15-MA’RUZA. SMARTFONLAR UCHUN OPERATSION TIZIMLAR

Mobil operatsion tizimlar

Mobil qurilmalarning sifati asosan apparat xarakteristikalariga bog’liq bo’lsa, ulardan foydalanish qulayligi ko’p jihatdan mobil operatsion tizimlarga (OT) bog’liq.

Hozirda mavjud mobil operatsion tizimlar foydalanuvchilarga nafaqat mobil telefonlar uchun odatiy bo’lgan SMS-xabarlarni jo’natish va telefon chaqiruvlarini bajarish kabi harakatlarni, balki ma’lumotlarni saqlash, tahrirlash va almashishi bo’yicha keng imkoniyatlarni taqdim etadi. Ba’zi mobil operatsion tizimlar ma’lumotlarni shifrlab saqlash, hamda mobil qurilmadagi ma’lumotlarni masofadan boshqarish bo’yicha qo’shimcha imkoniyatlarga ega.

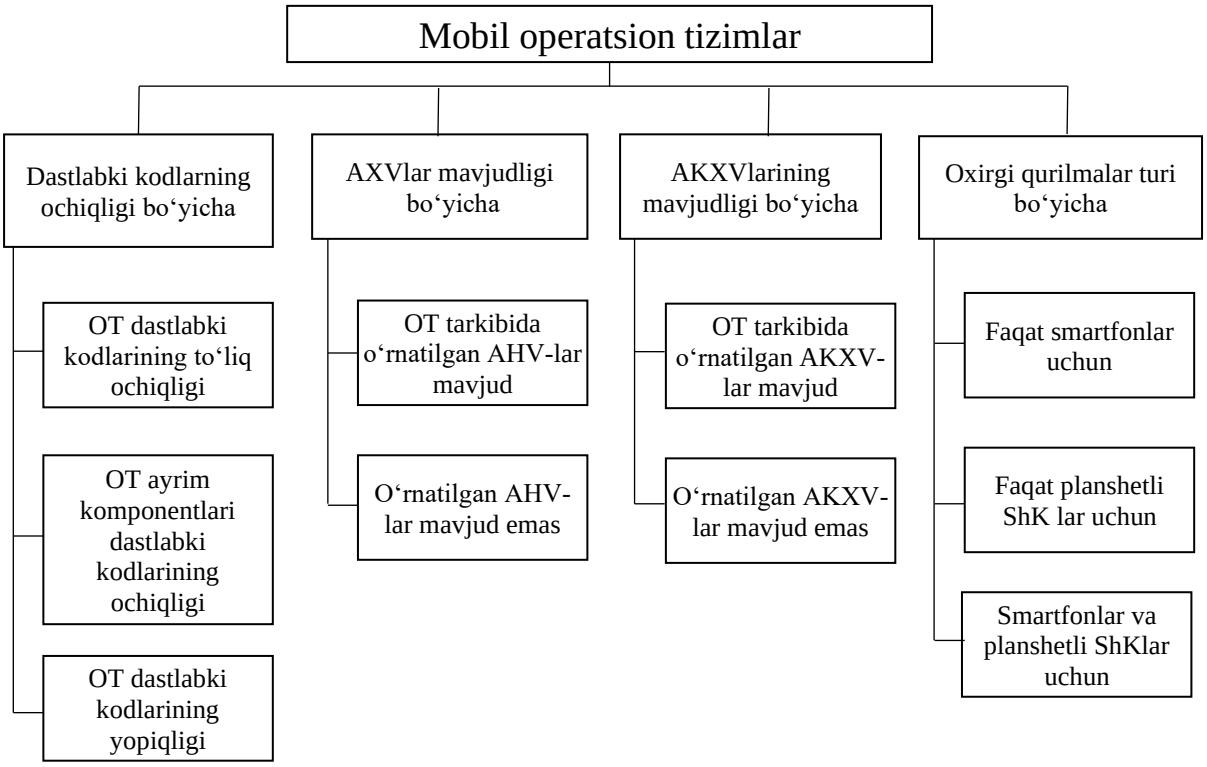
Mobil operatsion tizimlarni quyidagi alomatlari bo’yicha tasniflash mumkin (6.1-rasm):

- operatsion tizim ochiqligi;
- axborotni himoyalash vositalarining mavjudligi (AHV);
- axborotni kriptografik himoyalash vositalarining mavjudligi (AKHV);
- oxirgi qurilmalar turi.

