MA’LUMOTLAR BAZASIDA FOYDALANUVCHI HUQUQLARINI BOSHQARISH VA XAVFSIZLIK SIYOSATI

Mamarasulova Ruxshona Abdumuxtor qizi
Farg‘ona davlat texnika universiteti
Kompyuter injiniringi talabasi

Zokirov Sanjar Ikromjon o’g’li
Farg‘ona davlat texnika universiteti,
AAT kafedrasi dosenti.
Farg‘ona shahri, Mustaqillik shoh ko‘chasi, 185-uy 150100

Annotatsiya. Ushbu maqolada ma’lumotlar bazalarida foydalanuvchi huquqlarini boshqarish va xavfsizlik siyosatini shakllantirishning nazariy hamda amaliy jihatlari yoritiladi. Raqamli transformatsiya jarayonida axborot resurslarining ko‘payishi va ulardan ko‘p foydalanuvchili muhitda foydalanish ma’lumotlar xavfsizligini ta’minlash masalasini dolzarb qilib qo‘ymoqda. Maqolada autentifikatsiya va avtorizatsiya mexanizmlari, rollarga asoslangan kirish nazorati (RBAC), ma’lumotlarni himoyalash usullari, audit va monitoring jarayonlari tahlil qilinadi. Shuningdek, ma’lumotlar bazasida ruxsatsiz kirish, ichki tahdidlar va axborot sizib chiqishining oldini olishga qaratilgan xavfsizlik siyosatini ishlab chiqish tamoyillari ko‘rib chiqiladi. Tadqiqot natijalari axborot tizimlarida ishonchli, barqaror va xavfsiz ma’lumotlar boshqaruvini ta’minlashda muhim ahamiyatga ega.

Kalit so‘zlar: ma’lumotlar bazasi, foydalanuvchi huquqlari, xavfsizlik siyosati, autentifikatsiya, avtorizatsiya, RBAC, axborot xavfsizligi, audit.

Управление правами пользователей и политика безопасности в базе данных.

Мамарасулова Рухшона Абдумухтор кизи
Студентка факультета компьютерного инжиниринга
Ферганский государственный технический университет
Зокиров Санжар Икромжон угли
Доцент кафедры АИС (Автоматизированные информационные системы)
Ферганский государственный технический университет

город Фергана, улица Мустакиллик шох, дом 185, 150100.

Аннотация. В данной статье рассматриваются теоретические и практические аспекты управления правами пользователей и формирования политики безопасности в базах данных. В условиях цифровой трансформации и роста объёмов информации обеспечение защиты данных в многопользовательских средах приобретает особую актуальность. В работе анализируются механизмы аутентификации и авторизации, ролевой контроль доступа (RBAC), методы защиты данных, а также процессы аудита и мониторинга. Особое внимание уделяется разработке политики безопасности, направленной на предотвращение несанкционированного доступа, внутренних угроз и утечек информации. Результаты исследования способствуют повышению надёжности, устойчивости и безопасности систем управления базами данных.

Ключевые слова: база данных, права пользователей, политика безопасности, аутентификация, авторизация, RBAC, информационная безопасность, аудит.

USER RIGHTS MANAGEMENT AND SECURITY POLICY IN A DATABASE

Mamarasulova Ruxshona Abdumuxtor qizi
Student of Computer Engineering
Fergana State Technical University
Zokirov Sanjar Ikromjon o‘g‘li
Associate Professor of AIS (Automated Information Systems) Department
Fergana State Technical University
185, Mustaqillik Shokh street, Fergana city, 150100.

Abstract. This article discusses the theoretical and practical aspects of user rights management and security policy implementation in database systems. In the context of digital transformation and the rapid growth of data volumes, ensuring data security in multi-user environments has become a critical issue. The paper analyzes authentication and authorization mechanisms, role-based access control (RBAC), data protection methods, as well as auditing and monitoring processes. Special attention is given to the

development of security policies aimed at preventing unauthorized access, internal threats, and data leakage. The research findings contribute to improving the reliability, stability, and security of database management systems.

Keywords: database, user access control, security policy, authentication, authorization, RBAC, information security, audit.

