

OPERATSION TIZIMLARDA XAVFSIZLIK SIYOSATLARI VA MODELLARI

Allaberganova Nasiba Muradovna

Toshkent amaliy fanlar universiteti, o'qituvchisi,

ORCID: 0009-0003-4206-7780 e-mail: abisan_1990@mail.ru

Muxarramov Abdullo Nasritdin o'g'li

E-mail: abdullomuxarramov@gmail.com

Toshkent amaliy fanlar universiteti, Axborot texnologiyalar fakulteti KAX 23 01 talabasi

Annotatsiya: Ushbu maqolada operatsion tizimlarda xavfsizlik siyosatlari va modellari tahlil qilinadi. Axborot xavfsizligini ta'minlashda qo'llaniladigan asosiy yondashuvlar, jumladan, Bell-LaPadula va Biba xavfsizlik modellari ko'rib chiqiladi. Shuningdek, foydalanuvchi huquqlarini boshqarish, tizim resurslarini himoyalash hamda ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta'minlash masalalari yoritilgan.

Kalit so'zlar: Operatsion tizim, xavfsizlik siyosati, xavfsizlik modeli, Bell-LaPadula, Biba, autentifikatsiya, avtorizatsiya, maxfiylik, yaxlitlik, mavjudlik

Аннотация: В данной работе рассматриваются политики и модели безопасности в операционных системах. Особое внимание уделяется основным подходам к обеспечению информационной безопасности, включая модели Белла-ЛаПадулы и Биба. Также анализируются вопросы управления доступом пользователей, защиты системных ресурсов и обеспечения конфиденциальности, целостности и доступности данных.

Ключевые слова: Операционная система, политика безопасности, модель безопасности, Белла-ЛаПадулы, Биба, аутентификация, авторизация, конфиденциальность, целостность, доступность

Annotation: This paper discusses security policies and models in operating systems. It focuses on key approaches to information security, including the Bell-LaPadula and Biba models. The study also covers user access control, system resource protection, and ensuring data confidentiality, integrity, and availability.

Keywords: Operating system, security policy, security model, Bell-LaPadula, Biba, authentication, authorization, confidentiality, integrity, availability

Kirish (Introduction)

Zamonaviy axborot texnologiyalari tez sur'atlar bilan rivojlanib borayotgan sharoitda operatsion tizimlar har qanday kompyuter tizimining ajralmas qismi hisoblanadi. Ular apparat va dasturiy resurslarni boshqarish bilan birga, foydalanuvchi va tizim o'rtasidagi asosiy bog'lovchi vosita vazifasini bajaradi. Shu sababli operatsion tizimlarning ishonchli va xavfsiz ishlashi bugungi kunda alohida ahamiyat kasb etadi. Axborotlarning hajmi ortib borayotgani, tarmoqlar orqali ma'lumot almashish kengaygani sari turli xil kiberxavflar ham kuchayib bormoqda. Bu esa operatsion tizimlarda xavfsizlikni ta'minlash masalasini yanada dolzarb qiladi.

Operatsion tizimlarda xavfsizlikni ta'minlash muhimligi shundaki, aynan operatsion tizim orqali barcha dasturlar va foydalanuvchilar tizim resurslariga murojaat qiladi. Agar operatsion tizimda zaiflik mavjud bo'lsa, bu butun tizimning buzilishiga, ma'lumotlarning yo'qolishiga yoki ruxsatsiz foydalanilishiga olib kelishi mumkin. Xususan, maxfiy ma'lumotlarning oshkor bo'lishi, ma'lumotlarning buzilishi yoki tizimning ishlamay qolishi jiddiy oqibatlariga sabab bo'ladi. Shuning uchun operatsion tizim darajasida xavfsizlik siyosatlari va mexanizmlarini to'g'ri tashkil etish muhim hisoblanadi.