Quyida mobil qurilmalar uchun keng tarqalgan operatsion tizimlar ko’rilgan.

Symbian OS. Ushbu operatsion tizim Nokia firmasining madadi tufayli eng ommabop hisoblanar edi. Ushbu tizim o’lchamining kichikligi, hamda grafika interfeysining va tizim yadrosining bir-biridan ajratilganligi ham muhim rol o’ynadi. Bu uning turli mobil qurilmalariga osongina o’rnatilishiga imkon berdi. Keyinroq ko’p vazifalik qo’shilgan.

Har bir mutaxassis apparat platforma cheklovlariga bog’liq holda o’zining operatsion tizim versiyasini yaratar edi. Har bir versiya o’ziga xos xususiyatlarga ega bo’lib, har bir versiya uchun o’zining ilovalarini ishlab chiqish lozim edi. Bu noqulaylik edi. Shu sababli Windows Mobile, Android va iPhone operatsion tizimlari paydo bo’lganidan keyin Symbian operatsion tizim o’zining ommaviyligini yo’qotdi. Hozirda faqat Nokia kompaniyasi ushbu operatsion tizimdan o’zining smartfonlari uchun foydalanadi.



6.1-rasm. Mobil operatsion tizimlarning tasnifi

Symbian operatsion tizim afzalliklari:

- xotiraga va prosessorga talablarning pastligi;
- ishlatilmaydigan xotirani bo’shatish funksiyasi;
- barqarorlik;
- ushbu platforma uchun viruslar sonining kamligi;
- tezdan yangi versiya paydo bo’ladi va barqarorlik tiklanadi;
- dasturlarning katta soni.

Symbian operatsion tizim kamchiliklari:

- shaxsiy kompyuter bilan ulanish uchun qo’shimcha dastur o’rnatilishi lozim;
- eski va yangi versiyalar uchun dasturlarning nomuvofiqligi.

Windows Mobile operatsion tizim. Ushbu operatsion tizim operatsion tizimlarni ishlab chiqarishda dunyo miqyosida etakchi hisoblanuvchi Microsoft kompaniyasi tomonidan ishlab chiqilgan. Ushbu tizim shaxsiy kompyuterda ishlatiluvchi dasturiy interfeysdan foydalanadi. Bu dastur yozilishini ancha osonlashtiradi va foydalanuvchilarga qulay va tushunarli. Windows Mobile operatsion tizim komponentli, ko’p vazifali, ko’p oqimli va ko’p platformali operatsion tizim hisoblanadi. Shu tufayli ushbu operatsion tizim mobil qurilmalarda keng tarqalgan.

Windows Mobile operatsion tizimning afzalliklari:

- shaxsiy kompyuter versiyasi bilan o’xshashligi;
- sinxronlashning qulayligi;
- tarkibida ofis dasturlarining mavjudligi;
- ko’p vazifaligi.

Windows Mobile operatsion tizimning kamchiliklari:

- uskunalarga talablarning yuqoriligi;
- viruslar sonining ko’pligi;
- ishlashidagi beqarorlik.

Android operatsion tizim. Ushbu operatsion tizim Linux operatsion tizimga asoslangan va Open Handset Alliance tomonidan, Google madadi bilan ishlab chiqilgan eng yangi mobil operatsion tizimlardan biri hisoblanadi. Dastlabki koddan ochiq foydalanilgani tufayli ixtiyoriy ishlab chiqaruvchi o’zining ushbu operatsion tizim versiyasini yaratishi mumkin. Ilovalarni ishlab chiqaruvchilariga cheklashlarning katta bo’lmagan soni qo’yilgan. Shu sababli tekin va to’lovli ilovar to’plami mavjud.