KIRISH

Bugungi kunda raqamli texnologiyalarning jadal rivojlanishi natijasida axborot oqimi va ma’lumotlar hajmi misli ko‘rilmagan darajada oshib bormoqda. Davlat tashkilotlari, biznes subyektlari va ta’lim muassasalari faoliyatida katta hajmdagi ma’lumotlarni ishonchli saqlash, tezkor qayta ishlash va samarali boshqarish muhim strategik vazifaga aylanmoqda. Ayniqsa, ko‘p foydalanuvchili axborot tizimlarida ma’lumotlardan foydalanish jarayonini nazorat qilish va ularning xavfsizligini ta’minlash dolzarb masalalardan biridir.

An’anaviy ma’lumotlar bazalari uzoq yillar davomida axborotni saqlash va boshqarish vazifasini bajargan bo‘lsa-da, zamonaviy talablar ularning imkoniyatlarini kengaytirishni taqozo etmoqda. Bulutli ma’lumotlar bazalarining joriy etilishi infratuzilmani soddalashtirish, resurslarni dinamik masshtablash va xarajatlarni optimallashtirish imkonini yaratdi. Shu bilan birga, foydalanuvchilarning turli darajadagi huquqlarini aniqlash va ularni qat’iy boshqarish masalasi axborot xavfsizligining ajralmas qismiga aylandi.

Sun’iy intellekt texnologiyalarining rivojlanishi ma’lumotlar bazalari bilan ishlash jarayonlarini yangi bosqichga olib chiqdi. Avtomatlashtirilgan tahlil, bashoratlash va qaror qabul qilish mexanizmlari ma’lumotlardan yanada samarali foydalanish imkonini bermoqda. Biroq ushbu jarayonlarda ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlash, shuningdek ruxsatsiz kirish va ichki tahdidlarning oldini olish muhim ahamiyat kasb etadi.

Shu nuqtayi nazardan, ma’lumotlar bazalarida foydalanuvchi huquqlarini boshqarish, autentifikatsiya va avtorizatsiya mexanizmlarini joriy etish, xavfsizlik siyosatini ishlab chiqish va amaliyotga tatbiq etish zarurati yuzaga kelmoqda. Mazkur maqola ma’lumotlar bazalarida foydalanuvchi huquqlarini boshqarish va xavfsizlik siyosatini shakllantirishning asosiy tamoyillari, zamonaviy yondashuvlari hamda ularning amaliy qo‘llanilish imkoniyatlarini tahlil qilishga bag‘ishlanadi.

ASOSIY QISM

Zamonaviy axborot tizimlarida ma’lumotlar bazalari markaziy o‘rin egallab, ularda saqlanadigan axborotning hajmi va ahamiyati tobora ortib bormoqda. Bulutli texnologiyalar va sun’iy intellekt asosidagi tizimlarning keng joriy etilishi ma’lumotlardan foydalanish imkoniyatlarini kengaytirgan bo‘lsa-da, bir vaqtning o‘zida axborot xavfsizligini ta’minlash masalasini yanada murakkablashtirmoqda. Ayniqsa, ko‘p foydalanuvchili muhitda ma’lumotlar bazasiga kirishni tartibga solish va foydalanuvchi huquqlarini aniq belgilash muhim vazifa hisoblanadi.

Ma’lumotlar bazasida foydalanuvchi huquqlarini boshqarish jarayoni autentifikatsiya va avtorizatsiya mexanizmlariga asoslanadi. Autentifikatsiya foydalanuvchining shaxsini aniqlashni ta’minlasa, avtorizatsiya esa unga berilgan huquqlar doirasida ma’lumotlarga kirish imkoniyatini belgilaydi. Zamonaviy tizimlarda rollarga asoslangan kirish nazorati (RBAC) keng qo‘llanilib, foydalanuvchilarga lavozimi yoki vazifasiga mos huquqlarni berish orqali axborotdan foydalanish samaradorligi va xavfsizligi oshiriladi.

Bulutli ma’lumotlar bazalarida foydalanuvchi huquqlarini boshqarish yanada muhim ahamiyat kasb etadi. Chunki bunday muhitda ma’lumotlarga turli joylardan va turli qurilmalar orqali murojaat qilinadi. Shu sababli, minimal huquqlar tamoyili (Least Privilege Principle) asosida foydalanuvchilarga faqat zarur bo‘lgan ruxsatlarni berish axborot sizib chiqishining oldini olishga xizmat qiladi. Bundan tashqari, vaqtinchalik va shartli ruxsatlar orqali ma’lumotlar bazasining himoyalanganlik darajasi oshiriladi.