Ushbu maqolaning maqsadi operatsion tizimlarda xavfsizlik siyosatlarini va modellarning mohiyatini yoritish hamda ularning amaliy ahamiyatini tahlil qilishdan iborat. Mazkur maqsadga erishish uchun quyidagi vazifalar belgilangan: operatsion tizimlarda xavfsizlik tushunchasini izohlash, xavfsizlik siyosatlarining asosiy turlarini ko'rib chiqish, keng qo'llaniladigan xavfsizlik modellari (masalan, Bell-LaPadula va Biba)ni tahlil qilish hamda zamonaviy operatsion tizimlarda qo'llanilayotgan xavfsizlik mexanizmlarini o'rganish.

Operatsion tizim tushunchasi

Operatsion tizim (OT) — bu kompyuter apparat resurslarini boshqaruvchi va foydalanuvchi hamda dasturlar o'rtasida vositachi vazifasini bajaruvchi tizimli dasturiy ta'minotdir. U dasturlar bajarilishini nazorat qiladi hamda tizim resurslaridan samarali foydalanishni ta'minlaydi [1].

Operatsion tizimning asosiy vazifalariga jarayonlarni boshqarish, ya'ni dasturlarni ishga tushirish va ularning bajarilishini nazorat qilish; xotirani boshqarish, ya'ni operativ xotirani taqsimlash va undan foydalanishni tartibga solish; fayl tizimini boshqarish, ya'ni ma'lumotlarni saqlash, o'qish va yozishni tashkil etish; qurilmalarni boshqarish, ya'ni kirish-chiqish qurilmalari bilan ishlashni ta'minlash; hamda foydalanuvchi interfeysini yaratish kiradi [2].

Hozirgi kunda keng qo'llaniladigan operatsion tizimlar qatoriga Microsoft Windows, Linux va macOS kiradi. Microsoft Windows keng tarqalgan bo'lib, asosan shaxsiy kompyuterlarda qo'llaniladi va qulay grafik interfeysga ega [3].

Linux ochiq kodli operatsion tizim bo'lib, barqarorligi va xavfsizligi sabab server tizimlarida keng ishlatiladi [4]. macOS esa Apple Inc. tomonidan ishlab chiqilgan bo'lib, yuqori darajadagi optimizatsiya va xavfsizlik imkoniyatlari bilan ajralib turadi hamda Apple qurilmalarida ishlaydi [5].

Xavfsizlik tushunchasi

Axborot xavfsizligi — bu axborotni ruxsatsiz kirish, foydalanish, oshkor etish, o'zgartirish yoki yo'q qilishdan himoya qilishga qaratilgan usullar va vositalar majmuasidir. Axborot xavfsizligi tizimning ishonchli ishlashini ta'minlash va ma'lumotlarni himoyalashga xizmat qiladi [6].

Axborot xavfsizligining asosiy tamoyillari uchta muhim jihatni o'z ichiga oladi. Maxfiylik (Confidentiality) — axborotga faqat ruxsat etilgan foydalanuvchilar kirishini ta'minlashni anglatadi. Bu tamoyil ma'lumotlarning begona shaxslar tomonidan ko'rilishi yoki tarqalib ketishining oldini olishga qaratilgan [7].

Yaxlitlik (Integrity) — axborotning to'g'riligini va o'zgarmagan holda saqlanishini ta'minlaydi. Ya'ni, ma'lumotlar ruxsatsiz o'zgartirilmasligi, buzilmasligi yoki noto'g'ri shaklga keltirilmasligi kerak [6].

Mavjudlik (Availability) — axborot va tizim resurslari zarur bo'lgan vaqtda foydalanuvchilar uchun ochiq va ishlashga tayyor bo'lishini anglatadi. Bu tamoyil tizimning uzluksiz ishlashini va xizmatlardan foydalanish imkoniyatini ta'minlaydi [8].

Ushbu uch tamoyil birgalikda axborot xavfsizligining asosini tashkil etadi va har qanday operatsion tizimda xavfsizlikni ta'minlashda muhim rol o'ynaydi [9].

