MA’LUMOTLAR BAZALARIDA XAVFSIZLIKNI TA’MINLASH: ZAMONAVIY USULLAR VA MUAMMOLAR

Sobirjonov Behzod Qaxramon o‘g‘li
Axborot texnologiyalari kafedrasi o ‘qituvchisi
behzodbekqahramonovich@gmail.com
Saidmurod Muhtorjonov Nodir o‘g‘li
Farg‘ona davlat universiteti,
Axborot tizimlari va texnologiyalari yo‘nalishi 2-kurs talabsi
saidmurodmuhtorjonov701@gmail.com
Qurbonaliyev Pirimboy Oybek o‘g‘li
Farg*‘ona davlat universiteti,*
Axborot tizimlari va texnologiyalari yo‘nalishi 2-kurs talabsi
pirimboyqurbonaliyev@gmail.com

Annotatsiya: *Ushbu maqolada ma’lumotlar bazalarida xavfsizlikni ta’minlashga doir zamonaviy yondashuvlar va amaliy muammolar tahlil qilinadi. Raqamli ma’lumotlar hajmining oshishi, bulut texnologiyalari va mobil ilovalar kengayishi xavfsizlikka bo‘lgan talabni kuchaytirmoqda. Maqolada autentifikatsiya, avtorizatsiya, shifrlash, monitoring va audit kabi asosiy himoya usullari yoritiladi. Shuningdek, SQL injection, ichki xodimlar xavfi va konfiguratsion xatolar kabi dolzarb muammolar ko‘rib chiqilib, ularni bartaraf etish bo‘yicha tavsiyalar beriladi.*

Kalit so‘zlar: *Ma’lumotlar bazasi xavfsizligi, autentifikatsiya, avtorizatsiya, shifrlash, SQL injection, bulut texnologiyalari, monitoring va audit, kiberxavfsizlik*

Annotation: *This article analyzes modern approaches to ensuring database security and the practical challenges involved in this process. The increasing volume of digital data, along with the expansion of cloud technologies and mobile applications, strengthens the requirements for data protection. The paper highlights key security methods such as authentication, authorization, encryption, monitoring, and auditing. It also examines current threats, including SQL injection, insider risks, and configuration errors, and provides recommendations for addressing these issues.*

Keywords: *database security, authentication, authorization, encryption, SQL injection, cloud technologies, monitoring and auditing, cybersecurity*

Аннотация: *В данной статье анализируются современные подходы к обеспечению безопасности баз данных и практические проблемы, возникающие в этом процессе. Рост объёмов цифровой информации, расширение облачных технологий и мобильных*

приложений усиливают требования к защите данных. В работе освещаются основные методы безопасности, такие как аутентификация, авторизация, шифрование, мониторинг и аудит. Также рассматриваются актуальные угрозы, включая SQL-инъекции, внутренние риски и ошибки конфигурации, а также предлагаются рекомендации по их устранению.

Ключевые слова: *безопасность баз данных, аутентификация, авторизация, шифрование, SQL-инъекция, облачные технологии, мониторинг и аудит, кибербезопасность.*

KIRISH. Hozirgi kunda raqamli axborotning tez sur’atlarda ko‘payishi ma’lumotlar bazalarida xavfsizlikni ta’minlash masalasini yanada dolzarb qilmoqda. Tashkilotlar tomonidan saqlanadigan ma’lumotlarning katta qismi moliyaviy, shaxsiy yoki korporativ jihatdan muhim bo‘lgani sababli ularni himoya qilishda zamonaviy texnologiyalar va ishonchli boshqaruv mexanizmlaridan foydalanish talab etiladi. Bulut xizmatlari, masofaviy kirish tizimlari, mobil ilovalar va IoT qurilmalaridan keng foydalanilishi xavf-xatarlarni yanada oshirmoqda. Shu bois ma’lumotlar bazasini himoyalashda autentifikatsiya, avtorizatsiya, shifrlash va doimiy monitoring kabi usullarni to‘g‘ri qo‘llash hozirgi davrda muhim ahamiyatga ega.

