DOI: 10.65322/j.srd.05192026.108

MA'LUMOTLAR BAZASINI BOSHQARISH TIZIMLARIDA AXBOROT XAVFSIZLIGINI TA'MINLASH USULLARI

Сабирова О.Ш., *PhD,*
E-mail:ozodasobirova1984@gmail.com,
Namangan davlat texnika universiteti

Annotatsiya: *Ushbu maqolada ma'lumotlar bazasini boshqarish tizimlarida axborot xavfsizligini ta'minlashning asosiy usullari va mexanizmlari tahlil qilingan. Ma'lumotlar bazalarida saqlanadigan axborotni ruxsatsiz kirish, o'zgartirish va oshkor etilishdan himoyalash masalalariga alohida e'tibor qaratilgan. Tadqiqot doirasida Oracle Database, MySQL va Microsoft SQL Server tizimlarida qo'llaniladigan autentifikatsiya, avtorizatsiya, audit va shifrlash mexanizmlarining xususiyatlari ko'rib chiqilgan. Shuningdek, mazkur tizimlarning himoya vositalari, afzalliklari va ayrim cheklovlari tahlil etilgan. Tadqiqot natijalari ma'lumotlar bazalarida axborot xavfsizligini ta'minlashda foydalanuvchilar huquqlarini boshqarish, tizimdagi hodisalarni qayd etish va ma'lumotlarni shifrlash mexanizmlaridan kompleks foydalanish muhimligini ko'rsatadi.*

Аннотация*: В данной статье анализируются основные методы и механизмы обеспечения информационной безопасности в системах управления базами данных. Особое внимание уделяется защите информации, хранящейся в базах данных, от несанкционированного доступа, изменения и раскрытия. В рамках исследования рассматриваются особенности механизмов аутентификации, авторизации, аудита и шифрования, применяемых в системах Oracle Database, MySQL и Microsoft SQL Server. Также анализируются средства защиты, преимущества и отдельные ограничения указанных систем. Результаты исследования показывают, что для обеспечения информационной безопасности баз данных важное значение имеет комплексное применение механизмов управления правами пользователей, регистрации событий в системе и шифрования данных.*

Abstract*: This article analyzes the main methods and mechanisms for ensuring information security in database management systems. Particular attention is paid to protecting information stored in databases against unauthorized access, modification, and disclosure. The study examines the features of authentication, authorization, auditing, and encryption mechanisms implemented in Oracle Database, MySQL, and Microsoft SQL Server. The security tools, advantages, and certain limitations of these systems are also analyzed. The findings highlight the importance of applying user access control, system event logging, and data encryption mechanisms in combination to improve database information security.*

Kalit so'zlar: *ma'lumotlar bazasi, ma'lumotlar bazasini boshqarish tizimi, axborot xavfsizligi, autentifikatsiya, avtorizatsiya, audit, shifrlash, Oracle Database, MySQL, Microsoft SQL Server.*

Ключевые слова: *база данных, система управления базами данных, информационная безопасность, аутентификация, авторизация, аудит, шифрование, Oracle Database, MySQL, Microsoft SQL Server.*

Keywords: *database, database management system, information security, authentication, authorization, auditing, encryption, Oracle Database, MySQL, Microsoft SQL Server.*

Kirish. Hozirgi axborotlashgan jamiyatda ma'lumotlar bazalari davlat boshqaruvi, ta'lim, iqtisodiyot, bank-moliya tizimi, sanoat va boshqa ko'plab sohalarda axborotni saqlash, qayta ishlash hamda uzatishning muhim vositasi hisoblanadi. Ushbu jarayonlarda ma'lumotlar bazasini boshqarish tizimlari (MBBT) katta hajmdagi axborot bilan ishlash, ma'lumotlarning yaxlitligini

DOI: 10.65322/j.srd.05192026.108

ta’minlash va ulardan samarali foydalanish imkonini beradi. Ma’lumotlar bazasi xavfsizligi foydalanuvchilarni identifikatsiya qilish, ularning haqiqiyligini tekshirish, foydalanish huquqlarini belgilash, tizimdagi operatsiyalarni qayd etish hamda ma’lumotlarni shifrlash kabi o‘zaro bog‘liq mexanizmlarga asoslanadi. Ushbu mexanizmlarning samarali tashkil etilishi axborotdan faqat tegishli vakolatga ega foydalanuvchilar foydalanishini ta’minlashga xizmat qiladi.