Operatsion tizimlarda xavfsizlik siyosatlarini

Operatsion tizimlarda xavfsizlik siyosati — bu tizim resurslaridan foydalanish qoidalari va cheklovlarini belgilovchi tamoyillar majmuasidir. Xavfsizlik siyosati foydalanuvchilarning tizimga kirishi, ma'lumotlarga murojaati va resurslardan foydalanishini tartibga soladi hamda ruxsatsiz kirishni cheklashga xizmat qiladi [6].

Xavfsizlik siyosatlari turli yondashuvlarga asoslanadi. Eng keng tarqalgan turlaridan biri majburiy xavfsizlik siyosati (Mandatory Access Control — MAC) hisoblanadi. Bu modelda tizim resurslariga kirish huquqlari markazlashgan holda belgilanadi va foydalanuvchilar tomonidan o'zgartirilmaydi. Har bir obyekt va subyekt ma'lum darajadagi xavfsizlik belgilari bilan aniqlanadi va kirish shu belgilar asosida nazorat qilinadi [9].

Ixtiyoriy xavfsizlik siyosati (Discretionary Access Control — DAC) esa resurs egasiga o'z ma'lumotlariga kim kirishini belgilash imkonini beradi. Masalan, foydalanuvchi o'z fayliga boshqa foydalanuvchilarga o'qish yoki yozish huquqini berishi mumkin. Ushbu yondashuv moslashuvchan bo'lsa-da, xavfsizlik darajasi MAC ga nisbatan pastroq hisoblanadi [6].

Rolga asoslangan boshqaruv (Role-Based Access Control — RBAC) modelida foydalanuvchilarga to'g'ridan-to'g'ri huquqlar emas, balki rollar biriktiriladi. Har bir rolga ma'lum ruxsatlar to'plami beriladi va foydalanuvchi ushbu rol orqali tizim resurslaridan foydalanadi. Bu usul tizimni boshqarishni soddalashtiradi va yirik tizimlarda samarali qo'llaniladi [7].

Operatsion tizimlarda xavfsizlik siyosatlarini amalga oshirish maxsus mexanizmlar orqali ta'minlanadi. Bunga autentifikatsiya (foydalanuvchini aniqlash), avtorizatsiya (kirish huquqlarini belgilash), kirishni boshqarish ro'yxatlari (Access Control Lists — ACL), xavfsizlik jurnallari (audit) va monitoring tizimlari kiradi. Ushbu mexanizmlar yordamida tizim resurslariga kirish nazorat qilinadi va xavfsizlik siyosatlarining bajarilishi ta'minlanadi [8].

Xavfsizlik modellari

Xavfsizlik modeli — bu axborot tizimlarida xavfsizlik siyosatini ifodalash va uni amaliyotda qo'llash uchun ishlab chiqilgan nazariy modeldir. Xavfsizlik modellari tizimda ma'lumotlarga kirish qoidalarini formal tarzda belgilaydi va xavfsizlikni ta'minlash mexanizmlariga asos bo'lib xizmat qiladi [6].

Eng mashhur xavfsizlik modellari qatoriga Bell-LaPadula, Biba va Clark-Wilson modellari kiradi. Ushbu modellarning har biri axborot xavfsizligining muayyan jihatini ta'minlashga qaratilgan. Bell-LaPadula modeli axborotning maxfiyligini ta'minlashga yo'naltirilgan model hisoblanadi. Ushbu model “yuqoriga o'qish mumkin emas” (no read up) va “pastga yozish mumkin emas” (no write down) qoidalariga asoslanadi. Ya'ni, foydalanuvchi o'z darajasidan yuqori bo'lgan ma'lumotni o'qiy olmaydi va past darajadagi obyektlarga ma'lumot yozolmaydi. Bu model asosan maxfiy ma'lumotlarni himoya qilish uchun qo'llaniladi [9].

Biba modeli esa ma'lumotlarning yaxlitligini ta'minlashga qaratilgan. U Bell-LaPadula modelining teskarisi bo'lib, “pastdan o'qish mumkin emas” (no read down) va “yuqoriga yozish mumkin emas” (no write up) qoidalariga asoslanadi. Ushbu model ma'lumotlarning noto'g'ri yoki ishonchsiz manbalardan o'zgartirilishining oldini olishga xizmat qiladi [6].

