MA’LUMOTLAR BAZASINI BOSHQARISH TIZIMLARIDA (MBBT) KIBERXAVFSIZLIKNI TA’MINLASHNING ZAMONAVIY USULLARI

Mo’minova Madina Muxiddinovna
Andijon davlat pedagogika instituti
Matematika va informatika kafedrasi o’qituvchisi,
O‘ktamjonova Shirinoy Baxodirjon qizi
Andijon davlat pedagogika instituti
Matematika va informatika yo‘nalishi talabasi

Anotatsiya. *Ushbu maqolada ma’lumotlar bazasini boshqarish tizimlarida (MBBT) kiberxavfsizlikni ta’minlashning zamonaviy usullari tahlil qilinadi. Autentifikatsiya, avtorizatsiya, shifrlash, audit, monitoring va sun’iy intellekt asosidagi himoya texnologiyalarining ishlash prinsiplari yoritilgan. Shuningdek, SQL Injection kabi tahdidlar va ulardan himoyalanish usullari ko‘rib chiqilgan. Tadqiqot natijalari MBBT xavfsizligini ta’minlashda kompleks yondashuv muhimligini ko‘rsatadi.*

Kalit so‘zlar: *Ma’lumotlar bazasi, kiberxavfsizlik, MBBT, shifrlash, autentifikatsiya, avtorizatsiya, SQL Injection, audit, monitoring, sun’iy intellekt.*

Аннотация. *В данной статье анализируются современные методы обеспечения кибербезопасности в системах управления базами данных (СУБД). Рассматриваются принципы работы аутентификации, авторизации, шифрования, аудита, мониторинга и технологий защиты на основе искусственного интеллекта. Также изучаются угрозы, такие*

как SQL Injection, и методы их предотвращения. Результаты исследования показывают важность комплексного подхода к обеспечению безопасности СУБД.

Ключевые слова: *База данных, кибербезопасность, СУБД, шифрование, аутентификация, авторизация, SQL Injection, аудит, мониторинг, искусственный интеллект.*

Abstract. *This article analyzes modern methods of ensuring cybersecurity in database management systems (DBMS). It covers the principles of authentication, authorization, encryption, auditing, monitoring, and artificial intelligence-based security technologies. Threats such as SQL Injection and their prevention methods are also discussed. The results show that a comprehensive approach is essential for ensuring DBMS security.*

Keywords: *Database, cybersecurity, DBMS, encryption, authentication, authorization, SQL Injection, audit, monitoring, artificial intelligence.*

Kirish. Hozirgi kunda axborot texnologiyalarining jadal rivojlanishi natijasida ma’lumotlar hajmi keskin ortib bormoqda. Davlat tashkilotlari, bank tizimlari, ta’lim muassasalari, sog‘liqni saqlash, elektron tijorat va ijtimoiy tarmoqlarda katta hajmdagi ma’lumotlar ma’lumotlar bazalarida saqlanadi. Ushbu ma’lumotlarning xavfsizligi, maxfiyligi va yaxlitligini ta’minlash zamonaviy axborot tizimlarining eng muhim vazifalaridan biri hisoblanadi. Shu sababli ma’lumotlar bazasini boshqarish tizimlarida (MBBT) kiberxavfsizlik masalasi dolzarb ahamiyat kasb etmoqda.

Internet texnologiyalarining keng rivojlanishi bilan bir qatorda turli xil kiberhujumlar, zararli dasturlar, ma’lumotlarni o‘g‘irlash, SQL Injection, phishing va ruxsatsiz kirish kabi tahdidlar soni ham ortib bormoqda. Ayniqsa,

bulutli texnologiyalar va taqsimlangan tizimlarning rivojlanishi ma’lumotlar xavfsizligini ta’minlashni yanada murakkablashtirmoqda. Natijada tashkilotlar o‘z ma’lumotlarini himoyalash uchun zamonaviy xavfsizlik mexanizmlaridan foydalanishga majbur bo‘lmoqda. MBBTda kiberxavfsizlikni ta’minlash uchun autentifikatsiya, avtorizatsiya, ma’lumotlarni shifrlash, audit va monitoring, zaxiralash tizimlari hamda sun’iy intellekt asosidagi xavfsizlik texnologiyalari keng qo‘llanilmoqda. Ushbu usullar ma’lumotlarni ruxsatsiz foydalanishdan himoya qilish, tizimdagi xavfsizlik zaifliklarini aniqlash va kiberhujumlarning oldini olishda muhim rol o‘ynaydi.

Natija va muhokama. Tadqiqot natijalari shuni ko‘rsatdiki, ma’lumotlar bazasini boshqarish tizimlarida kiberxavfsizlikni ta’minlash zamonaviy axborot tizimlarining barqaror ishlashi uchun muhim omillardan biridir. Tahlillar davomida autentifikatsiya, avtorizatsiya, ma’lumotlarni shifrlash, audit va monitoring, zaxiralash hamda sun’iy intellekt asosidagi himoya texnologiyalarining samaradorligi o‘rganildi.

