O’ZBEKISTON RESPUBLIKASI O'LIY VA O'RTA MAXSUS TA'LIM VAZIRLIGI

O’ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI

MUXAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

Ganiev Salim Karimovich, Kuchkarov Taxir Anvarovich

TARMOQ XAVFSIZLIGI

(MOBIL TARMOQ XAVFSIZLIGI)

(o'quv qo'llanma)

Toshkent - 2019

UDK: 681.3 004.77(057.4)
BBK: 32.973
G 01
S. K. Ganiev, T. A. Kuchkarov. Tarmoq xavfsizligi (Mobil tarmoq xavfsizligi). O'quv qo'llanma. - T.: "Aloqachi", 2019, 150 b.

Ushbu o’quv qo’llanma tayanch oliy o’quv yurti Toshkent axborot texnologiyalari universitetining “Axborot xavfsizligini ta’minlash” kafedrasi professor-o’qituvchilari tomonidan tayyorlangan bo’lib, unda mobil tarmoq infrastrukturasi, simsiz tarmoqlar, Yerning sun’iy yo’ldoshli aloqa tizimlari, mobil tizimlarda xavfsizlik tahdidlari, mobil operatsion tizim xavfsizligi, mobil ilovalardagi zaifliklar, simsiz va mobil tarmoqlar xavfsizligini ta’minlovchi texnologiyalar, mobil kommersiyada xavfsizlikni ta’minlash, bulutli hisoblashlarda axborotni himoyalash usullari, simsiz tarmoq xavfsizligining auditi va monitoringi masalalari ko’rilgan.

O’quv qo’llanma oliy o’quv yurti talabalariga, malakani oshirish guruhlari tinglovchilariga hamda simsiz va mobil tizimlar himoyasi sohasida faoliyat ko’rsatuvchilariga mo’ljallangan.

UDK: 681.3 004.77(057.4)
BBK: 32.973
G 01

Taqrizchilar:

S.S. Parsiev, TATU "Telekommunikatsiyada boshqaruv tizimlarining apparat va dasturiy ta’minoti" kafedrasi mudiri, texnika fanlari nomzodi, dotsent.

A.A. Nigmanov, "Axborot va jamoat xavfsizligi" markazi, XVR bo’limi boshlig’i, texnika fanlari nomzodi.

ISBN 978-9943-5521-2-8

MUNDARIJA

MUQADDIMA

"Axborot xavfsizligi" ta’lim yo’nalishida "Mobil tarmoq xavfsizligi" fanining mazmuni quyidagicha belgilangan: fanning maqsadi talabalarga simsiz va mobil texnologiyalar bo’yicha zamonaviy va istiqbolli nazariy va amaliy bilimlarni berish. Fanni o’rganish axborotni uzatish muhitidan foydalanish, topologiya, standartlar, texnologiyalar, xavfsizlik masalalarini o’z ichiga oladi. Shuning bilan birga axborot yaxlitligining buzilishi, simsiz va mobil axborot tarmoqlaridan ruxsatsiz foydalanish, ularning ishga layoqatligining buzilishi kabi muammolar ko’rilishi lozim.

Radioaloqa, radioelektron tizimlar, radio va optik signallarni shakllantirish va uzatish, radioto’lqinlarning tarqalishi asoslarini bilish fanni o’zlashtirishdagi dastlabki qadam hisoblanadi.

Shu sababli, o’quv qo’llanmaning *birinchi bobi* radiosignal turlari va ularning asosiy xarakteristikalariga, ko’p nurlilikning signal tarqalishi ta’siriga, chastotalar spektri taqsimotiga, ko’pchilik foydalanuvchi tizim turlariga bag’ishlangan.

Ikkinchi bobda mobil tizimlarni qurish prinsiplari, mobil tarmoq komponentlari, mobil tizimlarda chastotalar va vaqt taqsimoti strukturasi, mobil tizimlarni qurishning o’ziga xos xususiyatlari, uyali mobil tizimlarni qurish asoslari yoritilgan.

Uchinchi bob keng polosali foydalanishni ta’minlovchi lokal, shahar hamda global simsiz tizimlar va tarmoqlarni qurish masalalariga bag’ishlangan.

To’rtinchi bobda Yerning sun’iy yo’ldoshli mobil aloqa tizimlari, ularni qurish prinsiplari, strukturali va asosiy xarakteristikalari hamda Yerning sun’iy yo’ldoshli mobil aloqaning Internet texnologiyalarda ishlatilishi ko’rilgan.

Beshinchi bobda axborot xavfsizligiga tahdidlar tasnifi, mobil tizimlarda axborot xavfsizligiga asosiy tahdidlar, axborot xavfsizligini buzuvchining modeli keltirilgan.

Oltinchi bobda turli operatsion tizimlarda xavfsizlikni ta’minlash mexanizmlari ko’rilgan. Dunyoda keng tarqalgan Android va iOS operatsion tizimlar xavfsizligini ta’minlash mexanizmlarining qiyosiy tahlili keltirilgan.

Yettinchi bob mobil ilovalardagi tahdidlarga va zaifliklarga bag’ishlangan. Mobil qurilmalar uchun ilovalar tasnifi keltirilgan. Mobil

ilovalarning namunaviy zaifliklari hamda mobil ilovalarning himoyalanganligiga tahdidlarning tahlili va baholanishi ko’rilgan.

Sakkizinchi bobning mazmuni - simsiz va mobil tarmoqlarda xavfsizlikni ta’minlovchi texnologiyalar. Simsiz va mobil tarmoqlar uchun IEEE 802.11 (Wi-Fi 802.11) bazaviy standart, EAP va IEEE 802.1x standartlari, IPSec protokollari yordamida axborotni himoyalash texnologiyalari ko’rilgan. Xavfsizlikni kompleks ta’minlovchi IEEE 802.11i standarti ham keltirilgan.

To’qqizinchi bobda mobil moliya xizmatlari modellari, mobil to’lovlarni amalga oshirishdagi mavjud tahdidlar va zaifliklarning tahlili hamda mobil to’lovlardan foydalanishda axborot xavfsizligini oshirish bo’yicha tavsiyalar ko’rilgan.

O’ninchi bob mobil bulutli texnologiyalarga bag’ishlangan. Mobil ilovalarning bulutli hisoblash tizimlari bilan o’zaro ta’sir arxitekturasi, mobil texnologiyalarda bulutli hisoblashlardan foydalanish muammolari, bulutli hisoblashlar modelidagi mobil agentlarning imkoniyatlari ko’rilgan. Bulutli hisoblashlarga tahdidlar tahlili va ulardan himoyalanish usullari keltirilgan.

O’n birinchi bobda mobil tizimlar xavfsizligining auditi va monitoringi masalalari ko’rilgan.

1 BOB. RADIOALOQA XUSUSIDA QISQACHA MA’LUMOT

1.1. Radiosignal turlari va xarakteristikalari

Xabarlarni masofaga simsiz uzatish elektromagnit maydon fazosida tarqaluvchi *elektromagnit to’lqinlar (radioto’lqinlar)* yordamida amalga oshiriladi. Elektromagnit maydon – elektr va magnit maydonlari o’zgaruvchilarining majmui.

Elektr maydonining asosiy xarakteristikasi uning kuchlanganligi *E* hisoblanadi. Kuchlanganlik musbat elektr zaryadi birligiga maydon tarafidan ta’sir etuvchi kuchdan iborat. Elektr maydon kuchlanganligi maydon mavjud bo’lgan muhitning dielektrik o’tkazuvchanligi *e* ga bog’liq. *E* kattaligi ushbu muhitdagi elektr maydon kuchlanganligining vakuumdagi maydon kuchlanganligidan qanchalik farqlanishini ko’rsatadi.

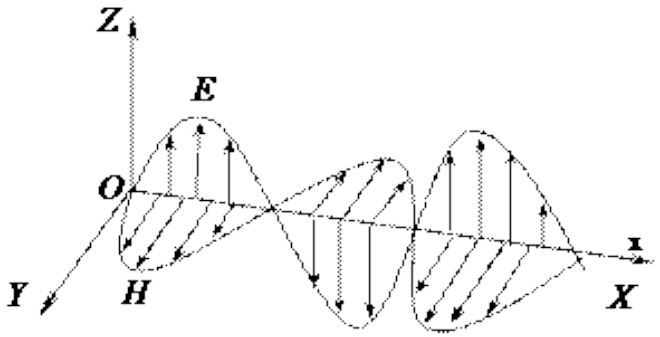
Magnit maydonining asosiy xarakteristikasi uning kuchlanganligi *N* hisoblanadi. Kuchlanganlik magnit induksiyasi *V* ning maydon mavjud bo’lgan muhitning magnit o’tkazuvchanligi *m* ga nisbatidan iborat. Magnit maydonining induksiyasi deganda magnit kuch chiziqlariga birlik tezlik bilan perpendikulyar harakatlanuvchi birlik musbat elektr zaryadiga maydon tarafidan ta’sir etuvchi kuch tushuniladi. *m* kattaligi ushbu muhitdagi magnit maydon induksiyasining vakuumdagi maydon induksiyasidan qanchalik farqlanishini ko’rsatadi.

E va *N* kattaliklari nafaqat son qiymatlari bilan, balki yo’nalishlari bilan ham xarakterlanuvchi vektor kattaliklar hisoblanadi. *E* va *N* vektorlar bir biriga va to’lqin tarqalishi yo’nalishiga perpendikulyar. *E* vektori fazosida orientirlash radioto’lqinning qutblanishini belgilaydi. Chiziqli, aylanma va elliptik qutblanishlar farqlanadi.

Agar elektr maydoni vektori *E* tarqalish chizig’i bo’ylab har bir nuqtada, qutblanish tekisligi deb ataluvchi bitta tekislikda yotsa radioto’lqin chiziqli qutblangan deb ataladi. Qutblanish tekisligining joylashishiga bog’liq holda vertikal va gorizontal qutblanish farqlanadi.

Aylanma qutblanishda elektr maydoni vektorning oxiri vaqt o’tishi bilan aylanaga aylanadi, elektr qutblanishda esa ellipsni tavsiflaydi.

1.1-rasmda OX yo’nalishida tarqaluvchi va vertikal chiziqli kutblanishga ega elektromagnit to’lqinning elektrik va magnit maydonlari quchlanishlari fazasidagi o’zgarish grafiklari tasvirlangan.



1.1–rasm. Elektromagnit to’lqin strukturasi

Radiosignallar – uzatiluvchi xabarlarni eltuvchi elektromagnit to’lqinlar yoki yuqori chastotali elektr tebranishlar. Radiosignalni hosil qilish uchun yuqori chastotali tebranishlar parametrlari berilgan qonuniyat bo’yicha o’zgaruvchi kuchlanishdan iborat boshqarish signallari yordamida o’zgartiriladi (modulyatsiyalanadi).

Modulyatsiyalanuvchi sifatida, odatda, yuqori chastotali garmonik tebranishlar ishlatiladi:

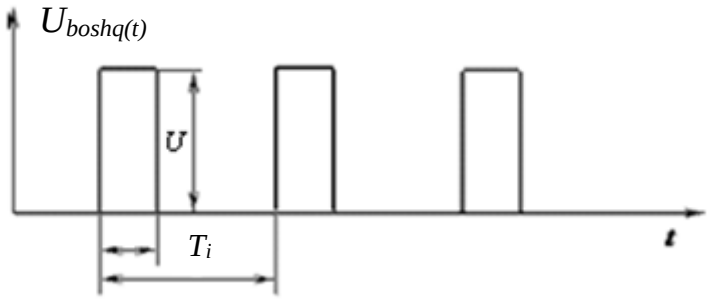
$$u(t) = U_0 \approx \sin(\omega_0 t), \qquad (1.1)$$

bu yerda $\omega_0 = 2\pi f_0$ - yuqori tutib turuvchi chastota;
U_0 - yuqori chastotali tebranishlar amplitudasi.

Eng sodda va ko’pincha ishlatiluvchi boshqarish signallariga garmonik tebranishlar tegishli:

$$U_{garm}(t) = U_m \sin(\Omega t - \Psi), \qquad (1.2.)$$

bu yerda Ω - w0 dan kichik past chastota; Ψ – boshlang’ich faza; U_m – amplituda, hamda to’g’ri burchakli impuls signallari. Ushbu signallarda impulslar davomligi deb ataluvchi vaqt intervali τ_i mobaynida kuchlanish qiymati $U_{boshq(t)} = U$, va impulslar orasidagi vaqt intervali mobaynida nulga teng (1.2 – rasm). T_i kattalik impulslarning takrorlanish davri deb ataladi; $F_i = 1/T_i$ - ularning takrorlanish chastotasi; T_i impulslarning takrorlanish davrining τi davomligiga nisbati impuls jarayonining chuqurligi (skvajnost) deb ataladi: Q = Ti/τi.