Clark-Wilson modeli amaliy xavfsizlik talablariga mos keladigan model bo'lib, asosan tijorat tizimlarida qo'llaniladi. Bu modelda ma'lumotlarga faqat maxsus tekshirilgan va ruxsat etilgan operatsiyalar orqali kirish mumkin. Model tranzaksiyalarni nazorat qilish va ma'lumotlar yaxlitligini saqlashga qaratilgan bo'lib, tizimda noto'g'ri o'zgarishlarning oldini oladi [7].

Ushbu xavfsizlik modellari operatsion tizimlarda xavfsizlik siyosatlarini amalga oshirishda muhim nazariy asos bo'lib xizmat qiladi va turli tizimlarda turli darajada qo'llaniladi.

Zamonaviy operatsion tizimlarda xavfsizlik

Zamonaviy operatsion tizimlarda xavfsizlik tizimning barcha qatlamlarida tashkil etiladi va u foydalanuvchilarni tekshirish, resurslarga kirishni nazorat qilish hamda zararli faoliyatni aniqlash kabi mexanizmlarni o'z ichiga oladi. Operatsion tizim xavfsizligi axborotning maxfiyligi,

yaxlitligi va mavjudligini ta'minlashga qaratilgan bo'lib, turli texnologiyalar orqali amalga oshiriladi [10].

Microsoft Windows operatsion tizimida xavfsizlik mexanizmlari kompleks tarzda tashkil etilgan. Tizimda foydalanuvchilarni autentifikatsiya qilish uchun login va parol tizimi, shuningdek, qo'shimcha himoya sifatida ikki bosqichli tekshiruv usullari qo'llaniladi. Windows Defender tizimni zararli dasturlardan himoya qiladi, User Account Control (UAC) esa foydalanuvchi tomonidan bajarilayotgan harakatlarni nazorat qiladi. Bundan tashqari, fayl tizimida ruxsatlar orqali foydalanuvchilarning huquqlari qat'iy boshqariladi [11].

Linux operatsion tizimida xavfsizlik ochiq kodli yondashuv asosida rivojlangan. Tizimda foydalanuvchi huquqlari aniq ajratilgan bo'lib, har bir foydalanuvchi o'ziga tegishli darajada ishlaydi. Linuxda qo'shimcha xavfsizlik vositalari sifatida SELinux va AppArmor ishlatiladi. SELinux majburiy kirishni boshqarish modeliga asoslanadi va tizim resurslariga kirishni qat'iy nazorat qiladi, AppArmor esa dasturlar faoliyatini cheklash orqali tizimni himoya qiladi [12].

Mobil operatsion tizimlarda xavfsizlik alohida ahamiyatga ega. Android tizimida har bir ilova alohida izolyatsiyalangan muhitda ishlaydi va foydalanuvchi ruxsatisiz boshqa resurslarga kira olmaydi. Ilovalar uchun ruxsatlar tizimi mavjud bo'lib, foydalanuvchi har bir funksiyaga alohida ruxsat beradi. iOS tizimi esa yopiq arxitekturaga ega bo'lib, ilovalar qat'iy tekshiruvdan o'tkaziladi va xavfsizlik darajasi yuqori hisoblanadi. Unda shifrlash va sandboxing texnologiyalari keng qo'llaniladi [13].

Shu tarzda zamonaviy operatsion tizimlar xavfsizlikni ta'minlash uchun turli mexanizmlarni qo'llaydi va ular doimiy ravishda takomillashtirib boriladi [14].