Ma’lumotlar xavfsizligini ta’minlashda shifrlash texnologiyalari muhim o‘rin tutadi. Ma’lumotlarni saqlash jarayonida (data at rest) va uzatish jarayonida (data in transit) shifrlash usullaridan foydalanish ruxsatsiz kirish holatlarida ham axborotning maxfiyligini saqlab qolishga yordam beradi. Shuningdek, zaxira nusxalarini yaratish va avariyadan tiklash mexanizmlarini joriy etish ma’lumotlarning yo‘qolish xavfini sezilarli darajada kamaytiradi.

Sun’iy intellekt texnologiyalari ma’lumotlar bazasi xavfsizligini oshirishda qo‘shimcha imkoniyatlar yaratmoqda. Intellektual monitoring tizimlari foydalanuvchilarning noodatiy faolligini aniqlash, shubhali kirish urinishlarini tahlil qilish va potentsial tahdidlarni oldindan bashorat qilish imkonini beradi. Bu esa xavfsizlik siyosatini yanada takomillashtirish va real vaqt rejimida himoya choralarini ko‘rishga xizmat qiladi.

Ma’lumotlar bazalarida xavfsizlik siyosatini ishlab chiqish jarayonida audit va nazorat mexanizmlarini joriy etish ham muhim hisoblanadi. Foydalanuvchilarning barcha harakatlarini qayd etish, tizim jurnalini yuritish va muntazam tahlil qilish orqali ichki va tashqi tahdidlarning oldini olish mumkin. Xalqaro xavfsizlik standartlariga mos siyosatni qo‘llash esa tizimning ishonchliligi va barqarorligini ta’minlaydi.

Umuman olganda, ma’lumotlar bazalarida foydalanuvchi huquqlarini boshqarish va xavfsizlik siyosatini to‘g‘ri tashkil etish axborot tizimlarining samarali ishlashini ta’minlaydi. Bulutli texnologiyalar va sun’iy intellekt bilan integratsiyalashgan bunday tizimlar ma’lumotlardan xavfsiz, tezkor va ishonchli foydalanish imkonini yaratib, tashkilotlarning raqamli rivojlanishida muhim ahamiyat kasb etadi.

METODOLOGIYA

Mazkur tadqiqotda ma’lumotlar bazalarida foydalanuvchi huquqlarini boshqarish va xavfsizlik siyosatini shakllantirish jarayonlarini chuqur o‘rganish maqsadida kompleks metodologik yondashuvlardan foydalanildi. Tadqiqot jarayonida nazariy tahlil, empirik kuzatishlar hamda zamonaviy axborot tizimlari tajribasiga asoslangan usullar uyg‘unlashtirildi. Bu yondashuvlar foydalanuvchi huquqlarini boshqarish mexanizmlarining samaradorligi va xavfsizlik darajasini baholash imkonini berdi.

Adabiyotlarni tahlil qilish. Tadqiqotning nazariy asoslarini shakllantirish maqsadida ma’lumotlar bazalari, axborot xavfsizligi, foydalanuvchi huquqlarini boshqarish, bulutli texnologiyalar va sun’iy intellekt sohalariga oid ilmiy maqolalar, monografiyalar hamda xalqaro standartlar tizimli ravishda tahlil qilindi. Ushbu bosqichda autentifikatsiya va avtorizatsiya mexanizmlari, rollarga asoslangan kirish nazorati (RBAC) hamda xavfsizlik siyosatini ishlab chiqish bo‘yicha asosiy konsepsiyalar aniqlab olindi.

Nazariy tahlil. Nazariy tahlil jarayonida foydalanuvchi huquqlarini boshqarish modellari, axborot xavfsizligi tamoyillari va xavfsizlik siyosatini joriy etish usullari o‘rganildi. Mazkur yondashuv orqali mavjud modellar va konsepsiyalarning afzalliklari hamda cheklovlari aniqlanib, ularni bulutli ma’lumotlar bazalari sharoitida qo‘llash imkoniyatlari baholandi.