1.2 – rasm. To’g’riburchakli impulslar ketma-ketligi

Boshqarish signali yordamida yuqori chastotali tebranishning qaysi parametri o’zgartirilishiga (modulyatsiyalanishiga) bog’liq holda amplitudali, chastotali va fazali modulyatsiyalash farqlanadi (APM, ChM, FM).

Impulslar ketma-ketligini, masalan, ikkili kodni (1.3-rasm, "a") uzatishda ham APM, ChM, FM ishlatilishi mumkin.

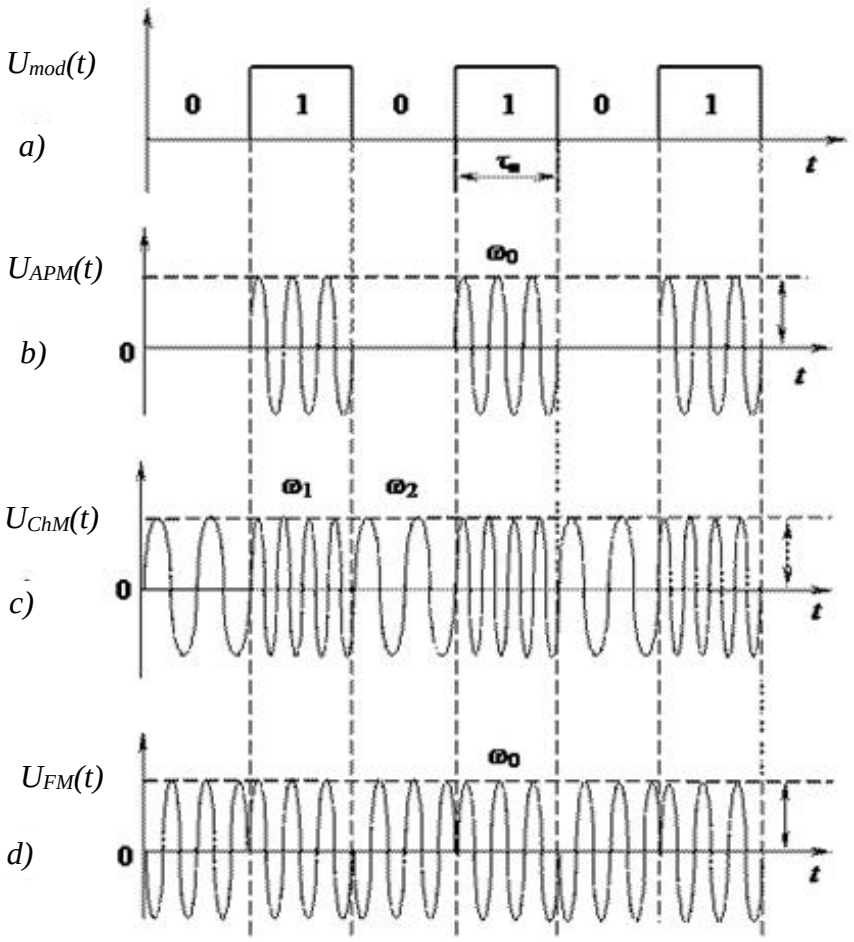
Amplitudali modulyatsiyalashda yuqori chastotali radioimpulslar hosil bo’lib, ularning amplitudasi modulyatsiyalovchi impulslar davomligi τi mobaynida o’zgarmaydi, va qolgan barcha vaqtda nulga teng (1.3 – rasm "b").

Chastotali modulyatsiyalashda o’zgarmas amplitudali va chastotasi ikkita joiz qiymatlarni oluvchi yuqori chastotali signal hosil bo’ladi (1.3 - rasm, "c").

Fazali modulyatsiyalashda amplituda va chastotasi o’zgarmas va fazasi modulyatsiyalovchi signal qonuniyati bo’yicha 180° ga o’zgaruvchi yuqori chastotali signal hosil bo’ladi (1.3 – rasm "d").

Signal peredatchikdan priyomnikgacha bo’lgan yo’lda har doim ham to’g’ri chiziq bo’yicha tarqalmaydi. Tarqalish yo’lida, odatda turli to’siqlar uchraydi. Bu to’siqlar signalning qaytarilishiga va trayektoriyasining o’zgarishiga olib keladi.

Natijada shunday vaziyat yuzaga kelishi mumkinki, priyomnikga bitta emas, balki birdaniga bir necha, vaqt bo’yicha siljigan turli amplitudali dastlabki signal nusxalari kelishi mumkin. Buning ustiga dastlabki signalning energiyasi nusxalar orasida notekis taqsimlanadi. Bu *signalning ko’p nurli tarqalishi* deb ataluvchi hodisa hisoblanadi. Mobil aloqa tizimidagi radioto’lqinlar tarqalishining ikki nurli modeli deb ataluvchi radiosignallar tarqalishining oddiy modelini ko’raylik (1.4-rasm).



1.3 – rasm. APM, ChM va FM da manipulyasiyalangan tebranishlarning qiyosiy ko'rinishi

Aytaylik, uzatuvchi va qabul qiluvchi antennalar yer sathidan, mos holda h_1 va h_2 balandlikda joylashgan. Ikkala antenna orasidagi Yer bo'ylab masofa r ga teng va ikkala antenna balandliklaridan anchagina katta. Faraz qilaylik, signal priyomnikga ikkita yo'l bilan keladi: to'g'ri (to'g'ri ko'rinish chizig'i r_1 bo'ycha) va Yerdan bitta qaytarish bilan (siniq chiziq r_2). Yer yuzasidan qaytarish yo'qotishsiz sodir bo'ladi deb qabul qilamiz, ya'ni tushuvchi to'lqin energiyasi qaytarilgan to'lqin energiyasiga teng. Bunday yondashishda priyomnik kirish yo'lidagi quvvat quyidagi ifoda bilan aniqlanishini isbotlash mumkin.

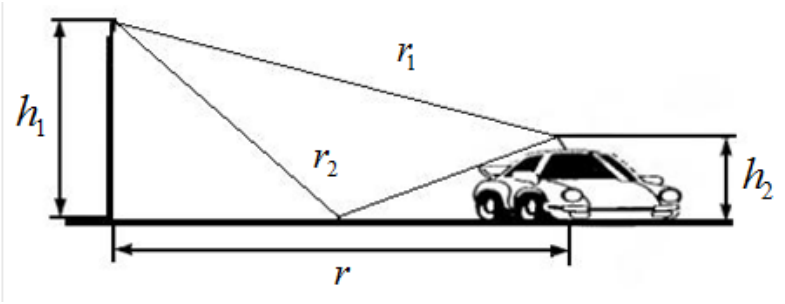
$$P_{ПРМ}(r) = G_{ПРД.А} G_{ПРМ.А} P_{ПРД} \frac{h_1^2 h_2^2}{r^4}, \qquad (1.3)$$

bu yerda:

$G_{ПРД}$ - uzatuvchi antennaning kuchaytirish koeffitsienti;

$P_{ПРД.А}$ - antennaning nurlanish quvvati;

$P_{ПРМ} = \Pi \cdot S_{э}$ - qabul qiluvchi antenna qabul qiladigan va antenna diametriga (S_d ga) bog'liq uzatuvchi antennaning nurlanish quvvatining qismi.



1.4 – rasm. Radioto'lqinlar tarqalishining ikki nurli modeli misoli

Quyida keltirilgan to'lqinlarning chastota diapazonida to'lqin uzunligi λ bir xil fazalarda tebranuvchi ikkita bir biriga eng yaqin nuqtalar orasidagi masofa (1.5-rasm).

Radioto'lqin uzunligini quyidagicha hisoblash mumkin: 300 ni (sekundagi megametrlardagi yorug'lik tezligini) megagersdagi chastotaga bo'lamiz, metrlardagi to'lqin uzunligini olamiz, masalan 600 MGs uchun to'lqin uzunligi 0,5 metrga teng.

1.2. Radioaloqani tashkil etish usullari

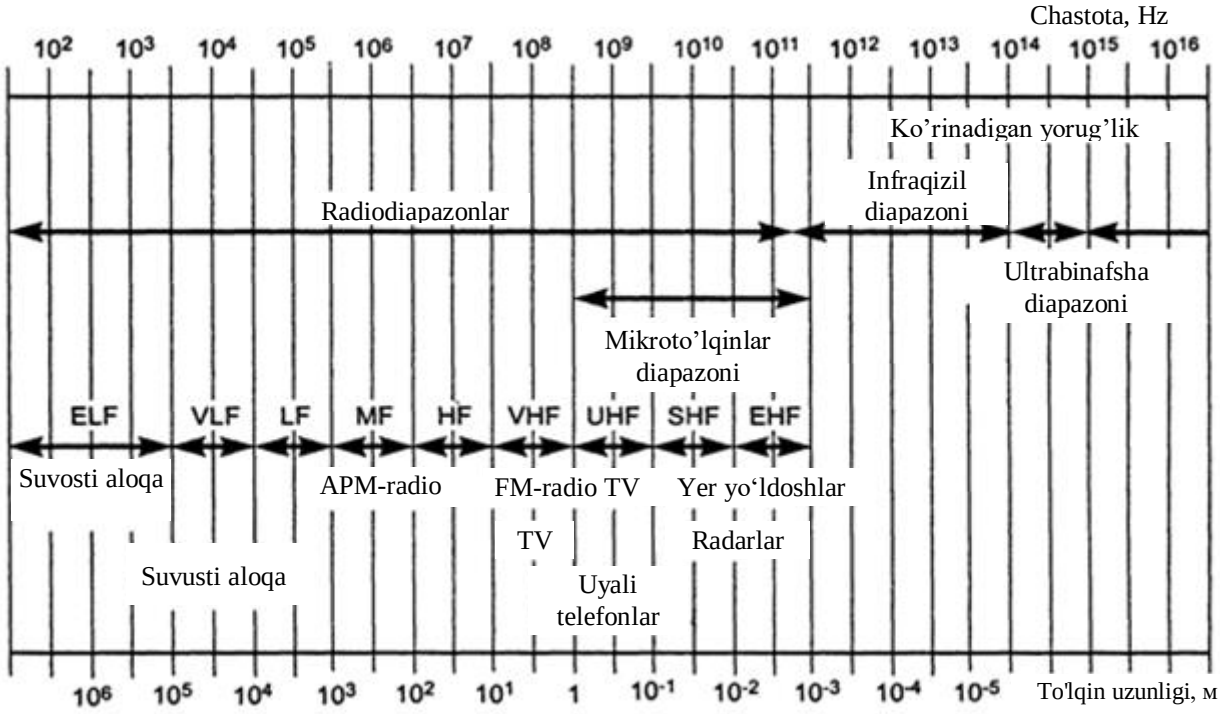
Axborotni uzatish va qabul qilish usulini tanlash va texnik amalga oshirish aloqa tizimini qurishning asosiy muammosi hisoblanadi.

Ushbu masalalar modulyatsiya va demodulyatsiya kabi jarayonlar bilan uzviy bog'langan.

Har qanday aloqa tizimi shunday loyihalanadiki, vaqt, chastota, energiya, dinamik diapazon kabi mavjud resurslardan foydalanib, eng ko'p hajmli axborotni berilgan aloqa sifati va joiz minimal energiya sarfi bilan uzatish ta'minlansin.

Hozirda axborotni analog uzatish ishlatilmaydi. Chunki zamonaviy mikroelektronika raqamli signallarni ishlashning yetarlicha murakkab algoritmlarini amalga oshirishga imkon beradi. Undan tashqari xabarlarni

uzatish sifati, boshqa barcha umumiy shartlarda, analog tizimlariga nisbatan raqamli tizimlarda yuqori.

