JOURNAL OF INTERNATIONAL SCIENTIFIC RESEARCH
Volume 3, Issue 7, December 2025 Online ISSN: 3030-3508
https://spaceknowladge.com

FOYDALANISHLARNI BOSHQARISHNING AXBOROT XAVFSIZLIGINI TA'MINLASHDAGI DAC, MAC, RBAC, ABAC MODELLARINING REALIZATSIYA JARAYONLARI TAHLILI

Munavarjonov Shohzod Zohidjon o‘g‘li
Farg’ona davlat texnika universiteti
Axborot xavfsizligi yo’nalishi 4-bosqich talabasi
Sadirova Xursanoy Xusanboy qizi
Farg‘ona davlat texnika universiteti “Dasturiy injiniring va kiberxavfsizlik” kafedrasi assistenti
E-mail: sadirovaxursanoy@gmail.com

MAQOLA MALUMOTI

MAQOLA TARIXI:

Received:26.12.2025
Revised: 27.12.2025
Accepted:28.12.2025

KALIT SO’ZLAR:

IDS, IPS, axborot xavfsizligi, kiberhujumlar, tarmoq xavfsizligi, siyosiy ahamiyat, texnik yechimlar, xavfsizlik monitoring. Axborot xavfsizligi, Access Control, DAC, MAC, RBAC, ABAC, autentifikatsiya, avtorizatsiya

ANNOTATSIYA:

Ushbu maqolada axborot xavfsizligini ta’minlashda foydalanishlarni boshqarish (Access Control) modellarining o‘rni va ahamiyati tahlil qilinadi. Xususan, diskretsion foydalanishlarni boshqarish (DAC), majburiy foydalanishlarni boshqarish (MAC), rollarga asoslangan foydalanishlarni boshqarish (RBAC) hamda atributlarga asoslangan foydalanishlarni boshqarish (ABAC) modellarining realizatsiya jarayonlari, afzalliklari va kamchiliklari ko‘rib chiqiladi. Har bir modelning amaliy qo‘llanilishi va zamonaviy axborot tizimlarida tutgan o‘rni solishtirma tahlil asosida yoritiladi.

Zamonaviy tashkilotlar uchun axborot resurslarini himoya qilish tobora murakkablashmoqda. Internet va korporativ tarmoqlarga bo‘lgan kirish imkoniyati ortib, kiberhujumlar soni va murakkabligi keskin oshdi. Shu sababli, tashkilotlarda nafaqat xavfsizlik siyosati ishlab chiqish, balki uni amalda qo‘llash va nazorat qilish tizimlari ham

muhim ahamiyat kasb etadi. IDS va IPS tizimlari tashkilot infratuzilmasining ajralmas qismi hisoblanadi. IDS tizimlari tahdidlarni aniqlashga, IPS tizimlari esa ularni bloklash va oldini olishga xizmat qiladi. Bu tizimlar yordamida xodimlarning noto‘g‘ri xatti-harakatlari monitoring qilinadi, tahdidlar real vaqtda aniqlanadi va avtomatik javob mexanizmlari orqali xavfsizlik darajasi oshiriladi. Siyosiy ahamiyati shundaki, IDS/IPS tizimlari xavfsizlik siyosatiga rioya qilishni nazorat qiladi, kiberxavfsizlik bo‘yicha javobgarlikni oshiradi va tashkilotning umumiy xavfsizlik madaniyatini rivojlantiradi. Texnik ahamiyati esa real vaqtda tarmoq monitoringi, log tahlili va tahdidlarni oldini olish bilan namoyon bo‘ladi.

Foydalanishlarni boshqarish (Access Control) axborot xavfsizligini ta’minlashning fundamental mexanizmlaridan biri bo‘lib, axborot resurslariga nisbatan subyektlarning huquqlarini aniqlash, chegaralash va nazorat qilish jarayonini ifodalaydi. Ushbu mexanizm axborot tizimlarida ruxsatsiz murojaatlarning oldini olish, ma’lumotlarning maxfiyligi va yaxlitligini saqlashga xizmat qiladi. Foydalanishlarni boshqarish jarayoni odatda autentifikatsiya va avtorizatsiya bosqichlari orqali amalga oshiriladi. Autentifikatsiya foydalanuvchining shaxsini aniqlashga qaratilgan bo‘lsa, avtorizatsiya unga berilgan huquqlar doirasida axborot resurslaridan foydalanish imkoniyatini belgilaydi. Axborot tizimlarida foydalanishlarni boshqarish mexanizmlarining joriy etilishi ichki va tashqi tahdidlarning oldini olish, foydalanuvchilar faoliyatini monitoring qilish hamda axborot xavfsizligi siyosatini amaliyotga tatbiq etish imkonini beradi. Shu bois, foydalanishlarni boshqarish modellarini to‘g‘ri tanlash va samarali realizatsiya qilish axborot xavfsizligini ta’minlashda muhim ahamiyat kasb etadi.