Empirik tadqiqotlar. Empirik tadqiqotlar doirasida real axborot tizimlari, jumladan bulutli platformalarda faoliyat yuritayotgan ma’lumotlar bazalari va ularga integratsiyalashgan xavfsizlik mexanizmlari tahlil qilindi. Tadqiqot davomida

foydalanuvchi kirishlarini boshqarish, ruxsatlarni taqsimlash va xavfsizlik hodisalariga javob berish jarayonlarining samaradorligi baholandi.

Kvantitativ va sifatli tahlil. Tizimlarning samaradorligini aniqlash uchun kvantitativ va sifatli tahlil usullari qo‘llanildi. Kvantitativ tahlil orqali ma’lumotlarga kirish tezligi, ruxsatlarni qayta ishlash va tizim yuklamasi kabi ko‘rsatkichlar o‘rganildi. Sifatli tahlil esa foydalanuvchi tajribasi, qulaylik darajasi va xavfsizlik siyosatining tushunarliligi kabi subyektiv omillarni baholashga xizmat qildi.

Case Study (holatni o‘rganish). Bulutli ma’lumotlar bazalarida foydalanuvchi huquqlarini boshqarish va xavfsizlik siyosati muvaffaqiyatli joriy etilgan bir nechta real loyihalar misolida chuqur tahlil amalga oshirildi. Ushbu usul orqali tizimlarning funksionalligi, himoyalanganlik darajasi, avtomatlashtirish imkoniyatlari va amaliy samaradorligi baholandi.

Ekspert intervyulari. Axborot texnologiyalari va axborot xavfsizligi sohasida faoliyat yuritayotgan mutaxassislar bilan o‘tkazilgan intervyular orqali foydalanuvchi huquqlarini boshqarishdagi mavjud muammolar, xavfsizlik tahdidlari va kelajakdagi rivojlanish istiqbollari yuzasidan ekspert xulosalari olindi. Ushbu ma’lumotlar tadqiqot natijalarini boyitish va amaliy tavsiyalar ishlab chiqishda muhim ahamiyat kasb etdi.

Tadqiqot metodlari jadvali

Tadqiqot metodi	Tavsif	Qo‘llanilish sohasi	Ma’lumotlar turi
Adabiyotlarni tahlil qilish	Ilmiy manbalarni tizimli o‘rganish	Ma’lumotlar bazalari va axborot xavfsizligi	Ilmiy maqolalar, monografiyalar
Nazariy tahlil	Nazariy modellar va konsepsiyalarni tahlil qilish	Foydalanuvchi huquqlarini boshqarish	Ilmiy manbalar
Empirik tadqiqotlar	Real tizimlarni amaliy o‘rganish	Bulutli ma’lumotlar bazalari	Amaliy misollar
Kvantitativ tahlil	Raqamli ko‘rsatkichlar asosida baholash	Tizim samaradorligi	Statistik ma’lumotlar
Sifatli tahlil	Foydalanuvchi tajribasini tahlil qilish	Inson–tizim o‘zaro aloqasi	Intervyu va kuzatishlar

Case Study	Alohida loyihani chuqur o‘rganish	Xavfsizlik siyosatini joriy etish	Real loyiha ma’lumotlari
Ekspert intervyulari	Mutaxassislar fikrlarini tahlil qilish	Professional baholash	Ekspert tavsiyalari

TAHLIL

Bulutli ma’lumotlar bazalari va sun’iy intellekt texnologiyalari ma’lumotlarni saqlash, qayta ishlash va tahlil qilish jarayonlarini sezilarli darajada soddalashtiradi. Bulutli platformalar foydalanuvchilarga ma’lumotlarga istalgan joy va vaqtda kirish imkonini berib, tizimning barqaror ishlashini va ma’lumotlar yo‘qolishining oldini oladi.

Sun’iy intellekt algoritmlari katta hajmdagi ma’lumotlarni tezkor tahlil qilish va bashoratlash imkonini bersa-da, noto‘g‘ri sozlangan yoki yetarli darajada himoyalanmagan tizimlar axborot xavfsizligiga tahdid tug‘dirishi mumkin. Shu sababli foydalanuvchi huquqlarini qat’iy boshqarish, ishonchli autentifikatsiya va doimiy monitoring muhim ahamiyatga ega.