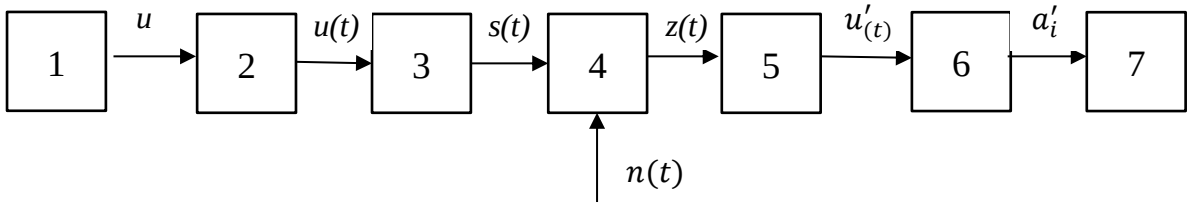


1.5 – rasm. To’lqinlarning chastota diapazoni

Raqamli tizimlarning quyidagi xususiyatlarini ko’rsatish mumkin:

- xabarlar {0,1} qiymatlarini oluvchi bitlar ketma-ketligi ko’rinishida uzatiladi;
- bitlar ketma-ketligi kanal simvollari deb ataluvchi signallarning biri bilan uzatiladi.

Xabarlarni bitta manbadan bitta qabul qiluvchiga bitta aloqa liniyasi orqali uzatishni ta’minlovchi aloqa tizimi *bir kanalli* deb yuritiladi. Bir kanalli aloqa tizimining struktura sxemasi 1.6-rasmda keltirilgan.



1.6-rasm. Bir kanalli aloqa tizimining struktura sxemasi

Bu yerda:

1 - xabar manbai - uzatiluvchi xabar u_i ni shakllantiruvchi inson yoki texnik qurilma;

2 - xabarni signalga o'zgartgich - xabarni birlamchi (past chastotali) *u(t)* signalga o'zgartiruvchi qurilma;

3 - signal o'zgartgichi (peredatchik). Birlamchi signalni aloqa liniyasi orqali uzatishga qulay ikkilamchi (yuqori chastotali) *s(t)* signalga o'zgartiruvchi qurilma;

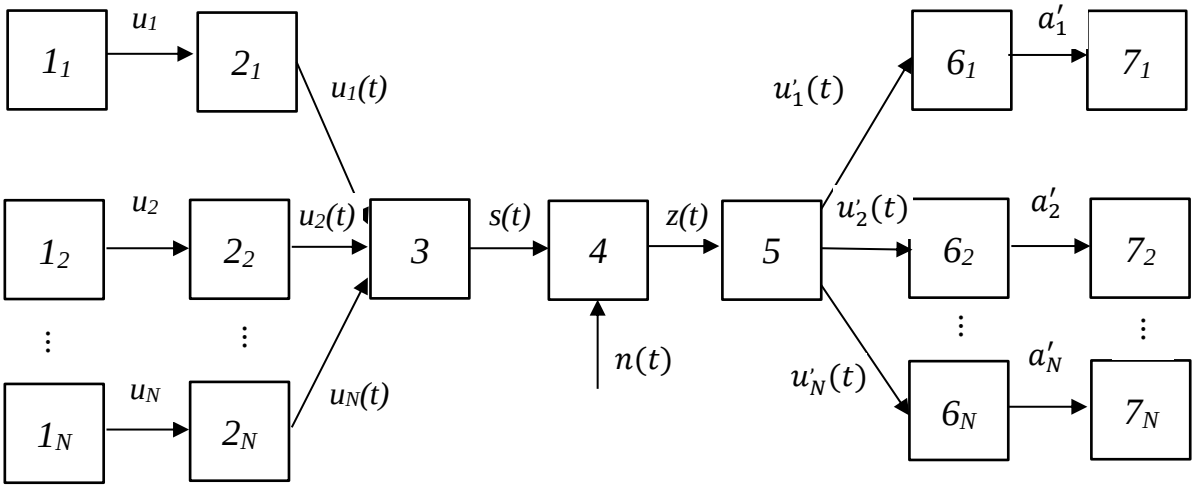
4 - aloqa liniyasi - signallarni peredatchikdan priyomnikga uzatishda foydalanuvchi muhit. Aloqa liniyasi orqali o'tishida elektr signallari $n_{(t)}$ xalallarga va buzilishlarga duchor bo'ladi. Bu aloqa liniyasining $z_{(t)}$ chiqishidagi signal va qabul qilingan a_i' xabar, mos holda, aloqa liniyasi kirishidagi signaldan va uzatiluvchi xabardan farqlanishiga olib keladi;

5 - signal o'zgartgichi (priyomnik). Qabul qilingan ikkilamchi signal bo'yicha birlamchi $u'_{(t)}$ signalni tiklaydigan qurilma;

6 - signalni xabarga o'zgartgich - birlamchi signalni qabul qilingan a_i' xabarga o'zgartiruvchi qurilma.

7 - xabarni qabul qiluvchi - xabarni o'zlashtiruvchi inson yoki qurilma.

Xabarlarni bir necha manbalardan bir necha qabul qiluvchilarga bitta umumiy aloqa liniyasi orqali bir vaqtda uzatishni ta'minlovchi aloqa tizimi *ko'p kanalli* deb yuritiladi. Ko'p kanalli aloqa tizimining struktura sxemasi 1.7-rasmda keltirilgan.



1.7-rasm. Ko'p kanalli aloqa tizimining struktura sxemasi

Bu yerda:

1_i - xabar manbai - uzatiluvchi xabar u_i ni shakllantiruvchi inson yoki texnik qurilma;

2_i - xabarni signalga o'zgartgich - xabarni birlamchi (past chastotali) $u_i(t)$ signalga o'zgartiruvchi qurilma;

3 - signal o'zgartgichi (peredatchik). Bu qurilmada birlamchi signallar kanallilariga o'zgartiriladi, so'ngra aloqa liniyasiga yo'naltiriluvchi guruh signaliga birlashtiriladi:

$$S(t) = \sum_{1=i}^{N} s_i(t), \qquad (1.4)$$

bu yerda:

$s(t)$ - kanal signallari - birlamchi signallar $u_i(t)$ bilan bir ma'noda bog'langan va qabul qilishda ajratishga imkon beruvchi ma'lum ahamiyatiga ega signallar;

N - tizimdagi kanallar soni.

4 - aloqa liniyasi - signallarni peredatchikdan priyomnikga uzatishda foydalanuvchi muhit. Aloqa liniyasi orqali o'tishda elektr signallari *n(t)* xalallarga va buzilishlarga duchor bo'ladi. Bu aloqa liniyasining *z(t)* chiqishidagi signal va qabul qilingan a_i' xabar, mos holda, aloqa liniyasi kirishidagi signaldan va uzatiluvchi xabardan farqlanishga olib keladi.

5 - signal o'zgartgichi (priyomnik). Buzilishlar va xalallar ta'sirida o'zgargan guruh signallardan kanal signallari $s_i'(t)$ ni ajratuvchi, so'ngra ularni birlamchi signallar $u_i'(t)$ ga o'zgartiruvchi qurilma.

6_i - signalni xabarga o'zgartgich - birlamchi signalni qabul qilingan a'_i xabarga o'zgartiruvchi qurilma.

7_i - xabarni qabul qiluvchi - xabarni o'zlashtiruvchi inson yoki texnik qurilma.

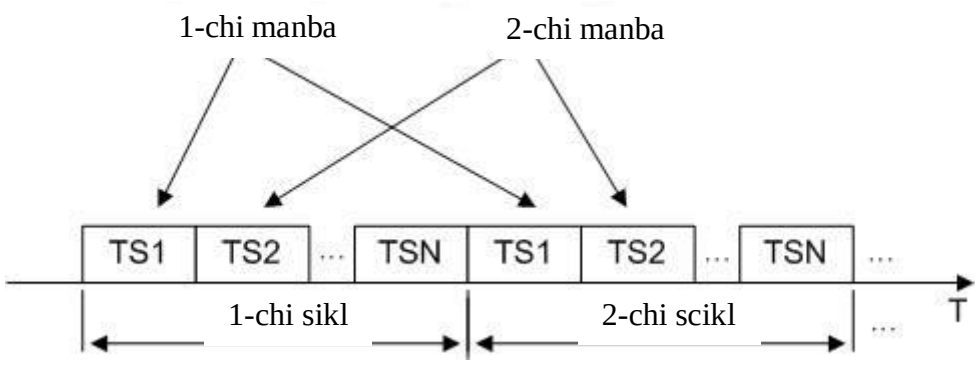
Hozirda ko'chma ob'ektli tizimlarda ko'p kanalli foydalanishning 3 ta asosiy usuli ishlatiladi:

- *TDMA* (Time Division Multiple Access) – vaqt taqsimoti bilan ko'p kanalli foydalanish;

- *FDMA* (Frequency Division Multiple Access) – chastota taqsimoti bilan ko'p kanalli foydalanish;

- *CDMA* (Code division multiple access) – kod taqsimoti bilan ko'p kanalli foydalanish.

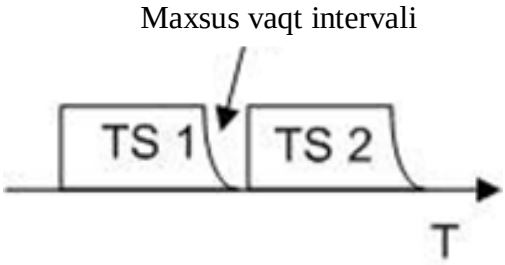
TDMA prinsipiga binoan mavjud resurs axborot almashish ishtirokchilari o'rtasida siklik qaytariluvchi vaqt oraliqlariga bo'linadi. Vaqt oraliqlari "taymslot" (timeslot, TS) nomini olgan (1.8-rasm).



1.8-rasm. TDMA sikli strukturasi

Bunda abonent kanal o’tkazish kengligining hammasidan faqat ma’lum vaqt bo’laklarida foydalanishi mumkin.

Bunday vaziyatda qo’shni taymslotlar signallari bir birining ustiga tushmasligi muhim. Bunga uzatish quvvatining haddan tashqari kattaligi, kanaldagi xalallar, ishlatiluvchi uskunaning mukammal emasligi sabab bo’lishi mumkin. Bu kabi slotlararo xalallardan qutilish uchun ko’pincha maxsus vaqt intervali kiritiladi (1.9‑rasm).



1.9-rasm. TDMA siklidagi vaqt intervali

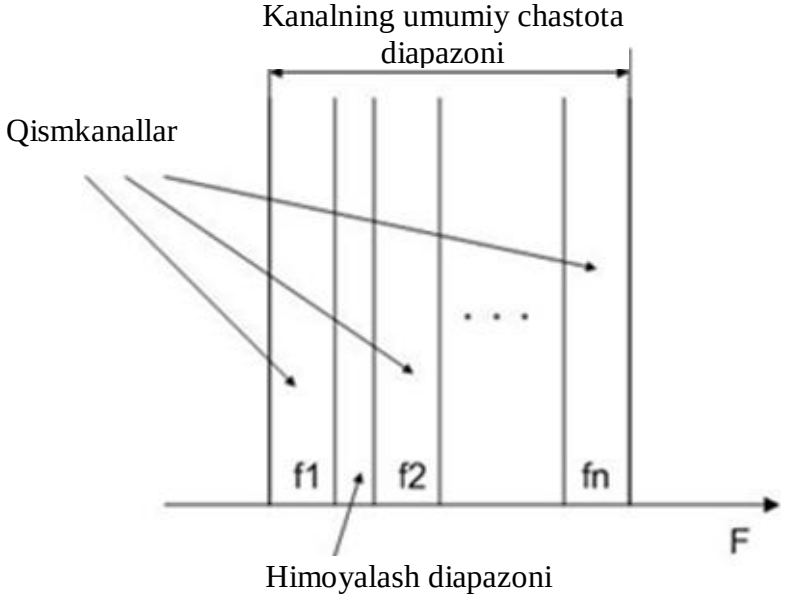
Shunday qilib, agar bitta peredatchik energiyasining qismi unga ajratilgan taymslot chegarasidan sizib o’tsa, u faqat axborot eltmaydigan himoya intervaliga ta’sir etadi. Bunday intervalning kiritilishi aloqa kanalining umumiy o’tkazish qobiliyatini pasaytirsada, xizmat sifatining berilgan xarakteristikalarini madadlash uchun zarur. *TDMA GSM* (Global System for Mobile Communication) uyali aloqa standartida ishlatiladi.

FDMA prinsipiga binoan butun chastota spektri foydalanuvchilar orasida teng yoki teng bo’lmagan chastota polosalariga bo’linadi (1.10-rasm).