Android *operatsion tizimning afzalliklari:*

- moslanuvchanlik;
- ochiq dastlabki kodlar;
-dasturlarning ko’pligi;
- yuqori tezkorlik;
- Google servislari bilan o’zaro aloqaning qulayligi;
- ko’p vazifaligi;

Android *operatsion tizimning kamchiliklari:*

- dolzarb versiyalarning ko’pligi;
- kodning ochiqligi tufayli xaker hujumlariga yuqori moyilligi;
- doimo kam-ko’stini to’ldirish talab etiladi.

iOS operatsion tizim. Ushbu operatsion tizim Apple kompaniyasi tomonidan taqdim etilgan bo’lib, faqat ushbu kompaniya mahsulotlarida tarqalgan. iPhone smartfonlarda, iPod pleyerlarda, iPad planshetlarda hamda Apple TV televizorga ulanadigan uskunalarda qo’llaniladi.

iOS operatsion tizimning afzalliklari:

- ishlatishda qulaylik;
- madadlashning sifatli xizmati;
- ishlashida ko’pgina muammolarni bartaraf etuvchi muntazam yangilashlar;
- App Store da turli dasturlar to’plamini xarid qilish imkoniyati.

iOS operatsion tizimning kamchiliklari:

- norasmiy ilovalarni o’rnatish uchun djaylbreyk dasturiy ilovadan foydalanish zaruriyati;
- operatsion tizimning blokirovkalangan xarakteri;
- ko’p vazifalikning mavjud emasligi;
- hujjatlarni o’rnatilgan muharirining yo’qligi.

Palm operatsion tizim. 1996 yili paydo bo’lgan va cho’ntak shaxsiy kompyuterida qo’llanilgan. Imkoniyatlarining kengligi va foydalanuvchilarga qulayligi tufayli keng tarqalgan edi. Hozirgacha deyarli ishlatilmagan. Ammo, HP kompaniyasi yordamida ulardan foydalanish imkoniyati paydo bo’ldi.

Palm operatsion tizimning afzalliklari:

- *resurslarga talabchan emas;*
- *foydalanuvchining qulay interfeysi;*
- *shaxsiy kompyuter bilan sinxronlashning qulayligi;*
- *ishonchligi.*

Palm operatsion tizimning kamchiliklari:

- *ko’p vazifalikning yetarlicha emasligi;*
- *multimedia funksiyalari rivojlanmagan.*

BlackBerry operatsion tizim faqat Research In Motion Limited (RIM) kompaniyasi ishlab chiqaruvchi qurilmalarida ishlaydi. Xabarlarni ushlab qolishning murakkabligi tufayli ushbu operatsion tizimli smartfonlar korporativ muhitda tarqalgan.

BlackBerry operatsion tizimning afzalliklari:

- elektron pochtadan foydalanishning qulayligi;
- shaxsiy kompyuter bilan osongina sinxronlanishi;
- xavfsizlikni sozlashning keng imkoniyatlari.

BlackBerry operatsion tizimning kamchiliklari:

- faqat matnli axborotni chiqarishga eng qulay sharoit yaratilgan, grafika bilan ishlash sifati juda yaxshi emas;
- juda qulay bo’lmagan brauzer.

Yuqorida keltirilganlardan kurinib turibdiki, mobil qurilmalarni tanlashda ularning texnik xarakteristikalari aslo asosiy parametr hisoblanmaydi. Haqiqatan, imkoniyati yuqori bo’lmagan operatsion tizimda ishlovchi zamonaviy apparatdan ma’no minimal.

Mobil operatsion tizimlar xavfsizligi va uni amalga oshirish mexanizmlari

Mobil qurilmalar uchun xavfsizlik mexanizmlarining rivoji shahsiy kompyuterlarga qaraganda boshqa yo’l bilan ketdi. Xavfsizlik mexanizmlari mobil qurilmalar himoyalanganligiga yanada qat’iy talablarni ta’minlashi lozim edi.