Xavfsizlik tahdidlari va hujumlar

Operatsion tizimlarda xavfsizlik tahdidlari — bu tizim resurslari va axborotga zarar yetkazishi mumkin bo'lgan omillar majmuasidir. Ushbu tahdidlar tizimning normal ishlashini buzishi, ma'lumotlarning yo'qolishiga yoki ruxsatsiz foydalanilishiga olib kelishi mumkin. Zamonaviy axborot tizimlarida tahdidlar soni ortib borayotgani sababli ularni aniqlash va oldini olish muhim hisoblanadi [10].

Viruslar va zararli dasturlar operatsion tizimlarga eng keng tarqalgan tahdidlardan biridir. Zararli dasturlar (malware) tizimga yashirin ravishda kirib, ma'lumotlarni o'g'irlash, o'zgartirish yoki tizim faoliyatini izdan chiqarishga xizmat qiladi. Ular viruslar, qurtlar (worms), troyan dasturlar va boshqa shakllarda uchraydi. Bunday dasturlar ko'pincha foydalanuvchi bilmasdan o'rnatiladi va tizimda yashirin faoliyat olib boradi [11].

Ruxsatsiz kirish tizim xavfsizligiga jiddiy tahdid hisoblanadi. Bu holatda hujumchi tizimga noqonuniy ravishda kirish uchun parollarni buzish, autentifikatsiya tizimidagi zaifliklardan foydalanish yoki ijtimoiy muhandislik usullarini qo'llaydi. Natijada maxfiy ma'lumotlar oshkor bo'lishi yoki tizim ustidan nazorat yo'qolishi mumkin [12].

Tarmoq hujumlari orqali ham operatsion tizimlarga zarar yetkazish mumkin. Bunday hujumlarga xizmatdan voz kechish (Denial of Service — DoS), “man-in-the-middle” va tarmoq trafikini kuzatish (sniffing) kiradi. Ushbu hujumlar orqali tizimning ishlashi to'xtatilishi yoki ma'lumotlar noqonuniy qo'lga kiritilishi mumkin [14].

Shu sababli operatsion tizimlarda xavfsizlik tahdidlarini kamaytirish uchun kompleks yondashuv, jumladan antivirus vositalari, tarmoq himoyasi va foydalanuvchi nazoratini kuchaytirish talab etiladi [15].

Xavfsizlikni ta'minlash usullari

Operatsion tizimlarda xavfsizlikni ta'minlash turli texnik va dasturiy vositalar yordamida amalga oshiriladi. Ushbu usullar tizimni ruxsatsiz kirishdan himoya qilish, ma'lumotlarni saqlash va xavfsiz ishlashni ta'minlashga qaratilgan. Xavfsizlikni ta'minlashda kompleks yondashuv qo'llanilib, bir nechta mexanizmlar birgalikda ishlaydi [10].

Autentifikatsiya va avtorizatsiya operatsion tizim xavfsizligining asosiy elementlaridan hisoblanadi. Autentifikatsiya foydalanuvchini aniqlash jarayoni bo'lib, login va parol, biometrik ma'lumotlar yoki maxsus kalitlar orqali amalga oshiriladi. Avtorizatsiya esa foydalanuvchiga tizim resurslaridan foydalanish huquqlarini belgilaydi. Ushbu ikki jarayon yordamida tizimga kirish qat'iy nazorat qilinadi va ruxsatsiz foydalanishning oldi olinadi [11].

Shifrlash ma'lumotlarni himoyalashning muhim usullaridan biridir. Bu usulda axborot maxsus algoritmlar yordamida kodlanadi va faqat tegishli kalit orqali ochilishi mumkin bo'ladi. Shifrlash ma'lumotlarning maxfiyligini saqlashga xizmat qiladi va ayniqsa tarmoq orqali uzatilayotgan axborotni himoya qilishda keng qo'llaniladi [14].

Antivirus va firewall tizimlari operatsion tizimni tashqi va ichki tahdidlardan himoya qiladi. Antivirus dasturlari zararli dasturlarni aniqlaydi, bloklaydi va yo'q qiladi. Firewall esa tarmoq orqali kelayotgan va chiqayotgan trafikni nazorat qilib, xavfli ulanishlarni cheklaydi. Ushbu vositalar tizim xavfsizligini ta'minlashda muhim rol o'ynaydi va doimiy ravishda yangilanib borilishi zarur [15].