Axborot manbalari ularga ajratilgan chastota resurslaridan vaqt bo’yicha istalgancha, qo’shni kanallarga xalal tug’dirmasdan

foydalanishlari mumkin. Bunday xalallardan qutilish uchun qo’shni kanallar orasida maxsus himoyalovchi chastota intervali kiritiladi. Bu chastota intervali axborotni uzatishda ishlatilmaydi va shuning uchun mavjud aloqa kanalining umumiy o’tkazish qobiliyati pasayadi.

Vaqt bo’linishi prinsipida barcha ajratilgan vaqt ishlatilmasligi kabi, chastota bo’linishi prinsipi ham butun chastota diapazonidan to’la foydalanmaydi.



1.10-rasm. *FDMA* ni tashkil etish prinsipi

Bunga sabab quyidagilar:

- uzatuvchi muhitda signal tezgina so’nishi sababli, signalni yuqori chastotali modulyatsiyalashsiz uzatish mumkin emas;
- chastotalar va vaqt ham uzatiluvchi ma’lumotlar hajmini ko’paytirish uchun ishlatiluvchi rusurslar hisoblanadi.

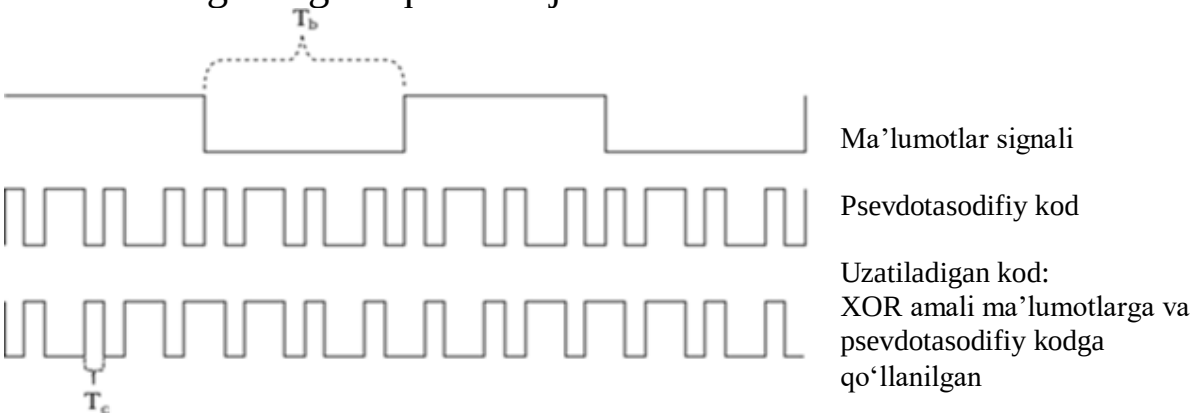
Shu sababli aloqani tashkil etishda birdaniga ikkala prinsip ishlatiladi. Masalan GSM standartida bir vaqtda TDMA va FDMA ishlatiladi. Butun chastota diapazoni har biri 200 kGs li chastota kanallariga bo’linadi, bu kanallar o’z navbatida 8 taymslotlardan tashkil topadi.

CDMA prinsipiga binoan har bir uzel uchun chastotalarning barcha spektri va vaqtning hammasi ajratiladi. Barcha peredatchiklar signallarni bir xil chastotada, fazo zonasida va vaqtning bir xil orasida, ammo turli kodlar bilan uzatadi. Har bir peredatchik ma’lumotlarning dastlabki oqimining har bir bitini CDM-simvolga, ya’ni 8, 16, 32, 64 va h.

uzunlikdagi bitlarga (ularni "chip" deb atashadi) almashtiradi. Har bir peredatchik uchun psevdotasodifiy kodlar ketma-ketligi noyob hisoblanadi. Odatda, ma’lumotlarning dastlabki oqimida "1" ni almashtirish uchun qandaydir CDM-kod ishlatilsa, "0" ni almashtirish uchun aynan o’sha, ammo invertirlangan, kod ishlatiladi. Priyomnik signalini qabul qilishi lozim bo’lgan peredatchikning CDM-kodini biladi. Muhitning bunday bo’linish usulida trafik kanallari keng polosali kodli modulyatsiyalangan radiosignal, ya’ni keng chastotali diapazonda uzatiluvchi shovqinga o’xshash signal yordamida hosil qilinadi (1.11-rasm).

Bir necha peredatchiklar ishlaganida ushbu chastota diapazonidagi efir yanada shovqinga o’xshash bo’ladi.

Har bir peredatchik, ushbu onda har bir foydalanuvchiga berilgan alohida son kodidan foydalanib, signalni modulyatsiyalaydi. Aynan ushbu kodga sozlangan priyomnik radiosignallarning umumiy kakofonidan ushbu priyomnikka atalgan signal qismini ajratib olishi mumkin.



1.11-rasm. CDMA signalining generatsiyasi

Ushbu prinsipda *TDMA* yoki *FDMA* ga o’xshash kanallarning vaqtiy yoki chastotali bo’linishi mavjud emas, har bir abonent signalni umumiy chastota diapazoniga uzatib va umumiy chastota diapazonidan qabul qilib, kanalning barcha kengligini muntazam ishlatadi. Bunda uzatish va qabul qilishning keng polosali kanallari turli chastota diapazonida joylashgan va bir-biriga xalaqit bermaydi.

Yuqoridagi qayd etilganlar *CDMA* prinsipining yuqori samaradorligidan darak beradi. Haqiqatan, ushbu prinsipda qo’llanuvchi kod bo’linishi *TDMA*, *FDMA* prinsiplaridagiga nisbatan ko’proq abonentlarga xizmat qilishga imkon beradi. Kod bo’linishida kanallar soniga qat’iy cheklash mavjud emas. Abonentlar soni oshishi bilan dekodlash xatoliklarining oshishi ehtimoli oshadi. Bu kanal sifatini

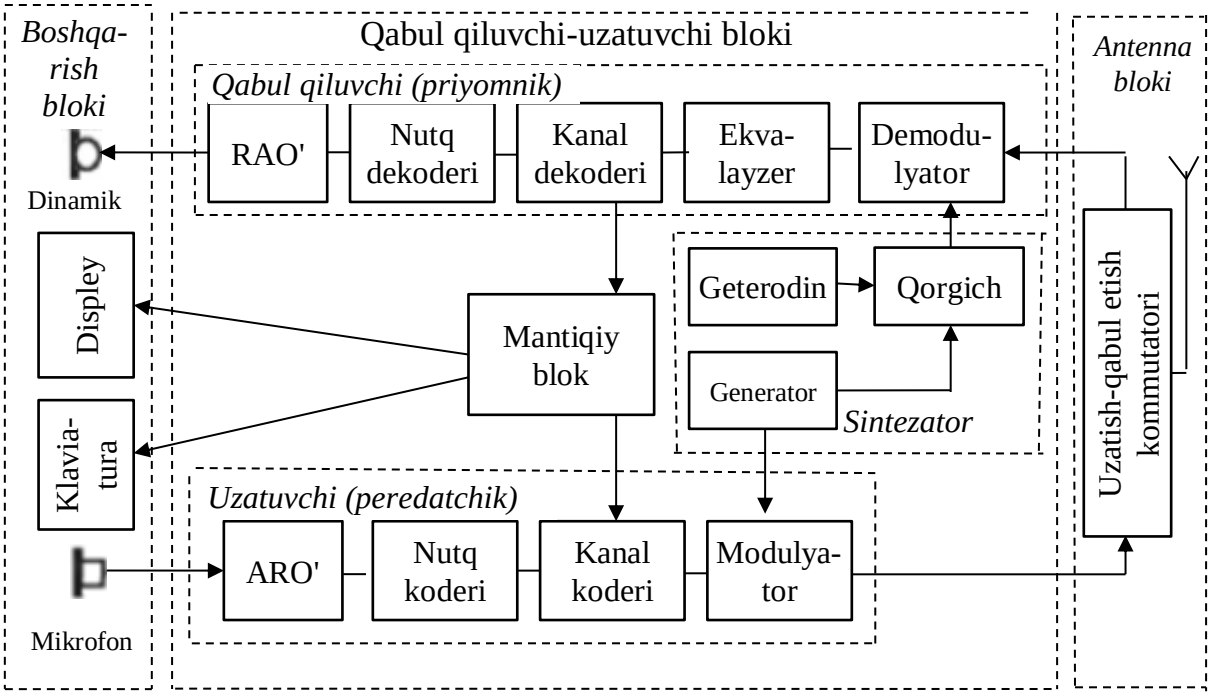
pasaytirishga olib kelsada, xizmatdan voz kechishga sabab bo’lmaydi. CDMA prinsipi kanallarning yuqori himoyalanganligiga ega. Kerakli kanalni ajratish, uning kodini bilmasdan mumkin emas. CDMA telefonlari nurlanishning kichik avj quvvatiga ega va, shuning uchun, zararsizroq.

2 BOB. MOBIL TARMOQ INFRASTRUKTURASI

2.1. Mobil tarmoq komponentlari

Mobil tarmoqning asosiy komponentlari - raqamli mobil stansiya, bazaviy stansiya va kommutatsiyalash markazi.

Raqamli mobil stansiyaning, boshqacha aytganda, zamonaviy mobil telefonning soddalashtirilgan blok-sxemasi 2.1-rasmda keltirilgan.



2.1-rasm. Raqamli mobil stansiyaning blok-sxemasi

Boshqarish bloki tarkibiga mikrofon va dinamik, klaviatura va displey kiradi. Klaviatura chaqiriluvchi abonent telefoni hamda stansiya ishlashi rejimini belgilovchi komandalar nomerini terishga mo'ljallangan. Displey axborotni akslantirish uchun mo'ljallangan.

Qabul qiluvchi va uzatuvchi blok peredatchik, priyomnik, chastotalar sintezatori va mantiqiy blokdan tashkil topgan.

Peredatchik tarkibiga quyidagilar kiradi:

- analog-raqam o'zgartirgichi (ARO') – mikrofon chiqish yo'lidagi signalni raqamli shaklga o'zgartiradi;

- nutq koderi – nutq signalini kodlashni amalga oshiradi, ya'ni raqamli signalning ortiqchaligini qisqartirish maqsadida uni o'zgartiradi;

- kanal koderi – xatoliklardan himoyalanish maqsadida radiokanal bo’yicha uzatiluvchi signalni kodlaydi, hamda uzatiluvchi signal tarkibiga mantiqiy blokdan keluvchi boshqarish axborot signalini kiritadi;

- modulyator – kodlangan signal axborotini eltuvchi chastotaga o’tkazadi.

Priyomnik tarkibiga quyidagilar kiradi:

- demodulyator – modulyatsiyalangan radiosignaldan axborot eltuvchi kodlangan videosignalni ajratadi;

- ekvalayzer – ko’p nurli tarqalish hisobiga signal buzilishini kompensatsiyalash uchun mo’ljallangan;

- kanal dekoderi – qabul qilingan signaldagi xatoliklarni aniqlaydi va tuzatadi, hamda kirish yo’li oqimidan boshqarish axborotini ajratadi va mantiqiy blokka yuboradi;

- nutq dekoderi – nutq signalini raqamli ko’rinishga tiklaydi;

- raqam-analog o’zgartirgichi (RAO’) – qabul qilingan nutqning raqamli signalini analog shaklga o’zgartiradi va uni dinamik kirish yo’liga uzatadi;

- mantiqiy blok – mobil stansiya ishlashini boshqaruvchi mikrokompyuter.

Antenna bloki – odatda mobil qurilma ichida joylashgan antenna va qabul qiluvchi–uzatuvchi elektron kommutatoridan iborat. Elektron kommutator antennani peredatchik chiqish yo’liga yoki priyomnikning kirish yo’liga ulaydi, chunki raqamli tizimning mobil stansiyasi bir vaqtning o’zida qabulga va uzatishga hech qachon ishlamaydi.

Ba’zi tizimlarda axborotni uzatish konfidensialligini ta’minlash maqsadida shifrlash rejimidan foydalaniladi. Bunda, mos holda, xabarlarni shifrlash va deshifrlash bloklari ko’zda tutiladi.