Himoyalanganlikka asosiy talablar quyidagilar:

- qurilma identifikatori (International Mobile Equipment Identifier, IMEI) ixtiyoriy vositalar, xususan, mexanik, elektrik va dasturiy vositalar, yordamida manipulyasiyalanishidan himoyalanishi lozim;
- mobil qurilmani ishlab chiqarish bosqichida kalibrlangan radiochastota sozlanmasi himoyalangan holda saqlanishi lozim;
- operatsion tizim Windows operatsion tizimiga xos "o’limning ko’k ekrani" deb ataluvchi kritik xatoning paydo bo’lishiga to’sqinlik qiluvchi, ishonchli bo’lishi lozim. Ushbu kritik xato natijasida operatsion tizim qayta yuklanadi.

Ushbu talablarning bajarilishini ta’minlash uchun dasturiy va apparat sathlarda himoya mexanizmlari yaratilgan va joriy etilgan.

Quyida keng tarqalgan ARM TrustZone prosessor misolida dasturiy va apparat sathlardagi himoya mexanizmlari batafsil bayon etilgan. Ushbu prosessor aksariyat smartfonlarda va planshetlarda o’rnatiluvchi komandalarning nabori qisqartirilgan (RISC) Advanced RISC Machine (ARM) arxitekturaga ega.

TrustZone xilidagi prosessorlarda dasturiy sathdagi himoya mexanizmlari.

ARM TrustZone konsepsiyasi asosida bajarish muhiti sathida himoyalangan (trusted), yoki boshqacha aytganda *bajarishning xavsiz muhiti TEE va himoyalanmagan* (non-trusted), yoki boshqacha aytganda *bajarishning ochiq muhiti REE* ga ajratish yotadi (6.2-rasm).

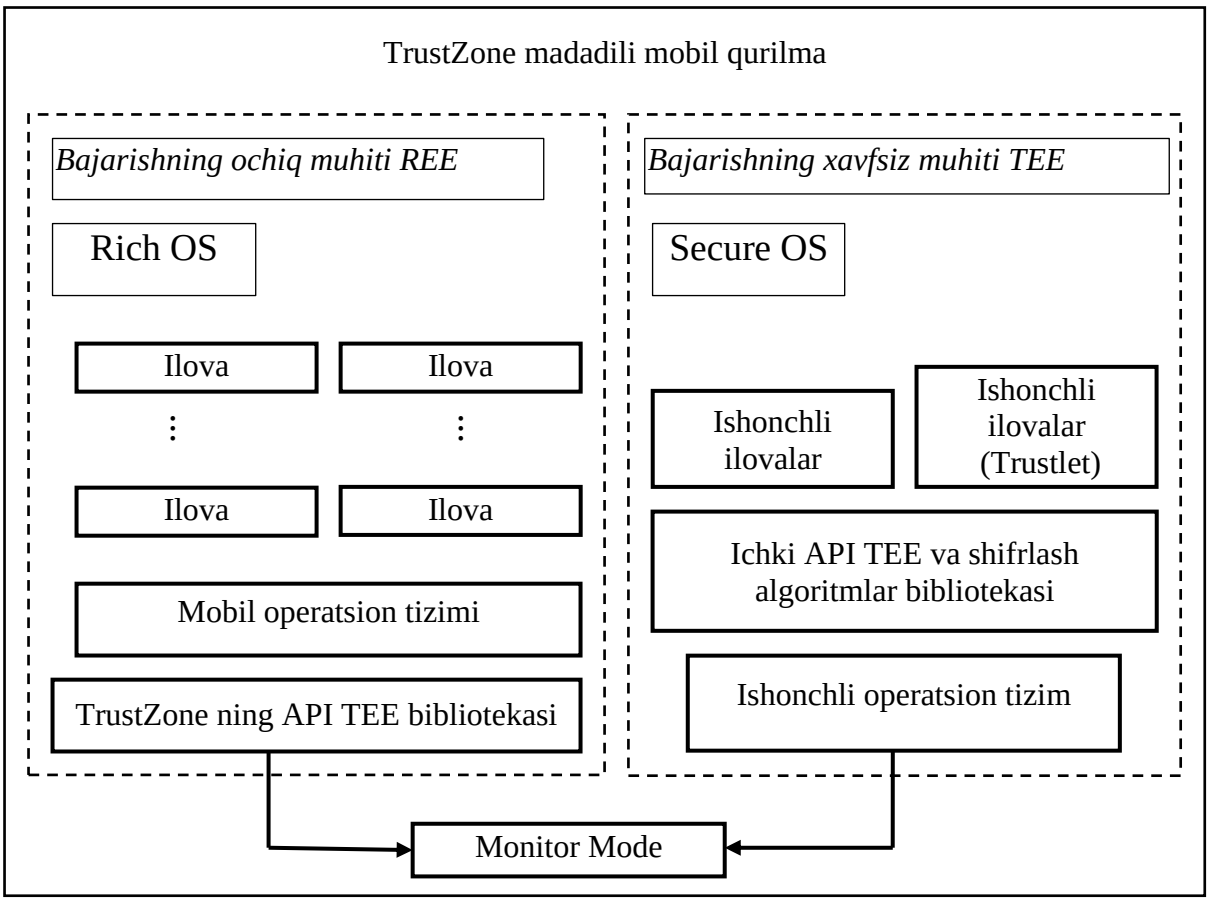
Rich OS - to’liq funksional operatsion tizim, ya’ni bibliotekalar, servislar va xizmatlar nabori. Bular tizim komponentlarini (ichki va chetki ilovalarni) boshqarishning umumiy funksiyalarini ta’minlaydi.