Maqolaning maqsadi ma’lumotlar bazasini boshqarish tizimlarida axborot xavfsizligini ta’minlash usullarini o‘rganish, keng tarqalgan MBBTlarda qo‘llaniladigan himoya mexanizmlarini tahlil qilish va ularning afzalliklari hamda cheklovlarini aniqlashdan iborat.

Ushbu maqsadga erishish uchun ma’lumotlar bazalarini himoyalashning asosiy yondashuvlarini o‘rganish, Oracle Database, MySQL va Microsoft SQL Server tizimlaridagi xavfsizlik mexanizmlarini ko‘rib chiqish hamda ma’lumotlar bazasi himoyasini takomillashtirishga oid xulosalarni shakllantirish vazifalari belgilandi.

Adabiyotlar tahlili. Ma’lumotlar bazalarini boshqarish va ularning xavfsizligini ta’minlash masalalari ma’lumotlar bazasi nazariyasi, axborot xavfsizligi va dasturiy tizimlarni boshqarish yo‘nalishlaridagi ilmiy adabiyotlarda yoritilgan.

C.J.Date tomonidan yozilgan An Introduction to Database Systems asarida ma’lumotlar bazalarini tashkil etish, ularning tuzilishi va boshqarish tamoyillari bayon qilingan. Ushbu manba ma’lumotlar bazalarining ishlash asoslarini tushunish va ularni boshqarish jarayonlarini o‘rganishda muhim nazariy manba hisoblanadi.

S.R.Alapati tomonidan tayyorlangan Oracle Database 11g: Руководство администратора баз данных asarida Oracle Database tizimini boshqarish, foydalanuvchilar bilan ishlash va ma’lumotlar bazasining asosiy ma’muriy mexanizmlari yoritilgan. Ushbu manba Oracle muhitida xavfsizlikni boshqarish tamoyillarini o‘rganishda ahamiyatga ega.

Bundan tashqari, DB-Engines resursining 2015-yil aprel oyidagi ma’lumotlari asosida Oracle Database, MySQL va Microsoft SQL Server keng tarqalgan ma’lumotlar bazasini boshqarish tizimlari sifatida tanlangan. Ushbu tizimlar misolida autentifikatsiya, avtorizatsiya, audit va shifrlash mexanizmlarini ko‘rib chiqish ma’lumotlar bazalarini himoyalash yondashuvlarini qiyosiy tahlil qilish imkonini beradi.

Tahlil qilingan manbalar ma’lumotlar bazalarini tashkil etish va boshqarishning nazariy asoslarini o‘rganishga yordam beradi. Shu bilan birga, mazkur maqolada asosiy e’tibor ma’lumotlar bazalarini himoyalashning amaliy mexanizmlari hamda ularning o‘zaro bog‘liqligiga qaratilgan.

Asosiy qism. Ma’lumotlar bazasini boshqarish tizimlari (MBBT) avtomatlashtirilgan boshqaruv tizimlarining (ABT) ajralmas tarkibiy qismi hisoblanadi. Zamonaviy kompyuter tarmoqlari asosida korporativ avtomatlashtirilgan boshqaruv tizimlari infratuzilmasini yaratishda ushbu tizimlarning axborot xavfsizligini ta’minlash masalasi muqarrar ravishda yuzaga keladi. Ma’lumotlar bazalaridan jamiyat hayotining barcha sohalarida keng foydalanilishi bilan belgilanadi. Shu sababli ma’lumotlar bazalarida saqlanadigan axborotning himoyalanganligini ta’minlash muhim ilmiy-amaliy ahamiyat kasb etadi.

Ma’lumotlarni himoyalash muammosi ko‘plab jihatlarni qamrab oladi. Jumladan, huquqiy, jismoniy va tashkiliy himoya choralari, apparat vositalari orqali himoyalash, operatsion tizimlarning imkoniyatlari, shuningdek, bevosita ma’lumotlar bazasini boshqarish tizimlariga taalluqli xavfsizlik masalalari shular jumlasidandir.

Zamonaviy ma’lumotlar bazasini boshqarish tizimlarida, odatda, ma’lumotlarni himoyalashni tashkil etishning keng tarqalgan ikkita usulidan biri –

1-*tanlab foydalanishni boshqarish (diskretsion nazorat)*

2-mandatli foydalanishni boshqarish usuli qo‘llab-quvvatlanadi.

