida saqlanadi. Ushbu ma'lumotlarning yo'qolishi, buzilishi yoki oshkor bo'lishi jiddiy iqtisodiy va ijtimoiy oqibatlarga olib kelishi mumkin.

Shu sababli, ma'lumotlar bazasida xavfsizlik va himoya mexanizmlarini ishlab chiqish va takomillashtirish dolzarb ilmiy-amaliy muammo hisoblanadi. Axborot xavfsizligini ta'minlash nafaqat texnik vositalar, balki tashkiliy va nazariy yondashuvlarni ham talab etadi.

Tadqiqotning maqsadi: Mazkur tadqiqotning asosiy maqsadi ma'lumotlar bazalarida axborot xavfsizligini ta'minlashning ilmiy-nazariy asoslarini chuqur o'rganish hamda mavjud himoya mexanizmlarining samaradorligini kompleks tahlil qilishdan iborat. Bugungi kunda axborot tizimlari orqali qayta ishlanayotgan ma'lumotlarning hajmi keskin ortib borayotgani sababli, ma'lumotlar bazasiga nisbatan bo'ladigan tahdidlar ham ko'paymoqda. Ushbu holat xavfsizlik masalasini faqat texnik muammo emas, balki strategik va ilmiy masala sifatida ko'rib chiqishni talab etadi.

Tadqiqot doirasida ma'lumotlar bazasida xavfsizlikni ta'minlashga qaratilgan asosiy tamoyillarni aniqlash, mavjud xavfsizlik modellarini o'rganish va ularning afzallik hamda kamchiliklarini baholash ko'zda tutilgan. Shuningdek, autentifikatsiya, avtorizatsiya, shifrlash, audit, monitoring va zaxira nusxalash

kabi mexanizmlarning ma'lumotlar bazasi xavfsizligidagi o'rni va ahamiyatini ilmiy jihatdan asoslash tadqiqotning muhim vazifalaridan biri hisoblanadi.

Tadqiqotning yana bir maqsadi — zamonaviy kiberxavflar sharoitida ma'lumotlar bazasini himoyalashda kompleks yondashuv zarurligini ilmiy dalillar asosida ko'rsatib berishdir. Bu esa kelgusida axborot tizimlarini loyihalash, modernizatsiya qilish va ekspluatatsiya jarayonlarida xavfsizlik choralarini samarali joriy etishga xizmat qiladi.

Materiallar va metodlar: Tadqiqot jarayonida ilmiy tadqiqotning umumqabul qilingan metodologik yondashuvlaridan foydalanildi. Jumladan, tizimli tahlil metodi orqali ma'lumotlar bazasi xavfsizligi bir butun tizim sifatida ko'rib chiqildi va uning tarkibiy qismlari o'zaro bog'liqlikda tahlil qilindi. Ushbu yondashuv ma'lumotlar bazasiga tahdidlarni aniqlash va ularni bartaraf etish mexanizmlarini mukammal o'rganish imkonini berdi.

Qiyosiy tahlil metodi yordamida turli ma'lumotlar bazasi boshqaruv tizimlarida qo'llaniladigan xavfsizlik mexanizmlari solishtirildi. Natijada ularning o'ziga xos jihatlari, kuchli va zaif tomonlari aniqlanib, ilmiy xulosalar chiqarildi. Shuningdek, ilmiy adabiyotlarni tahlil qilish metodi orqali mahalliy va xorijiy olimlarning ushbu sohadagi tadqiqotlari o'rganildi.

Tadqiqot asosan nazariy xarakterga ega bo'lib, empirik tajribalar mavjud ilmiy ishlarga tayangan holda umumlashtirildi. Mantiqiy umumlashtirish va deduksiya metodlari yordamida ma'lumotlar bazasi xavfsizligiga oid nazariy tushunchalar shakllantirildi. Bundan tashqari, xalqaro standartlar, xususan ISO/IEC 27001 talablari tahlil qilinib, ularning ma'lumotlar bazasi xavfsizligini ta'minlashdagi o'rni baholandi.

Muhokama: Ma'lumotlar bazasida xavfsizlikni ta'minlash masalasi ko'p qirrali bo'lib, u texnik, tashkiliy va inson omillari bilan chambarchas bog'liqdir. Zamonaviy axborot tizimlarida xavfsizlikka bo'lgan talablar tobora ortib borayotganligi sababli, himoya mexanizmlarini chuqur tahlil qilish zarurati yuzaga kelmoqda.

Autentifikatsiya va avtorizatsiya mexanizmlari ma'lumotlar bazasi xavfsizligining asosiy elementlaridan biri hisoblanadi. Autentifikatsiya foydalanuvchining shaxsini aniqlash orqali tizimga kirishni nazorat qiladi, avtorizatsiya esa foydalanuvchining bajarishi mumkin bo'lgan amallarini cheklaydi. Ushbu mexanizmlar noto'g'ri sozlangan taqdirda, ichki foydalanuvchilar tomonidan sodir etiladigan xavfsizlik buzilishlari yuzaga kelishi mumkin.