Secure OS – ishonchli operatsion tizim. Xavfsizlik yuzasidan funksiyalari cheklangan.

Trustlet – begona ishlab chiqaruvchilar taqdim etishi mumkin bo’lgan tekshirilgan ilova.

TEE (Trusted Execution Environments) – kritik muhim komponentlar xavfsizligini ta’minlovchi apparat (TrustZone) va dasturiy (Secure OS + ilovalar) vositalar majmui.

REE (Rich Execution Environment) – mobil qurilma ilovalari bilan ishlovchi mobil operatsion tizim.



6.2-rasm. TrustZone madadili mobil qurilmalar dasturiy ta’minotining arxitekturasi

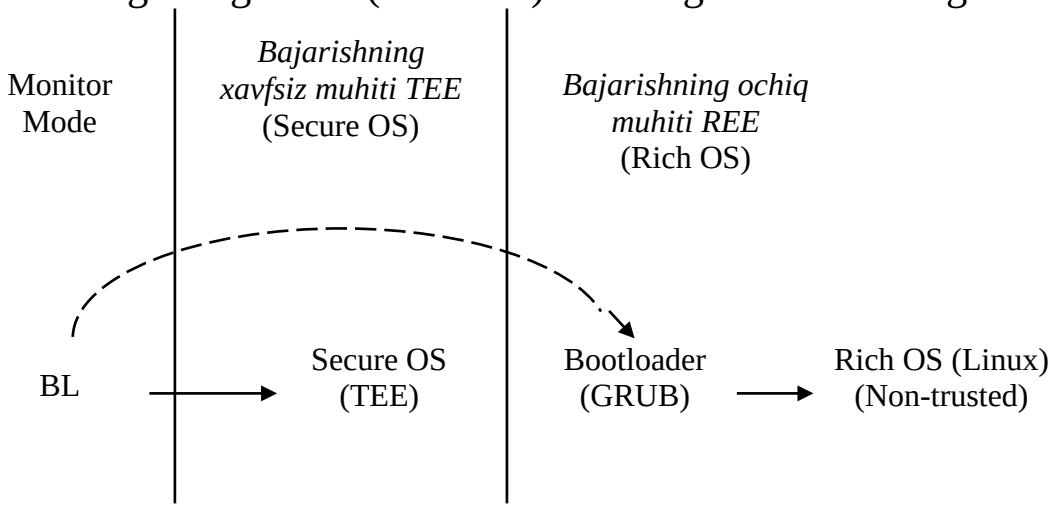
Umuman olganda, *TEE* va *REE* bajarish muhitlari orasidagi farq katta emas. Ikkalasida prosessorlarda mumkin bo’lgan barcha rejimlar (supervisor, user, data abort va h.) mavjud. Doimo himoyalangan Monitor Mode bundan mustasno.