Mobil stansiyada abonentni identifikatsiyalovchi maxsus olib qo’yiladigan blok (Subsriber Identity Module – SIM) ham ko’zda tutilgan. Mobil stansiyada nutq aktivligi detektori VAD (Voice Activity Detectog) ham mavjud. VAD peredatchikni nurlanishga faqat abonent so’zlagan vaqt intervalida ulaydi. Natijada ta’minot manbai energiyasi tejaladi, ishlab turgan peredatchikda boshqa stansiyalarga tug’diriluvchi xalallar darajasi pasayadi.

Bazaviy stansiyada qabul qilish sifatini oshirish uchun ajratilgan usuli qo’llaniladi. Bu mobil abonentlar bilan bog’lanishni tashkil etish xususiyatlaridan biri hisoblanadi va bazaviy stansiyalarda ikkitadan kam bo’lmagan qabul qiluvchi antennalar o’rnatilishiga sabab bo’ladi. Undan

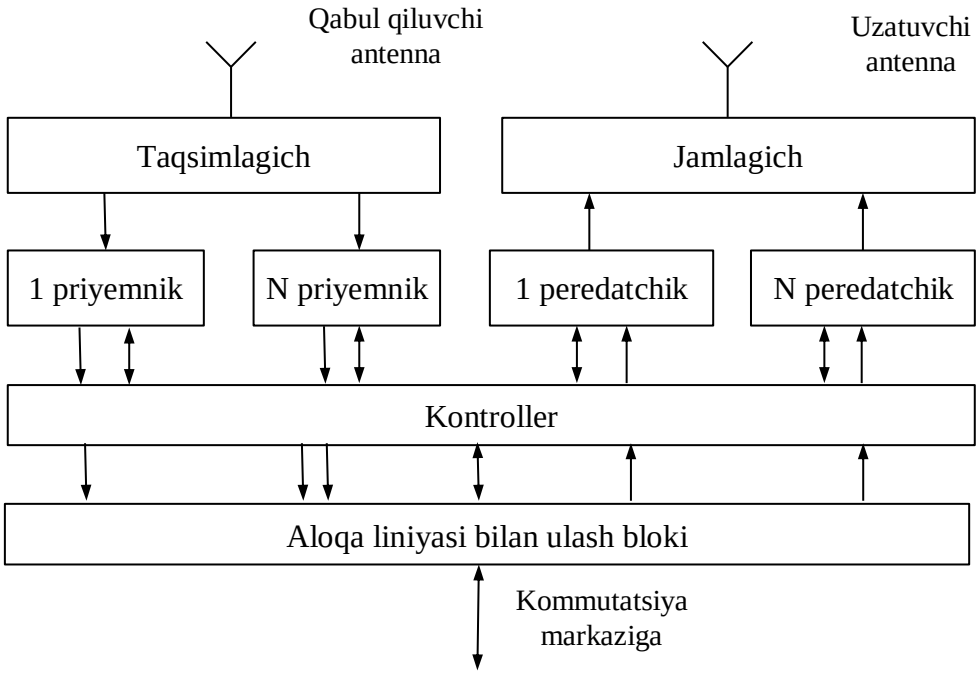
tashqari bazaviy stansiya uzatishga va qabul qilishga alohida antennalarga ega bo'lishi mumkin. Bazaviy stansiyaning yana bir xususiyati – turli chastotali bir necha kanallarda bir vaqtda ishlashni ta'minlash uchun bir necha priyomniklarning va shunday sonli peredatchiklarning mavjudligi. Bazaviy stansiyaning blok-sxemasi 2.2-rasmda keltirilgan.

Qabul qiluvchi va uzatuvchilar soni *N* bazaviy stansiyaning konstruksiyasi va komplektligi orqali aniqlanadi. *N* priyomniklarni bitta qabul qiluvchi antennaga bir vaqtda ishlashini ta'minlash uchun qabul qiluvchi antenna va priyomniklar orasida *N* chiqish yo'lli quvvat taqsimlagichi, peredatchiklar va uzatuvchi antenna orasida esa *N* kirish yo'lli quvvat jamlagichi o'rnatiladi.

Bazaviy stansiya kontrolleri (kompyuteri) (BSK) stansiya ishlashini boshqarishni, hamda uning tarkibidagi bloklar va uzellarning ishga layoqatligini nazoratlashni ta'minlaydi.

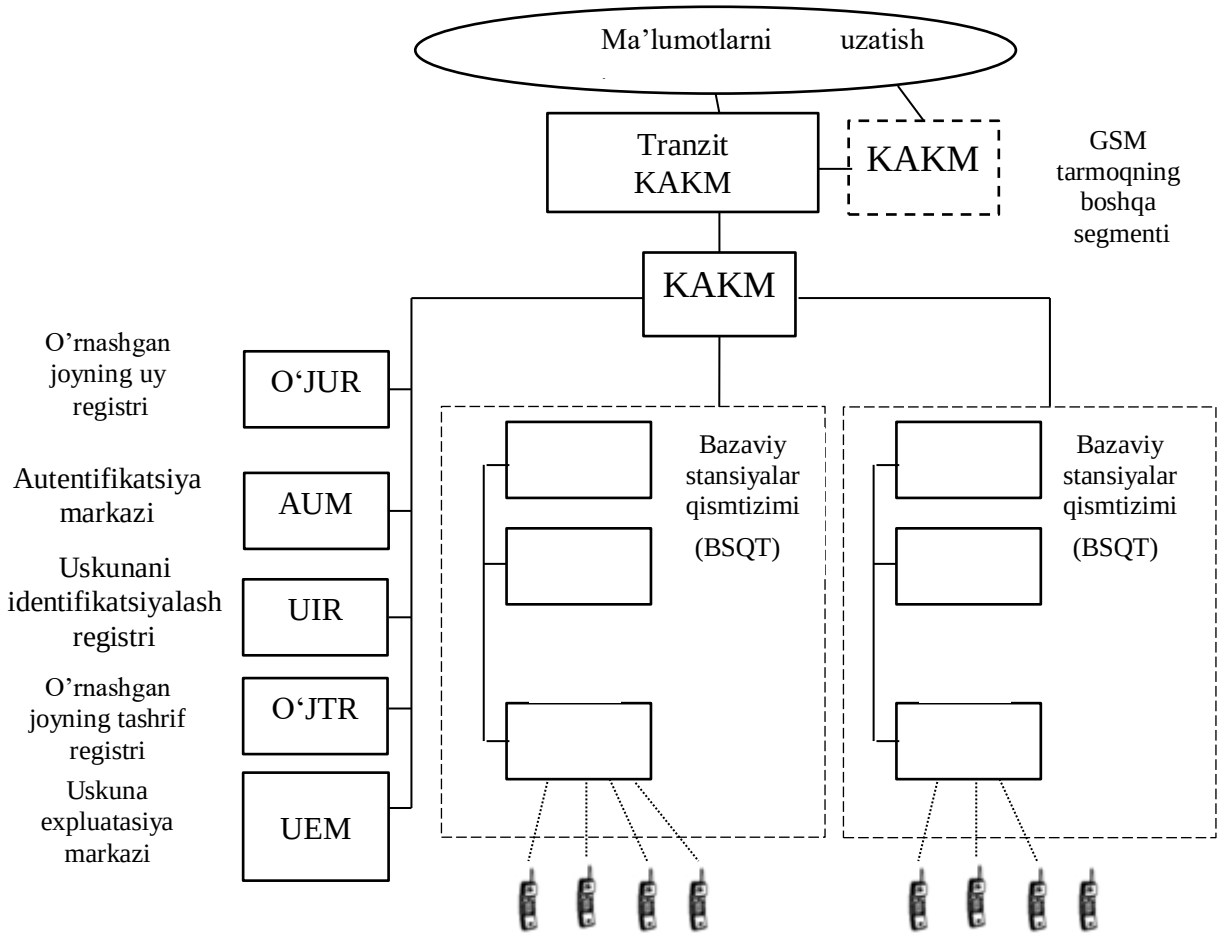
Aloqa liniyasi bilan bog'lovchi blok ko'chma aloqani kommutatsiyalash markaziga aloqa liniyasi bo'yicha axborotni uzatadi va qabul qiladi. Bazaviy stansiyani ko'chma aloqani kommutatsiyalash markazi bilan bog'lashda radiorele yoki optik-tola liniyasidan foydalaniladi.

Ishonchlikni ta'minlash uchun bazaviy stansiyaning ko'pgina bloklari va uzellari rezervlanadi (ikkilanadi), stansiya tarkibiga avtonom uzluksiz ta'minot (akkumulyatorlar) kiritiladi.



2.2-rasm. Bazaviy stansiyaning blok-sxemasi

Ko’chma aloqani kommutatsiyalash markazi (KAKM) elektron kommutatsiyaning ixtisoslashtirilgan markazi bo’lib, unga uyali ko’chma aloqa tizimiga xarakterli masalalarni hal etuvchi funksional bloklar (registrlar) qo’shilgan (2.3-rasm).



2.3-rasm. Ko’chma aloqani kommutatsiyalash markazining blok-sxemasi

O’rnashgan joyning uy registri (O’JUR) – muayyan operator tizimida doimiy ro’yxatga olingan ko’chma stansiyalarning ma’lumotlar bazasi joylashgan registr. Tarkibida har bir operatorga taqdim etiluvchi xizmatlar nabori xususidagi axborot ham mavjud. Ushbu registrda abonentni chaqirishni tashkil etish uchun uning joylashgan joyi qaydlanadi va haqiqatan ko’rsatilgan xizmatlar ro’yxatga olinadi.

Autentifikatsiya markazi (AUM) – ma’lumotlar bazasini autentifikatsiyalash markazi bo’lib, haqiqiylik moduliga - SIM-kartaga

(Subscriber Identity Module) ega abonentga tizim xizmatidan foydalanish ruxsat etilganligini aniqlashga imkon beradi.

Uskunani identifikatsiyalash registri (UIR) – tizimda ishlatiluvchi ko'chma stansiyalarning seriya nomerlarining ma'lumotlar bazasini identifikatsiyalovchi registr. O'g'irlangan yoki yo'qotilgan telefonlar nomeri *qora ro'yxatga* joylashtiriladi. Bu ushbu telefonlarni keyinchalik tizimda ishlatilmaslikka imkon beradi.

O'rnashgan joyning tashrif registri (O'JTR) – tarkibida berilgan operatorga xizmat ko'rsatish hududida (rouming) vaqtincha joylashgan ko'chma stansiyalar xususidagi kerakli axborot bo'lgan registr.

Uskuna ekspluatatsiyasi markazi (UEM) tarmoqning alohida elementlari ishlashini ta'minlaydi.

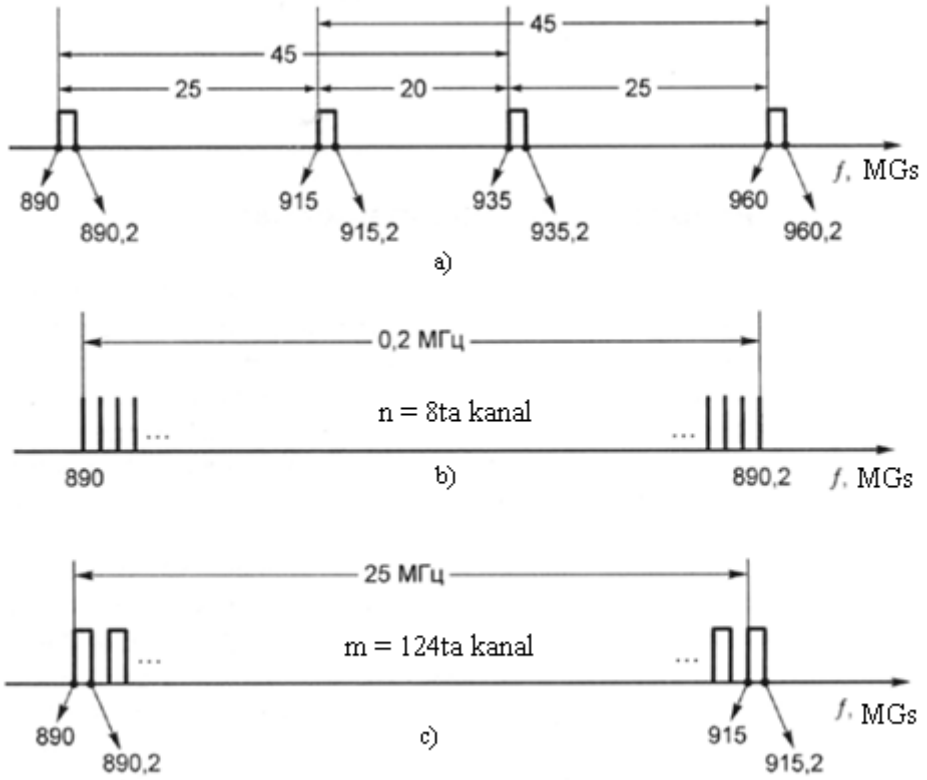
Tarmoqdagi barcha aloqani kommutatsiyalash markazlari bir-biri bilan bog'langan. Har bir ko'chma aloqani kommutatsiyalash markazi bitta yoki bir necha bazaviy stansiya qismtizimlarini (BSQT) nazoratlaydi. Ko'chma aloqani kommutatsiyalash markazining asosiy vazifasi tizimning ikkita mobil abonentlari orasida yoki bitta tizimdan foydalanuvchi va tashqi tarmoq abonenti orasida ulanish o'rnatilishini muvofiqlashtirishdan iborat.