Natijalarga ko‘ra, autentifikatsiya va avtorizatsiya tizimlari foydalanuvchilarni identifikatsiya qilish va ularga tegishli ruxsat darajalarini belgilash orqali ruxsatsiz kirishlarning oldini olishda muhim rol o‘ynaydi. Ayniqsa, ikki bosqichli autentifikatsiya va biometrik tekshiruvlardan foydalanish xavfsizlik darajasini sezilarli oshiradi. Shu bilan birga, ma’lumotlarni shifrlash texnologiyalari maxfiy axborotlarni himoyalashning eng samarali usullaridan biri ekanligi aniqlandi. AES, RSA va SHA algoritmlaridan foydalanish ma’lumotlarning noqonuniy o‘qilishi va o‘zgartirilishiga qarshi kuchli himoya yaratadi. Tahlillar davomida SQL Injection hujumlari MBBT uchun eng xavfli tahdidlardan biri ekanligi kuzatildi. Prepared Statements, input validation va ORM texnologiyalaridan

foydalanish bunday hujumlarning oldini olishda samarali vosita hisoblanadi. Bundan tashqari, audit va monitoring tizimlari foydalanuvchilar faoliyatini nazorat qilish hamda tizimdagi shubhali harakatlarni real vaqt rejimida aniqlash imkonini beradi.

Bulutli texnologiyalar asosidagi ma’lumotlar bazalarida esa xavfsizlikni ta’minlash yanada murakkab ekani ma’lum bo‘ldi. Chunki ma’lumotlar internet orqali uzatilishi sababli turli xil tashqi tahdidlar xavfi ortadi. Shu sababli VPN, Firewall, Zero Trust modeli va Multi-factor Authentication kabi zamonaviy himoya vositalaridan foydalanish muhim ahamiyatga ega.

Muhokamalar natijasida ma’lum bo‘ldiki, faqat bitta xavfsizlik mexanizmi barcha tahdidlardan to‘liq himoya qila olmaydi. Eng samarali yondashuv — bu ko‘p bosqichli xavfsizlik tizimini yaratishdir. Bunda autentifikatsiya, shifrlash, monitoring, zaxiralash va sun’iy intellekt asosidagi texnologiyalar birgalikda qo‘llaniladi. Bundan tashqari, inson omili ham kiberxavfsizlikda muhim rol o‘ynaydi. Kuchsiz parollar, noto‘g‘ri sozlamalar va foydalanuvchilarning ehtiyotsizligi ko‘plab xavfsizlik muammolariga sabab bo‘lishi mumkin.

SQL Injection’dan himoyalanish

SQL Injection — eng xavfli kiberhujumlardan biri hisoblanadi.

Himoyalanish usullari

- Prepared Statements ishlatish
- Input validation
- ORM texnologiyalaridan foydalanish
- Minimal huquq berish prinsipi

Misol

-- Xavfli so‘rov

SELECT * FROM users WHERE login = '$user';

-- Xavfsiz usul

SELECT * FROM users WHERE login = ?;

Ma’lumotlarni shifrlash

Shifrlash ma’lumotlarni maxsus algoritmlar yordamida kodlash orqali himoya qiladi.

Shifrlash turlari

Tur	**Tavsif**
Symmetric Encryption	Bir xil kalit bilan shifrlash
Asymmetric Encryption	Ochiq va yopiq kalitlardan foydalanish
Hashing	Ma’lumotni qayta tiklab bo‘lmaydigan ko‘rinishga o‘tkazish

Xulosa. Ma’lumotlar bazasini boshqarish tizimlarida (MBBT) kiberxavfsizlikni ta’minlash zamonaviy axborot texnologiyalarining eng dolzarb yo‘nalishlaridan biri hisoblanadi. Raqamli texnologiyalar va internet xizmatlarining keng rivojlanishi natijasida ma’lumotlar hajmi ortib borayotgani bilan bir qatorda, kiberhujumlar va axborot xavfsizligiga tahdidlar soni ham ko‘paymoqda. Shu sababli ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini himoya qilish muhim vazifaga aylangan.

Tadqiqot davomida autentifikatsiya, avtorizatsiya, ma’lumotlarni shifrlash, audit va monitoring, zaxiralash tizimlari hamda sun’iy intellekt asosidagi xavfsizlik texnologiyalarining MBBT xavfsizligini ta’minlashdagi ahamiyati tahlil qilindi. Natijalar shuni ko‘rsatdiki, zamonaviy himoya usullaridan kompleks foydalanish ma’lumotlarni ruxsatsiz kirish, o‘zgartirish va yo‘qotishdan samarali himoya qiladi. Ayniqsa, AES va RSA kabi shifrlash algoritmlari, ikki bosqichli autentifikatsiya hamda real vaqt monitoring tizimlari xavfsizlik darajasini sezilarli oshiradi.

Shuningdek, SQL Injection, zararli dasturlar va tarmoq hujumlari kabi tahdidlar MBBT uchun asosiy xavflardan biri ekanligi aniqlandi. Bunday hujumlarning oldini olishda Prepared Statements, Firewall, VPN va Zero Trust kabi texnologiyalar muhim rol o‘ynaydi. Bulutli tizimlarning rivojlanishi esa kiberxavfsizlikka bo‘lgan talabni yanada oshirmoqda.

FOYDALANILGAN ADABIYOTLAR

1. Microsoft Access 2019 Step by Step — Joan Lambert, Curtis Frye. Microsoft Press, 2019.
2. Database System Concepts — Abraham Silberschatz, Henry F. Korth, S. Sudarshan. McGraw-Hill Education, 2019.
3. Fundamentals of Database Systems — Ramez Elmasri, Shamkant Navathe. Pearson Education, 2016.
4. Microsoft Office Access 2007 Bible — Cary N. Prague, Michael R. Irwin. Wiley Publishing, 2007.
5. Microsoft Access rasmiy sahifasi
6. Microsoft Learn platformasi
7. Axborot texnologiyalari — O‘quv qo‘llanma, Toshkent, 2020.
8. Ma’lumotlar bazasi — Oliy ta’lim uchun darslik, Toshkent, 2019.