Monitor Mode mobil tizim monitoringi uchun quvvatli instrument hisoblanadi. Uning yordamida quyidagilar amalga oshirilishi mumkin:

- jarayonlarni nazoratlash, ya’ni keraksizini tezda to’xtatish imkoniyati bilan barcha ishga solingan jarayonlarni kuzatish;
- tarmoq interfeyslari monitoringini amalga oshirish, ya’ni ishlatiluvchi tarmoq interfeyslarini kuzatish;
- tarmoq aktivligini kuzatish va monitoringini amalga oshirish, ya’ni har bir ulanishdagi IP-adres xususidagi batafsil axborotni taqdim etish;
- ishlatiluvchi xotira, akkumulyator zaryadi, fayl tizimi holati xususidagi axborotni yig’ish;

- barcha tizimli xabarlarni vaqtning real rejimida kuzatish.

Quyida yuklash va muhitlarni TEE va REE larga ajratishning soddalashtirilgan algoritmi (6.3-rasm) va uning tavsifi keltirilgan.



6.3-rasm. Yuklash va muhitlarni REE va TEE larga ajratishning soddalashtirilgan algoritmi

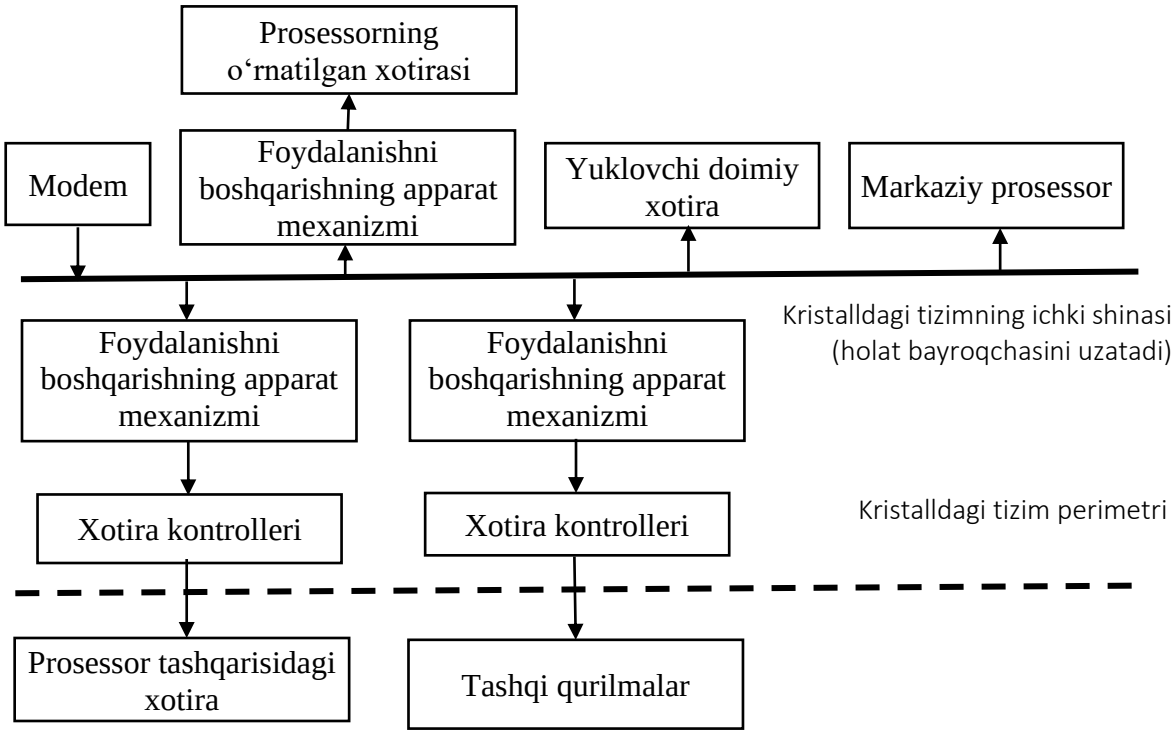
Prosessor Monitor Mode rejimida ish boshlaydi, ya’ni bajarishning xavfsiz muhiti TEEda bo’ladi va TEEning asosi hisoblanuvchi Secure OS ga bootloader ni yuklashni boshlab beradi. (BL-yuklovchi - Bootloader – yuklash jarayonining normal rejimda amalga oshirilishi uchun operatsion tizim yadrosini nazoratlovchi dastur). TEE tizimning barcha kerakli xavfsizlik konfiguratsiyasini sozlaydi. Masalan, u ochiq REE muhiti foydalanuvchisidan barmoq izlari skanerini va operativ xotira qismini bekitadi. So’ngra REEga o’tish boshlanadi. Undagi boshqa yuklagich, masalan GRUB (GRand Unified Bootloader) – operatsion tizim yuklagichi, foydalanuvchiga bir necha o’rnatilgan operatsion tizimlarga ega bo’lishiga va kompyuter ishga tushganida ularning birini yuklash uchun tanlashga imkon beradi. Undan so’ng Rich OS oddiy tartibda ishga tushiriladi.