DOI: 10.65322/j.srd.05192026.108

Tanlab foydalanishni boshqarish usulida har bir foydalanuvchiga, odatda, muayyan foydalanish huquqlari beriladi. Bunda turli foydalanuvchilar bitta ma'lumotlar bazasi obyektiga nisbatan turlicha foydalanish huquqlariga ega bo'lishi mumkin [1-3].

Mandatli nazorat usulida esa, aksincha, har bir ma'lumotlar obyektiga muayyan tasniflash darajasi belgilanadi, har bir foydalanuvchiga esa tegishli ruxsat darajasi tayinlanadi.

Mutlaq himoyani ta'minlaydigan tizimlar mavjud emas. Yetarlicha qat'iyatli va malakali buzg'unchi nazorat mexanizmlarini chetlab o'tishi mumkin. Shu sababli muhim ma'lumotlar bilan ishlash jarayonida tizimda sodir bo'ladigan barcha hodisalar qayd etiladigan nazorat jurnalini tashkil etish zarurati yuzaga keladi. Olingan natijalardagi har qanday nomuvofiqlik axborotning qasddan buzilganidan dalolat berishi mumkin. Bunday vaziyatlarda hodisaning sabablarini aniqlash uchun nazorat jurnalidagi yozuvlardan foydalanish mumkin.

Nazorat jurnali asosiy ma'lumotlar bazasi bilan ishlash jarayonida foydalanuvchilar tomonidan bajarilgan barcha operatsiyalar to'g'risidagi ma'lumotlar avtomatik ravishda qayd etiladigan fayl yoki ma'lumotlar bazasidan iborat bo'ladi.

Agar foydalanuvchi ma'lumotlar bazasiga tizimning standart vositalari orqali emas, balki tizimni chetlab o'tish yo'li bilan kirishga urinsa, masalan, axborot tashuvchilarni ko'chirish yoki aloqa liniyasiga bevosita ulanish orqali ma'lumotlarni qo'lga kiritishga harakat qilsa, bunday holatlarga qarshi kurashishning eng samarali usullaridan biri ma'lumotlarni shifrlash hisoblanadi. Ma'lumotlar bazalarida AES yoki RSA kabi turli shifrlash algoritmlaridan foydalanish mumkin.

Yuqoridagilardan kelib chiqib, ma'lumotlar bazalarida saqlanadigan axborot ruxsatsiz kirishdan himoyalangan bo'lishi lozim. Buning uchun quyidagi chora-tadbirlarni amalga oshirish zarur:

Parol yordamida himoyalash – tizimda ro'yxatdan o'tgan va vakolatga ega foydalanuvchilarning kirish huquqlarini belgilash imkonini beradi.

Ma'lumotlar bazasi obyektlariga kirish huquqlarini cheklash – foydalanuvchilarning ma'lumotlar bazasi obyektlari bilan bajarishi mumkin bo'lgan amallarini belgilash va nazorat qilishga xizmat qiladi.

Nazorat jurnallarini joriy etish – ma'lumotlar bazasini boshqarish tizimlari tomonidan taqdim etiladigan ushbu vositalar foydalanish huquqlarining buzilishi va tizimdagi xavfsizlik hodisalarini nazorat qilish imkonini beradi.

Ma'lumotlarni shifrlash – ma'lumotlar bazasining ayrim himoya bosqichlarini chetlab o'tgan ruxsatsiz foydalanuvchilarning ma'lumotlardan bevosita foydalanishiga yo'l qo'ymaslik uchun qo'llaniladi.

Ushbu himoyalash usullarini ma'lumotlar bazasi xavfsizligini ta'minlashning asosiy mexanizmlari sifatida baholash mumkin. Ular turli shakllarda bo'lsa-da, ko'rib chiqilayotgan ma'lumotlar bazasini boshqarish tizimlarining barchasida mavjud.

Ma'lumotlar bazasini boshqarish tizimlarida himoyalash usullari samaradorligini tahlil qilish

Ma'lumotlar bazalarini himoyalash usullarining samaradorligini tahlil qilish uchun eng keng tarqalgan ma'lumotlar bazasini boshqarish tizimlari tanlab olindi.

DB-Engines resursining 2015-yil aprel oyidagi ma'lumotlariga ko'ra, bunday tizimlar qatoriga Oracle Database, MySQL va Microsoft SQL Server kiradi. Ushbu tizimlar ommaboplik reytingida raqobatchilaridan sezilarli darajada ustunlik bilan dastlabki uchta o'rinni egallagan.

