AXBOROT TIZIMLARI XAVFSIZLIGI MODELLARI: ROLLANIB BOSHQARILADIGAN KIRISH NAZORATI (RBAC) VA UNING SPETSIFIKATSIYALARI

Shokirova Gulnoza
University of Business and Science talabasi
Mirsaidov Ibroximbek Tolib o‘g‘li
University Business of science universiteti, innovatsion texnologiyalar kafedrasi katta o‘qituvchisi
E-mail: Samsungd-820@mail.ru

*DOI: **https://doi.org/10.5281/zenodo.19828057***

Annotatsiya: *Ushbu maqolada axborot tizimlari xavfsizligini ta’minlashda rollarga asoslangan kirish nazorati (RBAC) modelining o‘rni, uning ishlash tamoyillari va o‘ziga xos spetsifikatsiyalari yoritiladi. Ma’lumotlar maxfiyligini saqlashda foydalanuvchi huquqlarini rollar orqali boshqarishning samaradorligi, tizim barqarorligiga ta’siri va zamonaviy axborot texnologiyalarida qo‘llanilishi tahlil qilinadi. Natijada, RBAC modelining boshqa kirish modellaridan afzalliklari va xavfsizlik siyosatini avtomatlashtirishdagi ahamiyati asoslab beriladi.*

Kalit so‘zlar*: Axborot tizimlari xavfsizligi, RBAC, rollarga asoslangan kirish nazorati, foydalanuvchi huquqlari, ruxsatnomalar, kiberxavfsizlik, axborot xavfsizligi, kirish nazorati, eng kam imtiyoz tamoyili, xavfsizlik siyosati.*

Annotatsiya: *This article highlights the role, operational principles, and specific specifications of Role-Based Access Control (RBAC) in ensuring information systems security. The effectiveness of managing user rights through roles in maintaining data confidentiality, its impact on system stability, and its application in modern information technologies are analyzed. As a result, the advantages of the RBAC model over other access models and its importance in automating security policies are substantiated.*

Keywords: *Information systems security, RBAC, Role-Based Access Control, user permissions, authorization, cybersecurity, information security, access control, least privilege principle, security policy.*

KIRISH. Bugungi kunda raqamli transformatsiya jarayonida axborot xavfsizligini ta’minlash eng dolzarb masalalardan biriga aylandi. Katta hajmdagi ma’lumotlar bazalari bilan ishlashda

foydalanuvchilarning tizim resurslaridan foydalanish huquqlarini to‘g‘ri taqsimlash kiberxavfsizlikning asosi hisoblanadi. An’anaviy usullar ko‘p foydalanuvchili tizimlarda murakkablik tug‘dirishi sababli, zamonaviy axborot tizimlarida rollarga asoslangan kirish nazorati (RBAC) modellaridan foydalanish yuqori samara bermoqda.

ASOSIY QISM. RBAC (Role-Based Access Control) – bu foydalanuvchilarga tizim resurslariga kirish huquqini bevosita emas, balki ularga biriktirilgan rollar orqali berish usulidir. Bu modelning asosiy tarkibiy qismlari quyidagilardan iborat:

Foydalanuvchilar (Users): Tizimda ishlovchi sub’ektlar.

Rollar (Roles): Muayyan lavozim yoki vazifaga mos keladigan huquqlar to‘plami (masalan: administrator, o‘qituvchi, talaba).

Ruxsatnomalar (Permissions): Muayyan ob’ekt ustida bajarilishi mumkin bo‘lgan amallar (o‘qish, yozish, o‘chirish).

Spetsifikatsiyalar va afzalliklar:

RBAC modeli spetsifikatsiyasiga ko‘ra, foydalanuvchi bir nechta rolga ega bo‘lishi mumkin, ammo uning huquqlari faqat o‘sha paytdagi faol roli bilan cheklanadi. Bu "eng kam imtiyoz" (Least Privilege) tamoyilini amalga oshirishga yordam beradi. Tizimda ierarxik rollar tuzilishi mumkin, ya’ni yuqori darajadagi rol (masalan, direktor) quyi darajadagi rolning (masalan, xodim) barcha huquqlarini o‘z ichiga oladi.

XULOSA. Axborot tizimlarida RBAC modelini joriy etish boshqaruvni soddalashtiradi va inson omili bilan bog‘liq xavfsizlik xatolarini kamaytiradi. Spetsifikatsiyalarning to‘g‘ri belgilanishi tizim ichidagi ma’lumotlar sizib chiqishining oldini oladi va kirish nazoratini toza hamda shaffof tashkil etish imkonini beradi.

Foydalanilgan adabiyotlar:

1. Gulyamov, S. S. Axborot xavfsizligi tizimlari. – Toshkent: Fan va texnologiya, 2022.
2. Sandhu, R., et al. "Role-Based Access Control Models". IEEE Computer, 2021.
3. O‘zbekiston Respublikasining "Kiberxavfsizlik to‘g‘risida"gi Qonuni, 2022.