Shunday qilib, ARM TrustZone ma’lumotlarning shifrlangan ko’rinishda himoyalangan saqlanishini, bazaviy kalit asosida kalitlarni generatsiyalashni va imzolarni tekshirishni ta’minlaydi. ARM TrustZone dan foydalanishning klassik misollari – elektron to’lovlarni himoyalash, video/audio kontentning xususiy patentlangan dasturiy ta’minotini, har xil ma’lumotlarni autentifikatsiyalash.

TrustZone xilidagi prosessorlarda apparat sathdagi himoya mexanizmlari. Mobil qurilmalarda axborotni apparat himoyalash yagona asosiy chipda integrallashgan doimiy va operativ xotiraning katta

bo’lmagan soniga ega markaziy prosessordan, tashqi qurilmalar va uzilishlar kontrollerlaridan hamda sozlash va trassirovka portlaridan iborat. Bunday prosessorga o’rnatilgan elementlar umumiy shina orqali ulangan, mobil qurilmaning boshqa komponetlari – asosiy (operativ) xotira, flesh-xotira, displey, antenna va h. – asosiy chipdan alohida amalga oshirilgan (6.4-rasm).

Apparat elementlaridan foydalanish prosessorning himoyalangan yoki shtat rejimida ishlashini aniqlovchi *holatlar bayrog’chasi* yordamida amalga oshirilgan. Holatlar bayrog’chasi markaziy prosessorning kommunikatsiya shinasi orqali uzatiladi.



6.4-rasm. Mobil qurilmaning apparat konfiguratsiyasi misoli

Markaziy prosessor mos holda, REE va TEE larga mo’ljallangan oddiy yoki himoyalangan rejimlarda ishlashi mumkin. Himoyalangan rejimda yuklash va sozlash ro’y beradi, so’ngra oddiy rejim harakatga keltiriladi. Ma’lum komandalar bajarilishida himoyalangan rejimga o’tkazilishi mumkin.

Ishonchli ilovalar, yuqorida aytilganidek, TEE da bajariladi. TEE da ishonchli ilovalar ishonchli operatsion tizimda minimal funksionallik bilan, ya’ni axborotni apparat himoyalash mexanizmining markaziy prosessorida ishlanadi. Ishonchli operatsion tizim ishonchli ilovalarning REE ilovalari bilan bog’lanishlari, hamda kriptografiya funksiyalarini

chaqirish va himoyalangan saqlanish uchun ishlatilishi mumkin bo’lgan TEE ning ichki dasturlash interfeysidan iborat.

Xavfsizlikni ta’minlashga yondashishlar kompleks xarakterga ega bo’lib, dasturiy ham apparat modullari kabi tizimning ko’p qismini qamrab oladi. Kompleks yondashish apparat qismi tomonidan oldin erishib bo’lmagan ishonchli himoyali dasturiy yondashishning moslanuvchanligini ta’minlaydi. Bu qurilmada oldindan o’rnatilgan funksiyalar nabori bilan cheklanmay, vaqt o’tishi bilan tizimni dasturiy va xavfsiz yangilashga imkon beradi.