Shu tarzda autentifikatsiya, shifrlash va himoya dasturlaridan foydalanish operatsion tizim xavfsizligini yuqori darajada ta'minlash imkonini beradi.

Xulosa

Ushbu maqolada operatsion tizimlarda xavfsizlik siyosatlari va modellari, shuningdek zamonaviy xavfsizlik mexanizmlari tahlil qilindi. Operatsion tizimlar kompyuter tizimining asosiy qismi bo'lib, ularning xavfsizligi butun tizim barqarorligi va ma'lumotlar himoyasini ta'minlashda hal qiluvchi ahamiyatga ega.

Maqola davomida axborot xavfsizligining asosiy tamoyillari — maxfiylik, yaxlitlik va mavjudlik — operatsion tizim xavfsizligining asosi ekani ko'rsatildi. Shuningdek, xavfsizlik siyosatlari, jumladan majburiy (MAC), ixtiyoriy (DAC) va rolga asoslangan (RBAC) boshqaruv yondashuvlari tizim resurslariga kirishni nazorat qilishda muhim vosita ekani yoritildi. Bell-LaPadula, Biba va Clark-Wilson kabi xavfsizlik modellari esa ushbu siyosatlarning nazariy asosini tashkil etishi ta'kidlandi.

Bundan tashqari, zamonaviy operatsion tizimlarda qo'llanilayotgan xavfsizlik mexanizmlari, turli tahdidlar va ularga qarshi kurash usullari ko'rib chiqildi. Xususan, autentifikatsiya, avtorizatsiya, shifrlash, antivirus va firewall kabi vositalar tizim xavfsizligini ta'minlashda muhim rol o'ynashi qayd etildi.

Xulosa qilib aytganda, operatsion tizimlarda xavfsizlikni ta'minlash kompleks yondashuvni talab qiladi. Texnik vositalar bilan bir qatorda foydalanuvchilarning xavfsizlik madaniyatini oshirish ham muhimdir. Zamonaviy sharoitda axborot xavfsizligini ta'minlash tizimlarning ishonchli va uzluksiz ishlashining asosiy sharti hisoblanadi.

Foydalanilgan adabiyotlar

1. Operating System Concepts Silberschatz A., Galvin P.B., Gagne G. *Operating System Concepts*. — 10th ed. — Wiley, 2018.

2. Modern Operating Systems Tanenbaum A.S., Bos H. *Modern Operating Systems*. — 4th ed. — Pearson, 2015.
3. Microsoft Corporation. *Windows Operating System Overview*. — Microsoft Docs, 2023.
4. Linux Foundation. *What is Linux?* — Official documentation, 2022.
5. Apple Inc. Apple Inc. *macOS Overview*. — Apple Developer Documentation, 2023.
6. Computer Security: Principles and Practice Stallings W., Brown L. *Computer Security: Principles and Practice*. — 4th ed. — Pearson, 2018.
7. Information Security Principles and Practice Stamp M. *Information Security: Principles and Practice*. — 2nd ed. — Wiley, 2011.
8. NIST NIST. *Computer Security Resource Center (CSRC)*. — 2023.
9. ISO/IEC 27001 ISO/IEC 27001. *Information Security Management Systems — Requirements*. — ISO, 2013.
10. Security Engineering Anderson R. *Security Engineering: A Guide to Building Dependable Distributed Systems*. — 2nd ed. — Wiley, 2008.
11. Computer Security Fundamentals Easttom C. *Computer Security Fundamentals*. — 3rd ed. — Pearson, 2019.
12. OWASP Foundation. *Top 10 Security Risks*. — 2023.
13. SANS Institute SANS Institute. *Information Security Resources*. — 2022.
14. Network Security Essentials Stallings W. *Network Security Essentials*. — 6th ed. — Pearson, 2017.
15. ENISA *Cybersecurity Threat Landscape*. — 2023.