Bulutli va intellektual tizimlar jarayonlarni avtomatlashtirib, inson omili bilan bog‘liq xatoliklarni kamaytiradi hamda qaror qabul qilish jarayonini tezlashtiradi. Kelajakda ushbu texnologiyalar yanada rivojlanib, xavfsizlik mexanizmlarining takomillashuvi orqali tizim samaradorligini oshirishi kutilmoqda.

NATIJALAR

Tadqiqot natijalari shuni ko‘rsatdiki, bulutli ma’lumotlar bazalari va sun’iy intellekt texnologiyalari tashkilotlarda ma’lumotlarni boshqarish jarayonlarini avtomatlashtirish va samarali tashkil etishga yordam beradi.

Texnologiyalarning samaradorligi: Bulutli platformalar va sun’iy intellekt modullari ma’lumotlarni real vaqt rejimida yangilash, avtomatik tahlil va bashorat qilish imkonini beradi. Natijada, qarorlar tez va aniq qabul qilinadi.

Xavf-xatarlar**.** Noto‘g‘ri sozlangan yoki yetarli darajada himoyalanmagan tizimlar ma’lumot xavfsizligiga tahdid soladi. Shifrlash, kuchli autentifikatsiya va doimiy monitoring muhim.

Integratsiya va optimallashtirish: Bulutli saqlash va avtomatlashtirilgan intellekt modullari ma’lumotlarni tez va ishonchli qayta ishlash imkonini beradi. Vizual va statistik tahlil vositalari qaror qabul qilishni yengillashtiradi.

Kelajak istiqbollari. Texnologiyalar rivojlanishi tizim samaradorligini oshiradi, xatoliklarni kamaytiradi va foydalanuvchi ma’lumotlarini himoya qiladi, biroq xavfsizlik choralarini muntazam yangilab borish zarur.

Ekspert baholari. Mutaxassislar texnologiyalarni samarali deb baholaydilar, ammo xavfsizlik, monitoring va foydalanuvchi huquqlarini boshqarishga doimiy e’tibor qaratish zarurligini ta’kidlaydilar.

XULOSA

Bulutli ma’lumotlar bazalari va sun’iy intellekt texnologiyalari tashkilotlarga ma’lumotlarni tezkor, ishonchli va samarali boshqarish imkonini beradi. Tadqiqot shuni ko‘rsatdiki, bu texnologiyalar ish samaradorligini oshiradi, xatoliklarni kamaytiradi va qaror qabul qilish jarayonlarini optimallashtiradi.

Shu bilan birga, xavfsizlik va foydalanuvchi ma’lumotlarini himoya qilishga alohida e’tibor qaratish lozim. Kelajakda tizimlarni doimiy yangilab borish, xavfsizlik choralarini kuchaytirish va monitoring qilish zarurati saqlanadi. Umuman olganda, bulutli va intellektual tizimlar tashkilotlarga tezkorlik, qulaylik va ishonchlilikni ta’minlaydi, ammo ularni joriy etishda ehtiyotkorlik va doimiy nazorat asosiy talab hisoblanadi.

FOYDALANILGAN ADABIYOTLAR:

1.Vasilenko, A., Kukushkin, A. Mobile Applications in Accounting Management: Current Trends and Challenges. Journal of Financial Technology, 2023, Vol. 15, No. 2, pp. 55–70.

2.Bishop, M. Introduction to Accounting Systems. Addison-Wesley, 2022, pp. 23–41.

3.Müller, J. M., Smolka, P. Big Data and Cloud Computing in Modern Enterprises. Springer, 2021, pp. 78–102.

4.Abduraxmanov, J. K. Diskret tuzilmalar. Toshkent: Fan, 2019, 45–63-betlar.

5.Shvets, I. Cloud Computing Security and Data Privacy. Moscow: Informatics, 2020, pp. 112–134.

6.Kagan, A., Brown, S. Artificial Intelligence in Business Analytics. Wiley, 2022, pp. 56–79.

7.Polvonov, A. Physika gazovogo razryada [Gaz razryadi fizikasi]. Toshkent: TATU Press, 2018, 91–115-betlar.
8.Zubarev, E., Ivanov, P. Data Management and Security in Cloud-Based Systems. Springer, 2021, pp. 139–162.