Axborot xavfsizligini ta’minlashda foydalanishlarni boshqarish modellarining to‘g‘ri tanlanishi va samarali realizatsiya qilinishi muhim ahamiyat kasb etadi. Amaliyotda keng qo‘llaniladigan diskretsion (DAC), majburiy (MAC), rollarga asoslangan (RBAC) va atributlarga asoslangan (ABAC) foydalanishlarni boshqarish modellarining har biri muayyan xavfsizlik talablariga javob beruvchi nazariy va amaliy xususiyatlarga ega.

Diskretsion foydalanishlarni boshqarish (Discretionary Access Control — DAC) modeli tarixan eng dastlabki va sodda yondashuvlardan biri hisoblanadi. Ushbu modelda axborot obyektining egasi unga nisbatan foydalanish huquqlarini mustaqil belgilash vakolatiga ega bo‘lib, resurslar ustidan ruxsatlarni boshqa subyektlarga berish yoki cheklash imkoniyati yaratiladi. DAC modelining nazariy asosi subyektlar va obyektlar o‘rtasidagi munosabatlarni foydalanish matritsasi yoki foydalanishlarni boshqarish ro‘yxatlari (Access

Control List — ACL) orqali ifodalashga asoslanadi. Amaliy jihatdan ushbu model Linux va Windows kabi zamonaviy operatsion tizimlarning fayl tizimlarida keng qo‘llanilib, UNIX-ga o‘xshash tizimlarda “o‘qish”, “yozish” va “bajarish” ruxsatlari orqali realizatsiya qilinadi. DAC modelining asosiy afzalligi uning moslashuvchanligi va boshqaruvning soddaligida namoyon bo‘lsa-da, ruxsatlarning nazoratsiz tarqalishi hamda zararli dasturlar orqali huquqlarning noqonuniy egallanishi ehtimoli ushbu modelning muhim cheklovlari sifatida baholanadi.

Majburiy foydalanishlarni boshqarish (Mandatory Access Control — MAC) modeli esa qat’iy markazlashtirilgan xavfsizlik siyosatiga asoslanadi. Ushbu yondashuvda foydalanuvchilar foydalanish huquqlarini mustaqil o‘zgartirish imkoniyatiga ega emas bo‘lib, barcha ruxsatlar tizim administratorlari tomonidan oldindan belgilanadi. MAC modelining nazariy asosini subyekt va obyektlarga biriktirilgan maxsus xavfsizlik belgilari (security labels) tashkil etadi hamda foydalanish to‘g‘risidagi qarorlar ushbu belgilarning mosligi asosida qabul qilinadi. Mazkur model asosan yuqori darajadagi xavfsizlik talab etiladigan harbiy va davlat axborot tizimlarida qo‘llanilib, SELinux va AppArmor kabi mexanizmlar uning amaliy realizatsiyasiga misol bo‘la oladi. MAC modeli yuqori darajadagi axborot himoyasini ta’minlashi va ichki tahdidlarga nisbatan samaradorligi bilan ajralib tursa-da, moslashuvchanlikning pastligi hamda tizimni sozlash jarayonining murakkabligi uning asosiy kamchiliklari hisoblanadi.

Rollarga asoslangan foydalanishlarni boshqarish (Role-Based Access Control — RBAC) modeli tashkilotning tashkiliy tuzilmasiga mos holda foydalanish huquqlarini taqsimlash imkonini beradi. Ushbu modelda foydalanuvchilarga bevosita ruxsatlar emas, balki muayyan rollar biriktiriladi. RBAC modelining konseptual asosi “foydalanuvchi – rol – ruxsat” munosabatiga tayanib, har bir rol muayyan funksional vazifalar va vakolatlar majmuasini ifodalaydi. Amaliyotda RBAC modeli bank axborot tizimlari, universitet boshqaruv platformalari hamda yirik korporativ axborot tizimlarida keng qo‘llaniladi. Ushbu yondashuv boshqaruv jarayonining soddaligi va xodimlar almashinuvida qulaylik yaratishi bilan ajralib tursa-da, rollarning haddan tashqari ko‘payib ketishi va dinamik muhitlarda moslashuvchanlikning cheklanganligi uning asosiy kamchiliklari sifatida qayd etiladi.