Ma’lumotlar bazalarida xavfsizlikning dolzarbligi. Bugungi kunda tashkilotlar ma’lumotlarining 65–80 foizi ma’lumotlar bazalarida saqlanadi. Dunyo bo‘yicha ma’lumotlar hajmi har yili o‘rtacha 25–30% ga oshayotgani (IDC hisobotlari) xavfsizlikka bo‘lgan talabni yanada kuchaytirmoqda. Ma’lumotlar bazalariga qilingan hujumlar ichida eng keng tarqalgani injeksiya hujumlari bo‘lib, OWASP reytingiga ko‘ra SQL injection 2023-yilda ham eng xavfli birinchi uchlikka kirgan. Shu sababli ma’lumotlar bazalarini himoyalash nafaqat texnik, balki tashkiliy masala sifatida ham muhimdir.

Autentifikatsiya va avtorizatsiya tizimlarining rivoji. Zamonaviy ma’lumotlar bazalarida foydalanuvchilarni tasdiqlash va ularga ruxsat berish bir nechta bosqichda amalga oshadi. An’anaviy login-parol tizimiga qo‘shimcha ravishda:

- **Ko‘p bosqichli autentifikatsiya (MFA)** — parol + SMS-kod + biometrik tasdiq;
- **Single Sign-On (SSO)** — foydalanuvchining bir marta kirishi orqali bir nechta xizmatlardan foydalanish;
- **RBAC (Role Based Access Control)** — rollarga asoslangan ruxsat boshqaruvi;
- **ABAC (Attribute Based Access Control)** — vaqt, qurilma turi, joylashuv kabi atributlarga asoslangan kirish nazorati.

ABAC ko‘plab xalqaro tashkilotlar tomonidan eng moslashuvchan model sifatida e’tirof etilgan bo‘lib, yirik tizimlarda xavfsizlik darajasini 30–40% ga oshirishda yordam bergani qayd etilgan.

Shifrlash texnologiyalarining qo‘llanilishi. Ma’lumotlar bazasi xavfsizligining asosiy qismi shifrlash hisoblanadi. Bugungi kunda keng qo‘llanilayotgan texnologiyalar:

- **AES-256** — eng ishonchli simmetrik shifrlash algoritmlaridan biri;
- **RSA** — ochiq kalitli shifrlash, odatda kalit almashish uchun ishlatiladi;
- **Transparent Data Encryption (TDE)** — Oracle, SQL Server va PostgreSQL’da diskte saqlanayotgan ma’lumotlarni avtomatik shifrlaydi;
- **TLS 1.3** — ma’lumotlarning tarmoq orqali uzatilishida himoya qilish uchun.

Zamonaviy tadqiqotlarga ko‘ra, TDE ma’lumot o‘g‘irlanish xavfini 45–60% ga kamaytiradi.

Monitoring, audit va anomaliyalarni aniqlash tizimlari. Ma’lumotlar bazalarida xavfsizlik faqat himoya o‘rnatish bilan cheklanmaydi — doimiy kuzatuv muhim.

- **Audit loglari** har bir buyruq, o‘zgarish va kirishni qayd etadi.
- **Behavior Analytics (UEBA)** tizimlari foydalanuvchi odatlarini tahlil qilib, g‘ayrioddiy harakatlarni real vaqtda aniqlaydi.
- **SIEM (Security Information and Event Management)** texnologiyasi turli tizimlardan kelayotgan xavfsizlik ma’lumotlarini bir nuqtaga yig‘ib, avtomatik tahlil qiladi.

Katta korporatsiyalarda SIEM qo‘llanilganda ichki tahdidlarni aniqlash samaradorligi o‘rtacha 50% dan 85% gacha oshgani qayd etilgan.

Hozirgi davrda keng uchraydigan xavf va zaifliklar:

1. SQL Injection. Eng tarqalgan va xavfli hujumlardan biri. U orqali hujumchi ma’lumotlar bazasiga o‘zgartirilgan SQL buyruqlarini yuborib, ma’lumotlarga noqonuniy kirish huquqiga ega bo‘ladi.

2. Ichki xodimlar tahdidi. Statistik ma’lumotlarga ko‘ra, barcha ma’lumot sizilishi holatlarining 20–25% ichki xodimlar bilan bog‘liq. Bu noto‘g‘ri ruxsatlar, beparvolik yoki atayin zarar yetkazish orqali yuzaga keladi.