Oracle Database tizimida ma'lumotlar bazalarini himoyalashning asosiy usullari quyidagilardan iborat:

- Qonuniy foydalanuvchilarning kirish imkoniyatlarini cheklash (autentifikatsiya).
- Ma'lumotlardan foydalanishni boshqarish (avtorizatsiya).
- Foydalanuvchilar faoliyatining hisobdorligini ta'minlash (audit).
- Ma'lumotlar bazasidagi asosiy ma'lumotlarni himoyalash (shifrlash).

DOI: 10.65322/j.srd.05192026.108

Oracle Database tizimida ma’lumotlar bazasi foydalanuvchisini autentifikatsiya qilish parollardan foydalanish orqali uning kirish vakolatlarini standart tartibda tekshirishni anglatadi [2].

MySQL tizimi, odatda, imkon qadar yuqori tezlikda ishlashga mo‘ljallangan. Shu sababli unda ma’lumotlar bazasi jadvallarini shifrlashning o‘rnatilgan mexanizmi mavjud emas. Biroq MySQL shifrlangan SSL ulanishlarini qo‘llab-quvvatlaydi. Bu mijoz va server o‘rtasida ma’lumotlarni uzatish jarayonida begona shaxslarning ushbu ma’lumotlar bilan tanishib chiqishi xavfini kamaytirish uchun zarur.

SSL protokolida umumiy foydalanishdagi tarmoqlar orqali uzatiladigan ma’lumotlar xavfsizligini ta’minlashga xizmat qiluvchi turli shifrlash algoritmlaridan foydalaniladi. Mazkur protokol ma’lumotlarning o‘zgartirilishi, yo‘qotilishi va takroran uzatilishi kabi holatlarni aniqlash imkonini beruvchi vositalarni ham o‘z ichiga oladi.

MySQL tizimida foydalanuvchini identifikatsiya qilish uchun login va paroldan foydalaniladi. Ushbu tizimning ijobiy jihati shundaki, parol shifrlangan ko‘rinishda saqlanadi va uni dastlabki holatiga qaytarish imkoniyati nazarda tutilmagan. Shu sababli, hatto buzg‘unchi shifrlangan parolni qo‘lga kiritgan taqdirda ham, undan bevosita foydalanish imkoniyati cheklanadi.

Tizimning kamchiliklaridan biri parollarga nisbatan majburiy xavfsizlik siyosatining mavjud emasligidir. Ya’ni, foydalanuvchi o‘z parolining murakkablik darajasini mustaqil belgilaydi. Masalan, “1111” kabi sodda parollardan foydalanish axborot xavfsizligi talablariga javob bermaydi.

MySQL tizimida foydalanuvchini avtorizatsiya qilish imtiyozlar tizimi orqali amalga oshiriladi. Muayyan amalni bajarish uchun foydalanuvchi aynan shu amalni bajarish huquqiga ega bo‘lishi kerak.

Mazkur tizimning afzalligi imtiyozlarning turli darajalarga ajratilganligidir. Kamchiligi esa MBBT uchun mo‘ljallangan boshqa xavfsizlik tizimlariga nisbatan imtiyozlarni boshqarish mexanizmining soddalashtirilganligidir.

MySQL tizimida audit mexanizmi hisobga olish jurnallari orqali amalga oshiriladi. Biroq ushbu mexanizm ham nisbatan soddalashtirilgan shaklda tashkil etilgan.

MySQL tizimida ma’lumotlar bazasi jadvallarini yoki butun ma’lumotlar bazasini shifrlash uchun o‘rnatilgan mexanizm mavjud emas. Shu bilan birga, mijoz va server o‘rtasida ma’lumotlarni himoyalangan holda uzatish uchun shifrlangan SSL ulanishlaridan foydalanish imkoniyati mavjud.

Shunday qilib, MySQL tizimida ma’lumotlar bazasini himoyalashning barcha asosiy usullari amalga oshirilgan, biroq ular nisbatan soddalashtirilgan shaklda taqdim etilgan, degan xulosaga kelish mumkin.

Microsoft SQL Server tizimida ma’lumotlar bazalarini himoyalashning barcha asosiy usullari mavjud.

Ma’lumotlar bazasida foydalanuvchi yaratish jarayonida shaxsning haqiqiyligini tekshirish mexanizmlarini ma’lumotlar bazasi va operatsion tizim darajalarida sozlash mumkin.