2.2. Mobil tizimda chastotalar va vaqt taqsimotining strukturasi

Chastotalar taqsimoti strukturasini GSM-900 (Global Sistem Mobile Communication) misolida ko'ramiz, chunki aynan u GSMning bazaviy spetsifikatsiyasi hisoblanadi. Standart har biri 25 MGs kengligidagi ikkita chastotalar diapazonida ishlashni ko'zda tutadi (2.4-rasm):

- chastotalar polosasi 890-915 MGs – xabarlarni mobil stansiyadan bazaviy stansiyaga uzatish (MS-BS) uchun (uplink);
- chastotalar polosasi 935-960 MGs – xabarlarni bazaviy stansiyadan mobil stansiyaga uzatish (BS-MS) uchun (downlink).

Ko'rinib turibdiki, ma'lumotlarni dupleks uzatish *FDD (Frequency Division Duplex - chastota taqsimotli dupleks uzatish)* rejimida amalga oshiriladi. Aloqa seansi vaqtida kanallarning o'zgarishida ushbu chastotalar orasidagi (ikkita diapazon orasidagi, qo'shni chastotalar orasidagi emas) farq o'zgarmaydi va 45 MGs ga teng. Qo'shni kanallar orasidagi chastotalar farqi 200 KGs ni tashkil etadi. Shunday qilib, qabul qilish/uzatish uchun ajratilgan 25 MGs kengligidagi chastota polosasida aloqaning 124 ta kanali joylashadi.



2.4-rasm. a) MS-BS va BS-MS yo'nalishlaridagi chastotalar orasidagi farq; b) dupleks radiokanalidagi fizik nutqiy radiokanallar soni; c) fizik dupleks nutqiy radiokanallar soni.

GSM standartida ko'p stansiyali foydalanish FDMA/TDMA, ya'ni kanallarning chastota-vaqt taqsimoti ishlatiladi. Bu esa bitta eltuvchi chastotada bir vaqtning o'zida 8ta nutqiy kanallarni joylashtirishga imkon beradi.

GSM standartida vaqt birligi *slot* deb ataladi. Sakkizta vaqt sloti *kadr*ni tashkil etadi.

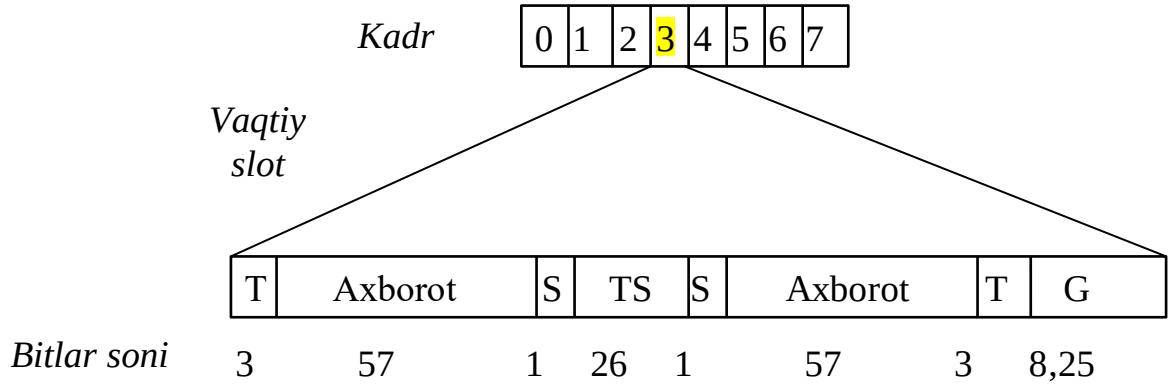
Signallarning vaqt slotida qanday taqsimlanishini ko'raylik. GSM tizimining eng kichik vaqt elementi – 3,69 mks davom etuvchi yakka impuls (bit). GSM tizimida ma'lumotlarni uzatish tezligi 270,833 Kbit/s ni tashkil etadi. Har bir vaqt slotida 148 bitli paket uzatiladi. Standart vaqt slotining davomligi 577 mks ni tashkil etadi. Slotning fizik uzunligi bilan paketning samarali uzunligi orasidagi farq *himoya intervali* deb ataladi. Uning mavjudligi xar bir ma'lumotlar paketini uzatishning boshlanishida va oxirida peredatchik quvvatini kuchaytirgichini ulash/o'chirish uchun vaqtni rezervlash zarurligi bilan bog'liq. Undan tashqari, himoya intervali vaqt sloti ichiga ma'lumotlar paketining aniq joylanishini ta'minlash

uchun zarur. Har bir slot o’zining nutq kanaliga mos, ya’ni har bir kadrda sakkizta nutq kanallari axboroti uzatiladi (2.5-rasm).

Vaqt slotining strukturasi quydagilardan tashkil topgan:

T - Tail bit (oxirgi bitlar). Ikki marta qaytariladi. Paket chetlari bo’yicha himoya oralig’i sifatida zarur.

S - Stealing flag (yashirin bayroqchalar). Ikki marta qaytariladi. Uzatiluvchi axborot xilini aniqlaydi, chunki u foydalanuvchi yoki xizmatchi bo’lishi mumkin.



2.5-rasm. Vaqt slotidagi axborot mazmuni

TS - Training Sequence (o’rganuvchi ketma-ketlik). Aloqa sifatini baholashga, bazaviy stansiya bilan mobil stansiya orasidagi axborot kechikishini aniqlashga mo’ljallangan.

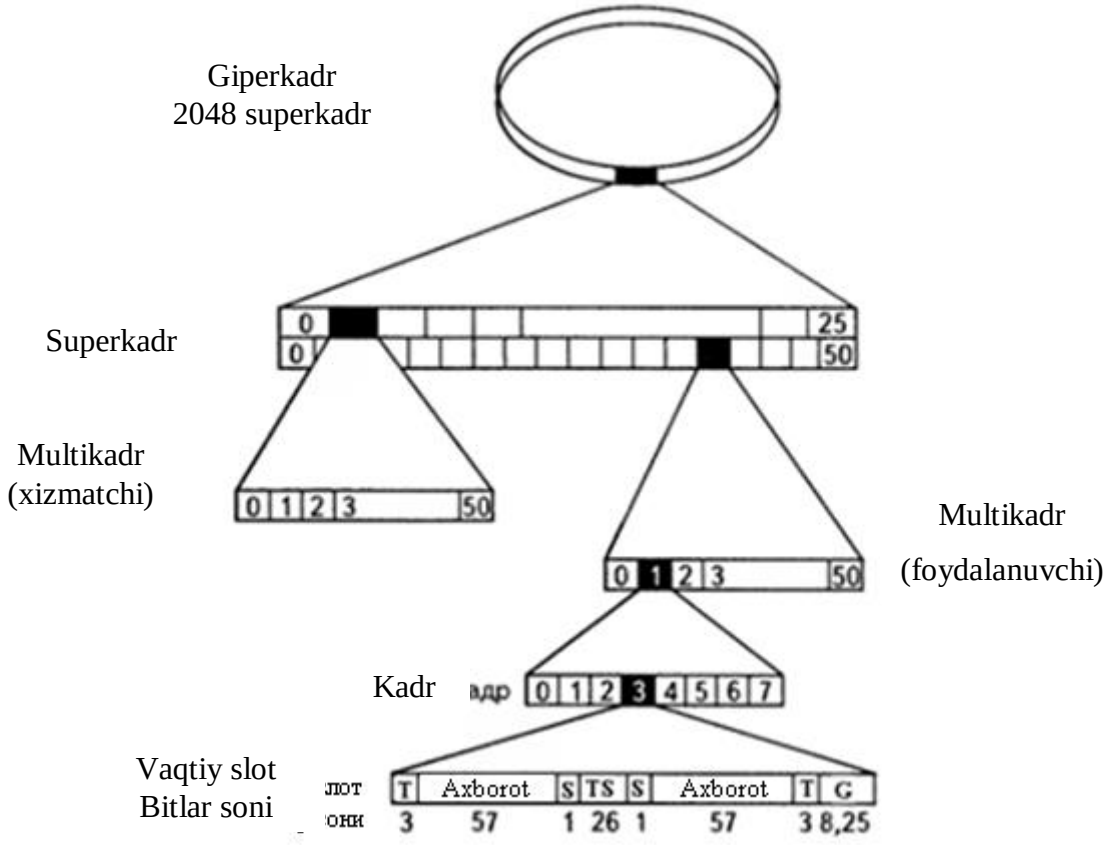
G- Guard period (himoya intervali). Trafik kanallarida (foydalaniluvchi kadr) va u bilan assotsiatsiyalangan boshqarish kanallarida (xizmatchi kadr) 26 ta kadr multikadrni tashkil etadi. O’z navbatida 51 ta kadr multikadr 6,12 s davomli superkadrni hosil qiladi. Ikkali holda 2048 ta superkadr giperkadrni, ya’ni GSM tizimning vaqt ierarxiyasining eng yuqori sathini hosil qiladi (2.6-rasm). U 3 soat 28 min 760 ms davom etadi. Ushbu vaqt o’tishi bilan tizim soatlari o’zining dastlabki holatiga qaytadi.

2.3. Mobil tarmoqlarni qurishning o’ziga xos xususiyatlari

Real sharoitlarda uyali tizimda mobil stansiyalarning notekis taqsimlanishi yuz beradi. Undan tashqari abonentlar ehtiyoji vaqt va fazo

bo’yicha o’zgaradi. Ushbu muammo uyali tarmoq ko’lamini orttirish yo’li bilan hal etiladi. Uyali tarmoq ko’lamini orttirishda kanallarni taqsimlash usullaridan foydalaniladi. 2.7-rasmda kanallarni taqsimlash usullarining tasnifi keltirilgan.

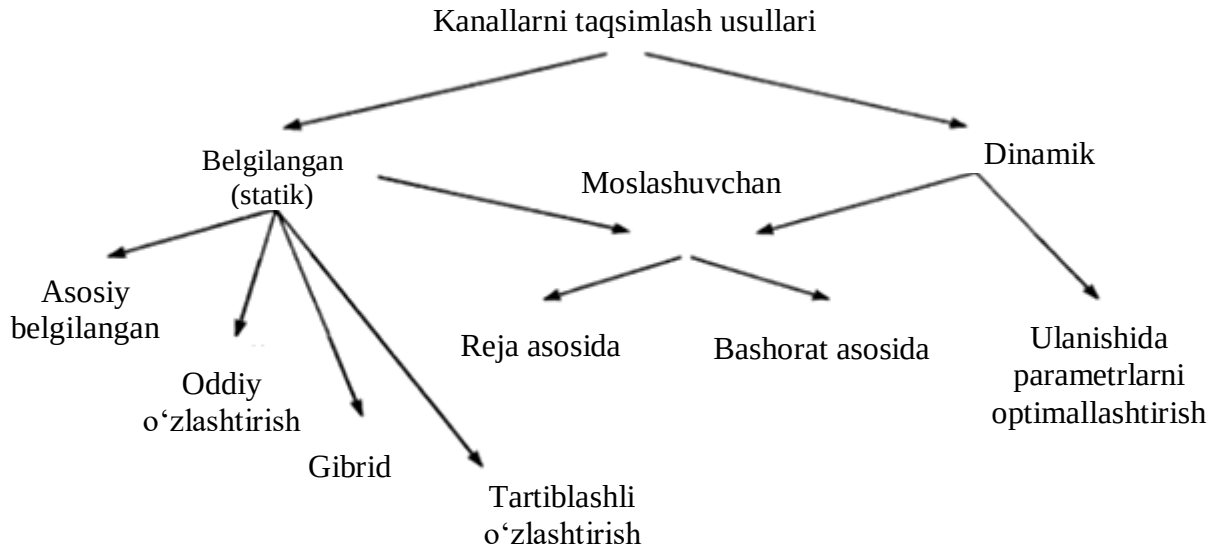
Kanallarni belgilangan (statik) taqsimlash – tizim resurslarini taqsimlashning eng sodda usuli hisoblanadi. Ushbu usulga binoan berilgan uyada yangi ulanishni faqat unda bo’sh kanallar bo’lganida o’rnatish mumkin. Shu sababli, kanallarni belgilangan taqsimlash yuklamaning eng yuqori vaqtlarida blokirovkalash ehtimolligining oshishiga olib keluvchi samarasiz yechim bo’lishi mumkin.