Atributlarga asoslangan foydalanishlarni boshqarish (Attribute-Based Access Control — ABAC) modeli esa foydalanishlarni boshqarishning eng zamonaviy va yuqori moslashuvchan yondashuvi hisoblanadi. Ushbu modelda foydalanish to‘g‘risidagi qarorlar

subyekt, obyekt, muhit va bajarilayotgan harakat atributlarining majmuasiga asoslanadi. Natijada murakkab va noan'anaviy xavfsizlik siyosatlarini amalga oshirish imkoniyati yaratiladi. ABAC modeli bulutli hisoblash muhitlari, Internet of Things (IoT) tizimlari hamda mikroxizmatlarga asoslangan arxitekturalarda samarali qo‘llaniladi. Ushbu yondashuvning asosiy ustunligi yuqori darajadagi moslashuvchanlik bo‘lsa, yuqori hisoblash resurslariga bo‘lgan ehtiyoj va joriy etish jarayonining murakkabligi uning asosiy cheklovlari sifatida e'tirof etiladi.

Umuman olganda, foydalanishlarni boshqarish modellarining har biri muayyan axborot tizimlari va xavfsizlik talablariga mos holda qo‘llaniladi. Zamonaviy axborot tizimlarida yuqori darajadagi himoya va moslashuvchanlikni ta'minlash maqsadida ko‘pincha ushbu modellar kombinatsiyalashgan, ya'ni gibrid yondashuvlar asosida realizatsiya qilinadi.

O‘tkazilgan tahlil natijalari shuni ko‘rsatadiki, foydalanishlarni boshqarish modellarining har biri muayyan sharoit va xavfsizlik talablariga mos holda qo‘llaniladi. Zamonaviy axborot tizimlarida yuqori darajadagi himoya va moslashuvchanlikni ta'minlash maqsadida ko‘pincha gibrid yondashuvlar qo‘llanilib, bir nechta modellar kombinatsiyasi asosida axborot xavfsizligi ta'minlanadi.

Axborot xavfsizligini ta'minlashda foydalanishlarni boshqarish modellarining o‘rni beqiyosdir. Tadqiqot natijalariga ko‘ra, DAC modeli soddaligi bilan ajralib tursa-da, yuqori xavfsizlik talab etiladigan tizimlar uchun yetarli emas. MAC modeli qat'iy nazoratni ta'minlaydi, RBAC modeli esa tashkilotlar uchun optimal boshqaruv imkonini yaratadi. ABAC modeli esa zamonaviy, dinamik axborot muhitlari uchun eng istiqbolli yechim hisoblanadi. Kelajakda ushbu modellarni sun'iy intellekt asosida optimallashtirish dolzarb ilmiy yo‘nalishlardan biri bo‘lib qoladi.

Foydalanilgan adabiyotlar

1. D. Ferraiolo, D. Kuhn, “Role-Based Access Controls,” 15th NIST-NCSC National Computer Security Conference, 1992..
2. R. Sandhu et al., “Role-Based Access Control Models,” IEEE Computer, vol. 29, no. 2, pp. 38–47, 1996.
3. V. C. Hu et al., “Guide to Attribute Based Access Control (ABAC),” NIST SP 800-162, 2014.
4. M. Bishop, Computer Security: Art and Science, Addison-Wesley, 2018.

5. W. Stallings, Network Security Essentials, Pearson, 2020.
6. Xursanoy, S. (2025). SPECIALIZED TECHNICAL DEVICES AND COUNTER-CRIMINALISTICS (COUNTER-FORENSIC SCIENCE). Universum: технические науки, 9(5 (134)), 24-26.
7. Qizi, S. X. X., & O‘G‘Li, R. R. R. (2025). KOMPYUTER TARMOQLARIDA HUJUM IZLARINI ANIQLASH VA ULARNI TURLARI BO ‘YICHA TIZIMLI TASNIFLASH. Al-Farg’oniy avlodlari, 1(2), 40-44.
8. Akramjonovich, R. Z., Qizi, S. X. X., & O‘G‘Li, A. A. A. (2025). ELGAMAL SHIFRLASH ALGORITMI KALITLARNI YARATISH, SHIFRLASH VA DESHIFRLASH JARAYONLARI. Al-Farg’oniy avlodlari, 1(2), 20-22.
9. Raxmatov, R. (2025). INNOBELL–aqlli maktab qo ‘ng ‘irog ‘i tizimi. Engineering problems and innovations, 3(5), 21-25.
10. Qizi, S. X. X., & O‘G‘Li, R. R. R. (2025). KOMPYUTER TARMOQLARIDA HUJUM IZLARINI ANIQLASH VA ULARNI TURLARI BO ‘YICHA TIZIMLI TASNIFLASH. Al-Farg’oniy avlodlari, 1(2), 40-44.
11. Nurmaxamadovna, G. A. S. (2023). ZAMONAVIY TA’LIMNI TASHKIL ETISHDA VR TEXNOLOGIYALARIDAN FOYDALANISH METODIKASI. QO ‘QON UNIVERSITETI XABARNOMASI, 135-137.
12. Narmuradovna, N. S. (2023). OLIY TA’LIMDA ELEKTRON TA’LIM RESURLARINI FOYDADANISHNING AHAMIYATI. QO ‘QON UNIVERSITETI XABARNOMASI, 95-96.