Ma'lumotlarni shifrlash mexanizmlari maxfiy axborotni himoyalashda muhim ahamiyatga ega. Kriptografik algoritmlar yordamida shifrlangan ma'lumotlar ruxsatsiz shaxslar tomonidan qo'lga kiritilgan taqdirda ham foydasiz bo'lib qoladi. Shu bilan birga, shifrlash jarayonlari tizim unumdorligiga ta'sir qilishi mumkinligi sababli, optimal algoritmlarni tanlash muhim hisoblanadi.

Audit va monitoring mexanizmlari xavfsizlikni ta'minlashda nazorat vositasi sifatida xizmat qiladi. Audit loglari yordamida foydalanuvchilarning barcha harakatlari qayd etiladi va keyinchalik tahlil qilinadi. Monitoring tizimlari esa real vaqt rejimida xavfsizlik holatini kuzatib boradi va tahdidlarni tezkor aniqlash imkonini beradi.

Natijalar: O'tkazilgan ilmiy-nazariy tadqiqotlar natijasida ma'lumotlar bazasi xavfsizligini ta'minlashda kompleks yondashuvning ustunligi aniqlandi. Tadqiqot shuni ko'rsatdiki, faqat bitta himoya mexanizmini joriy etish yetarli emas, chunki zamonaviy kiberxavflar ko'p bosqichli va murakkab xarakterga ega.

Natijalarga ko'ra, autentifikatsiya va avtorizatsiya mexanizmlarining samaradorligi foydalanuvchi rollarini to'g'ri belgilash va minimal huquqlar tamoyiliga amal qilish bilan bevosita bog'liq. Shifrlash mexanizmlari esa ma'lumotlarning maxfiyligini ta'minlashda eng samarali vositalardan biri ekanligi ilmiy asoslandi.

Audit va monitoring tizimlari xavfsizlik hodisalarini aniqlash va ularga tezkor javob qaytarishda muhim rol o'ynashi isbotlandi. Shuningdek, zaxira nusxalash mexanizmlari ma'lumotlar mavjudligini ta'minlashda ajralmas vosita ekanligi aniqlandi. Ushbu natijalar ma'lumotlar bazasi xavfsizligini ta'minlashda tizimli yondashuv zarurligini ko'rsatadi.

Ilmiy-nazariy tadqiqotlar va nazariyalar: Ma'lumotlar bazasi xavfsizligi nazariy jihatdan bir nechta fundamental konsepsiyalarga asoslanadi. Ulardan eng muhimi CIA modeli bo'lib, u axborot xavfsizligining uch asosiy tamoyilini — maxfiylik, yaxlitlik va mavjudlikni belgilaydi. Ushbu model ma'lumotlar bazasini himoyalashda nazariy asos sifatida keng qo'llaniladi.

Shuningdek, "Defense in Depth" nazariyasi ma'lumotlar bazasi xavfsizligini ta'minlashda muhim o'rin tutadi. Ushbu nazariyaga ko'ra, axborot bir nechta mustaqil himoya qatlamlari orqali himoyalanishi lozim. Agar bitta qatlam buzilsa ham, qolgan qatlamlar xavfsizlikni ta'minlab turadi.

Rollarga asoslangan kirish nazorati (RBAC) modeli ham ma'lumotlar bazasi xavfsizligida keng qo'llaniladigan nazariy yondashuv hisoblanadi. Ushbu model foydalanuvchilarga individual emas, balki rollar orqali huquqlar berishni nazarda tutadi. Bu esa boshqaruvni soddalashtiradi va xatoliklar ehtimolini kamaytiradi.

Xulosa: Mazkur tadqiqot natijalari asosida quyidagi xulosalarga kelish mumkin: ma'lumotlar bazasida xavfsizlik va himoya mexanizmlari axborot tizimlarining ishonchli ishlashini ta'minlovchi asosiy omil hisoblanadi. Zamonaviy axborot muhitida tahdidlar doimiy ravishda rivojlanib borayotganligi sababli, xavfsizlik choralarini muntazam takomillashtirib borish zarur.

Tadqiqot shuni ko'rsatdiki, autentifikatsiya, avtorizatsiya, shifrlash, audit, monitoring va zaxira nusxalash mexanizmlarining kompleks qo'llanilishi yuqori darajadagi xavfsizlikni ta'minlaydi. Ilmiy-nazariy xulosalar kelgusida ma'lumotlar bazasi xavfsizligi sohasidagi tadqiqotlar va amaliy loyihalar uchun metodologik asos bo'lib xizmat qilishi mumkin.

Foydalanilgan adabiyotlar:

1. Silberschatz A., Korth H.F., Sudarshan S. *Database System Concepts*. McGraw-Hill, 2019.
2. Elmasri R., Navathe S. *Fundamentals of Database Systems*. Pearson, 2020.
3. Stallings W. *Cryptography and Network Security*. Pearson, 2018.
4. Date C.J. *An Introduction to Database Systems*. Addison-Wesley, 2017.
5. ISO/IEC 27001. Information Security Management Systems.