2.6-rasm. GSM misolida mobil tizimning vaqt strukturasi

Kanallarni oddiy o’zlashtirish usuli belgilangan taqsimlashning asosiy strategiyasini yaxshilangan varianti bo’lib, unga ozgina dinamika qo’shilgan. Agar muayyan uyaga ajratilgan barcha kanallar band bo’lsa, bo’sh kanalni qo’shni uyadan olish mumkin. Berilgan uyaning bo’sh kanaldan foydalanish onidan boshlab, kanallararo va kanallar ichidagi xalallardan qutilish uchun, o’zlashtirilgan kanaldan atrofdagi qator uyalarning foydalanishi man etiladi. Ushbu strategiyani qo’llash tufayli

blokirovkalash ehtimolligi, trafik jadalligi orqali aniqlanuvchi ma’lum bo’sag’a darajagacha kamayadi.



2.7-rasm. Kanallarni taqsimlash usullarining tasnifi

Kanallarni gibrid taqsimlash usuli oldingi usulning kamchiliklarini bartaraf etadi. Ushbu usulda har bir uyadagi kanallar ikkita kategoriyaga bo’linadi: birinchi kategoriyaga faqat berilgan uyada ishlatiluvchi kanallar kiradi; ikkinchi kategoriyaga o’zlashtirilishi mumkin bo’lgan kanallar kiradi. Ikkala kategoriyadagi kanallar nisbati kutiluvchi trafik asosida aniqlanadi.

Tartiblashli o’zlashtirish usulida har bir kategoriyaga kiruvchi kanallar soni trafik hajmiga bog’liq holda dinamik o’zgaradi. O’zlashtirilishi lozim bo’lgan har bir kanalga o’zlashtirish ehtimolligi beriladi. Kanallar ushbu ehtimollikning kamayishi tartibida saralanadi. Ehtimolliklar qiymati o’zlashtirilgan kanallar soni xususidagi ma’lumotga asosan yangilanadi.

Kanallarni dinamik taqsimlash usulida uyalarga doimo biriktirilgan kanallar mavjud emas. Kanallar muayyan ulanishga yoki ketma-ket bir necha ulanishga ajratiladi. Kanalni ajratish xususidagi qaror kommunikatsiya markazi yoki mobil stansiya tomonidan qabul qilinadi. Birinchi holda markaziy boshqarish xususida so’z boradi; ikkinchi holda

kanallarni ajratish jarayonini taqsimlangan boshqarish xususida so’z boradi.

Kanallar ulanishida parametrlarni optimallashtirish usuli kanallarni taqsimlash strategiyasini aniqlashga asoslangan. Ushbu strategiya tizimning ba’zi parametrlarini, kanallardan qayta foydalanishni hisobga olgan holda, optimallashtirish lozim.

Kanallarni moslanuvchan taqsimlash usuli o’zida belgilangan va dinamik taqsimlashlarning afzalliklarini mujassamlantiradi. Har bir uya o’z ixtiyorida o’rtacha jadallikka ega trafikga xizmat qilishga yetarli kanallar naboriga ega.

Kanallarni rejalashtirishli moslanuvchan taqsimlash usulida qo’shimcha kanallarni ajratish oldindan, sutka vaqtini va uyaning o’rnashgan joyini hisobga olgan holda, rejalashtiriladi. Kanallarni taqsimlash trafik jadalligining kritik o’sishidan oldingi, barvaqt o’rnatilgan onlarda o’zgaradi.

Kanallarni bashoratli moslanuvchan taqsimlash usulida trafik jadalligi vaqtning real rejimida o’lchanadi va ko’chma aloqani kommutatsiyalash markazi vaqtning ixtiyoriy onida kanallarni qayta taqsimlashi mumkin.

Modellash va tahlillash natijalari shuni ko’rsatadiki, trafikning kichik jadalligida dinamik taqsimlash belgilangan taqsimlashga nisbatan yaxshi natija beradi. Ammo, belgilangan taqsimlash, trafikning katta hajmi va ko’chma stansiyalarning tizimni qamrab oluvchi zona bo’yicha bir tekis taqsimlash sharoitida, o’zining afzalligini ko’rsatdi. Belgilangan taqsimlashda kanallar shunday ajratiladiki, ularni maksimal ko’p marta ishlatilishi ta’minlansin. Bunga dinamik taqsimlash holida erishish mumkin.

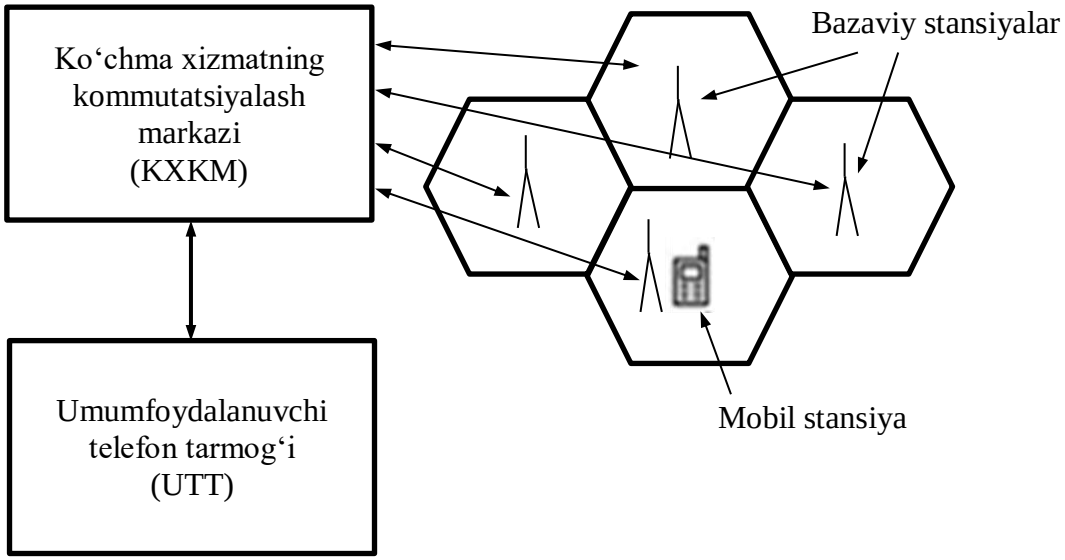
Yuqorida keltirilgan kanallarni taqsimlash usullari maxsus adabiyotlarda keltirilgan kanallarni taqsimlash usullarining turli-tumanligi xususidagi umumiy tasavvurni beradi, xolos.

2.4. Mobil tarmoqlarni qurish prinsiplari

Mobil yoki ko’chma radioaloqaning professional tizimlari PMR (Professional Mobile Radio) – radiokanaldan aloqa kanali sifatida foydalanuvchi va qo’lda ko’tarib yuradigan foydalanish terminallarini ishlatishni ko’zda tutuvchi telekommunikatsiya tizimlari.

Odatda, ular tarmoqning radiokanal yoki radial zonali (uyali) strukturaga ega va simpleks (bir tomonlama) va dupleks (ikki tomonlama) aloqa kanallaridan foydalanishlari mumkin. Turli funksional tarkibli va atalishi bo'yicha ko'pgina mobil aloqa tizimlari mavjud. Xalqaro talqinda umumlashgan tasniflash uchun "ko'chma xizmat aloqa tizimi" (sistema svyazi podvijnoy slujbы, SSPS) atamasi ishlatiladi.

Umumfoydalanuvchi ko'chma xizmat aloqa tizimi ikki sathli tarkibli telekommunikatsiya tarmog'i hisoblanadi: mobil radioaloqa tizimi (birinchi sath) va umumfoydalanuvchi telefon tarmog'i (ikkinchi sath) (2.8-rasm).



2.8-rasm. Ko'chma xizmat aloqa tizimi strukturasi

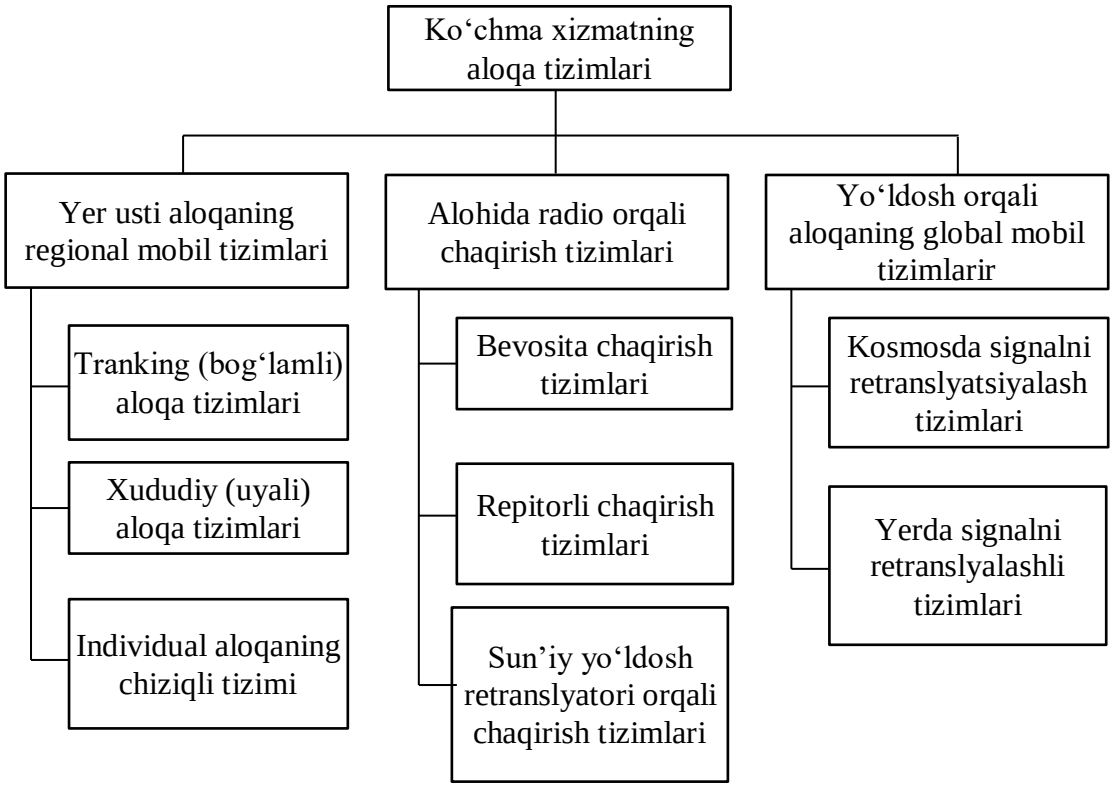
Ikki sathli telekommunikatsiya tarmog'i axborotni kommutatsiyalash va taqsimlash vazifasini tarkibiy qismlarning har birida ta'minlaydi.

Magistral bog'lovchi liniyalarda kanallarni taqsimlash jarayoni vaqtning talab qilingan onida mobil stansiya abonentlari va umumfoydalanuvchi telefon tarmog'i abonentlari orasida so'zlashishlarga xizmat qilish uchun bo'sh aloqa liniyalarini taqdim etish kabi ko'riladi.

Shunday qilib, ko'chma xizmat aloqa tizimi kanallari telekommunikatsiya tizimining muayyan tarmog'i sathi va radiosathni birlashtiruvchi tarkibli kanallari hisoblanadi.