Microsoft SQL Server tizimida avtorizatsiyani amalga oshirish uchun ruxsatlar va rollar mexanizmlaridan foydalaniladi. Foydalanuvchilarning harakatlarini tekshirish maqsadida avtomatlashtirilgan audit tizimi joriy etilgan. Bundan tashqari, Microsoft SQL Server tizimida fayllarni, ustunlarni, ma’lumotlarni va kalitlarni shifrlashni o‘z ichiga olgan, turli darajalarda ishlovchi ma’lumotlarni shifrlash mexanizmlari mavjud.

SQL Server resurslaridan foydalanish uchun so‘rov yuborishi mumkin bo‘lgan barcha subyektlar *ishtirokchilar* deb ataladi. Ishtirokchilar turli ta’sir doiralariga ega bo‘lib, ular muayyan ierarxik tartibda joylashadi:

- Windows darajasidagi ishtirokchi.

DOI: 10.65322/j.srd.05192026.108

➢ SQL Server darajasidagi ishtirokchi. Standart holatda administratorning tizimga kirish nomi “sa” hisoblanadi.

➢ Ma’lumotlar bazasi darajasidagi ishtirokchi – ma’lumotlar bazasi foydalanuvchisi.

Har bir ishtirokchi SQL Server tizimiga ulanayotgan foydalanuvchi yoki jarayonni identifikatsiya qilish uchun xizmat qiladigan muayyan kirish nomiga ega [3].

Microsoft SQL Server tizimini o‘rnatish jarayonida autentifikatsiya rejimini tanlash va uni tegishli tarzda sozlash talab etiladi.

Windows va SQL Server autentifikatsiyasini birgalikda qo‘llashni nazarda tutuvchi aralash autentifikatsiya rejimida “sa” hisob qaydnomasi uchun ishonchli parol o‘rnatilishi va ushbu parol tasdiqlanishi lozim.

Windows autentifikatsiyasi foydalanuvchining nomi va parolini Windows ishtirokchisining xavfsizlik tokeni yordamida tekshiradi. Ushbu usul SQL Server autentifikatsiyasiga nisbatan yuqoriroq xavfsizlik darajasini ta’minlaydi. Shuningdek, u operatsion tizimning parollar siyosatini, jumladan, ishonchli parollarning murakkablik talablarini tekshirish mexanizmlarini qo‘llash imkonini beradi.

SQL Server autentifikatsiyasidan foydalanilganda, SQL Server tizimida Windows foydalanuvchilarining hisob qaydnomalariga asoslanmagan kirish nomlari yaratiladi. Bunda foydalanuvchining nomi va paroli SQL Server tizimida saqlanadi.

Mazkur autentifikatsiya usuli parollar siyosatidan foydalanish imkonini beradi. Ushbu siyosatni ALTER LOGIN buyrug‘ini bajarish orqali faollashtirish mumkin.

Xulosa. Yuqorida bayon etilgan fikrlardan quyidagi xulosalarga kelish mumkin:

1. DB-Engines resursida keltirilgan tadqiqot ma’lumotlariga ko‘ra, dunyoda eng keng tarqalgan ma’lumotlar bazasini boshqarish tizimlari Oracle Database, MySQL va Microsoft SQL Server hisoblanadi. Shu sababli mazkur ishda ushbu tizimlarni o‘rganishga asosiy e’tibor qaratilgan.

2. Ma’lumotlar bazalarini himoyalash usullari orasidan to‘rtta asosiy mexanizm ajratib ko‘rsatilgan. Bular autentifikatsiya, avtorizatsiya, ma’lumotlar bazasi auditi va ma’lumotlarni shifrlash usullaridir.

3. Ma’lumotlar bazasini boshqarish tizimlarida qo‘llaniladigan himoya usullarining asosiy afzalliklari va kamchiliklari tahlil qilingan. Ushbu tahlil mavjud himoya mexanizmlarining kamchiliklarini bartaraf etish bo‘yicha tavsiyalar ishlab chiqish hamda ma’lumotlar bazalarida saqlanadigan axborotning himoyalanganlik darajasini oshirish imkonini beradi.

Foydalanilgan adabiyotlar

1. Date, C. J. *An Introduction to Database Systems*. 8-nashr. Moskva: «Вильямс» nashriyot uyi, 2005. – 1328 b.

2. Alapati, S. R. *Oracle Database 11g: Руководство администратора баз данных*. Moskva: «Вильямс» nashriyot uyi, 2005. – 1440 b.

3. Kirillov, V. V. *Введение в реляционные базы данных*. Sankt-Peterburg: БХВ-Петербург, 2009. – 464 b.