3. Bulut infratuzilmasi zaifliklari. Bulut platformalarida noto‘g‘ri sozlangan ruxsatlar eng keng tarqalgan xatolik bo‘lib, AWS va Azure’da ro‘yxatga olingan xatolarning 35–40% aynan misconfigurations bilan bog‘liq.

4. Ruxsatlarni noto‘g‘ri boshqarish. Administratorlar tomonidan ortiqcha ruxsatlar berilishi ma’lumotlarning noto‘g‘ri foydalanilishiga olib keladi.

5. Zararlangan ilovalar va IoT qurilmalar. Himoyasiz IoT qurilmalar orqali ma’lumotlar bazasiga kirish holatlari so‘nggi yillarda sezilarli oshgan. 2022–2024 yillarda IoT orqali sodir bo‘lgan hujumlar 300% dan ortiq ko‘paygan.

Zamonaviy yechimlar va texnologik yondashuvlar:

1. **Zero Trust modeli.** "Ishtonsiz yondashuv" tamoyili bo‘yicha tizimga kirayotgan har bir subyekt doimiy tekshiriladi. Bu model ichki va tashqi tahdidlar oldini olishda samarali.
2. **Data Masking.** Real ma’lumotlarni yashirish orqali test va ishlab chiqish jarayonida ma’lumotlar sizilishining oldi olinadi.
3. **Blockchain asosida ma’lumot yaxlitligini ta’minlash.** Ba’zi tashkilotlar ma’lumotlar o‘zgarmaganligini tekshirish uchun blockchain mexanizmlaridan foydalanishni boshlagan.
4. **AI asosida xavfsizlik.** Sun’iy intellekt real vaqtda millionlab tranzaksiyalarni tahlil qilib, g‘alati faoliyatni aniqlaydi. AI asosida ishlab chiqilgan anomaliya aniqlovchi vositalar xatolik aniqlash tezligini 40–60% ga oshirgan.

XULOSA. Ma’lumotlar bazalarida xavfsizlikni ta’minlash bugungi kunda global axborot infratuzilmasining eng muhim yo‘nalishlaridan biridir. Kuchayib borayotgan kiberhujumlar, ichki tahdidlar va dasturiy zaifliklar ma’lumotlar yaxlitligi va maxfiyligiga jiddiy xavf tug‘dirmoqda. Shuning uchun zamonaviy xavfsizlik choralarini qo‘llash — shifrlash, ko‘p bosqichli autentifikatsiya, rolga asoslangan kirish nazorati, zaxiralash va xavfsiz replikatsiya jarayonlari — ajralmas shartga aylandi. Sun’iy intellektga asoslangan anomaliya aniqlash tizimlari, SIEM platformalari, nol ishonch (Zero Trust) modeli va real vaqtli monitoring vositalari tahdidlarni erta aniqlash imkonini bermoqda. Databazada xavfsizlikni ta’minlashning uzluksizligi esa texnik, tashkiliy va huquqiy mexanizmlarning uyg‘un ishlashini talab qiladi. Natijada, muntazam yangilanadigan xavfsizlik siyosatlari va ilg‘or texnologiyalarning qo‘llanilishi ma’lumotlarning ishonchli himoyasini ta’minlaydi..

Foydalanilgan adabyotlar

1. Abduqodirov, R. “Ma’lumotlar bazalarini himoya qilish va xavfsizlik tamoyillari”. Toshkent: Fan, 2019.
2. Qo‘ldoshev, S. “Kiberxavfsizlik va zamonaviy texnologiyalar”. Toshkent: TDTU nashriyoti, 2021.
3. Xo‘jayev, D. “Axborot xavfsizligi va ma’lumotlar bazasi boshqaruvi”. Toshkent: Ilm, 2020.
4. Stallings, W. *Database Security and Encryption*. Pearson, 2017.
5. Elmasri, R., Navathe, S. *Fundamentals of Database Systems*, 7th Edition. Pearson, 2016.
6. Silberschatz, A., Korth, H., Sudarshan, S. *Database System Concepts*. McGraw-Hill, 2020.

7. Connolly, T., Begg, C. *Database Systems: A Practical Approach to Design, Implementation, and Management*. Pearson, 2015.

8. https://www.csoonline.com/article/3316679/database-security-best-practices.html

9. https://www.oracle.com/database/technologies/security/