Hozirda dunyoning turli mamlakatlarda ko'chma xizmat aloqa tizimining turli ko'rinishlari ishlatiladi va ular ushbu mamlakatlar iqtisodiyotining axborotga bo'lgan ehtiyojini ta'minlaydi. Ko'chma xizmat

aloqa tizimining turlarga bo’linishi radiosathning strukturasi orqali aniqlanadi (2.9-rasm).

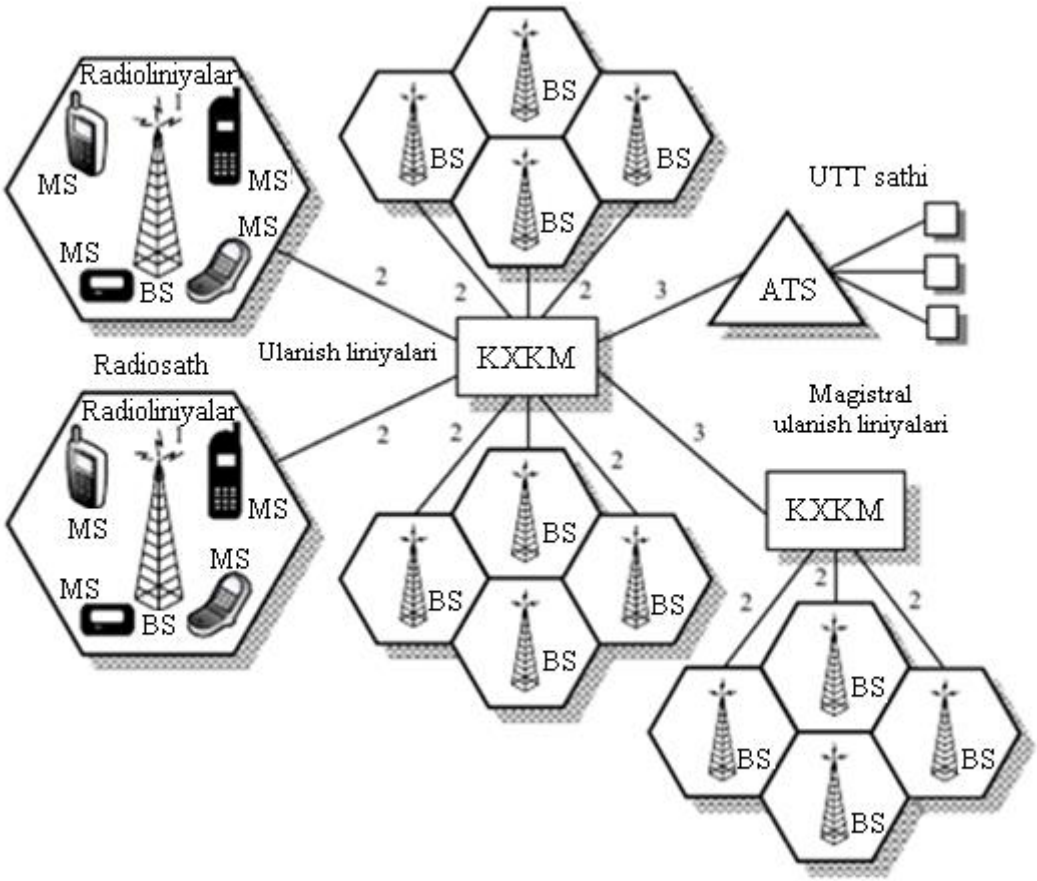


2.9-rasm. Ko’chma xizmat aloqa tizimining tasnifi

Mobil tarmoqlar xizmat ko’rsatiluvchi hududni qoplovchi kataklar (uyalar) majmui ko’rinishida quriladi (2.10-rasm). Kataklar odatda to’g’ri olti burchaklar ko’rinishida tasvirlanadi. Har bir katakning markazida o’zining katagi chegarasidagi barcha mobil stansiyalarga (MS) xizmat ko’rsatuvchi bazaviy stansiya (BS) joylashadi. Abonentning tizimning kataklari orasida ko’chib yurishida xizmatning bir bazaviy stansiyadan ikkinchisiga uzatish, ya’ni estafetali uzatish (handover) sodir bo’ladi. Barcha bazaviy stansiyalar ajratilgan simli yoki aloqaning radioreley kanallari bo’yicha mobil tizimining kommutatsiya markazi bilan bog’langan. Abonentning mobil aloqaning boshqa tizimi hududiga ko’chishida unga xizmat ko’rsatish bir mobil stansiya tizimidan boshqa mobil stansiya tizimiga uzatiladi – rouming (rouming).

Tarkibli tarmoqning 1 qismlari mobil stansiyalar (MS) va bazaviy stansiyalar (BS) orasida tashkil etilgan radioliniyalar hisoblanadi. Tarmoqning 2 qismlari bazaviy stansiyalar (BS) va ko’chma xizmatning

kommutatsiyalash markazi (KXKM) orasidagi ko’p kanalli bog’lovchi liniyalardan iborat. Tarmoqning 3 qismlari radiosath va umumfoydalanuvchi telefon tarmog’i (UTT) orasidagi magistral bog’lovchi liniyalardan iborat. Bazaviy stansiyalar to’plami tizimga xizmat qilishning butun zonasi bo’yicha joylashgan va ko’chma xizmatning kommutatsiyalash markazi orqali radiosathning ixtiyoriy abonentining boshqa mobil abonent yoki umumfoydalanuvchi telefon tarmog’i abonenti bilan barqaror radioaloqani ta’minlashga imkon beradi. Bunda mobil abonentning xizmat qilish zonasining qanday nuqtasida joylashgani ahamiyatga ega emas. Shunday qilib, ko’chma xizmatning kommutatsiyalash markazi xizmat qilish zonasida turli mobil stansiyalarni o’zaro kommutatsiyasini ta’minlovchi avtomatik radiokross rolini, mobil stansiyalarning tarmoqning abonentli telefon apparati bilan kommutatsiyasini, hamda boshqa xizmat qilish zonasining ko’chma xizmatning kommutatsiyalovchi markaziga chiqishini ta’minlaydi.



2.10-rasm. Mobil tarmoqning funksional sxemasi

Turli standartlarning uyali mobil aloqa jihozlarining ishlash algoritmlari bir-biriga o’xshash va quyidagilar orqali xarakterlanadi.

1. Mobil stansiya kutish rejimida bo’lganida, uning qabul qiluvchi qurilmasi tizimning barcha kanallarini yoki faqat boshqarish kanallarini skanerlaydi.

2. Tarmoq fragmentining barcha bazaviy stansiyalari abonentni chaqirish uchun boshqarish kanallari bo’yicha chaqiruv signalini uzatadi.

3. Chaqiriluvchi abonentning mobil stansiyasi chaqiruv signalini olganida boshqarishning bo’sh kanallarining biri bo’yicha javob beradi.

4. Javob signalini olgan bazaviy stansiya, uning parametri xususidagi axborotni ko’chma aloqani kommutatsiyalash markaziga uzatadi. Ushbu markaz chaqiriluvchi abonentning mobil stansiyasi signali sathi maksimal bo’lgan bazaviy stansiyaga so’zlashuvni o’tkazadi.

5. Nomer terilgan vaqtda chaqiriluvchi abonentning mobil stansiyasi bazaviy stansiyaning signal sathi maksimal bo’lgan bo’sh kanallaridan birini ishg’ol qiladi.

6. Chaqiriluvchi abonentning bazaviy stansiyadan uzoqlashgani sari yoki radioto’lqinlar tarqalishi sharoiti yomonlashishiga bog’liq holda signal sathi pasayadi. Bu aloqa sifatining pasayishiga olib keladi. So’zlashuv sifatining yaxshilanishiga chaqiriluvchi abonentni avtomatik tarzda radoaloqaning boshqa kanaliga o’tkazish yo’li bilan erishiladi.

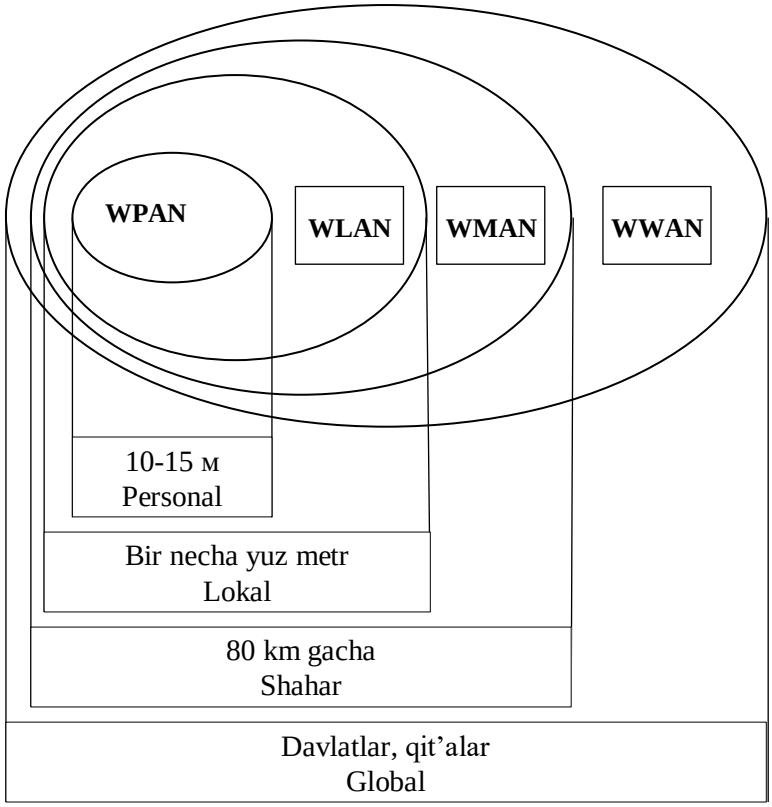
3 BOB. SIMSIZ TARMOQLAR

3.1. Simsiz tarmoqlar qurilishining asosiy prinsiplari

Ma’lumki, radio ixtiro etilganidan so’ng, ko’p o’tmay telegraf aloqani simsiz amalga oshirish imkoniyati paydo bo’ldi. Aslida, hozirgi raqamli kodni radiokanal bo’yicha uzatishda o’sha prinsipdan foydalanishadi, ammo ma’lumotlarni uzatish imkoniyati bir necha bor oshdi.

Zamonaviy simsiz tarmoqlarni ta’sir doirasi va vazifasi bo’yicha quyidagilarga ajratish mumkin (2.1-rasm):

- shaxsiy (Wireless Personal Area Network, WPAN);
- lokal (Wireless Local Area Network, WLAN);
- shahar (Wireless Metropolitan Area Network, WMAN);
- global (Wireless Wide Area Network, WWAN).



3.1-rasm. Simsiz tarmoqlar tasnifi

3.1-jadvalda simsiz tarmoqlarning xarakteristikalari keltirilgan.

Simsiz shaxsiy tarmoqlar (WPAN) uzatishning katta bo’lmagan masofasi bilan (17 metrgacha) ajralib turadi va katta bo’lmagan binoda

ishlatiladi. Bunday tarmoqlarning xarakteristikalari o’rtacha bo’lib, uzatish tezligi odatda 2 Mbit/s dan oshmaydi.

Simsiz tarmoqlarning asosiy xarakteristikalari. 3.1-jadval

Simsiz tarmoqlar / Xarakte-ristikalar	**WPAN (shaxsiy simsiz tarmoqlar)**	**WLAN (lokal simsiz tarmoqlar)**	**WMAN (shahar simsiz tarmoqlar)**	**WWAN (global simsiz tarmoqlar)**
Qo’llanish sohasi	Tashqi qurilma simlarini almashtirish	Simli tarmoqlarning mobil kengaytirish-lari	Keng polosali simsiz foydalanish	Bino tashqarisida Internetdan mobil foydalanish
Taxnologiyalar	Bluetooth, UWB, ZigBee	Wi-Fi (802.11)	WiMax (802.16), MBWA-m (802.20)	GSM, GPRS, WCDMA, EDGE, HSPA+, WiMax, LTE

Bunday tarmoq, masalan, foydalanuvchi shaxsiy kompyuterida yoki noutbukda ma’lumotlarni simsiz sinxronlashni ta’minlashi mumkin. Xuddi shu tariqa printer bilan simsiz ulanish ta’minlanadi. Kompyuterni tashqi qurilmalar bilan ulovchi simlar chigalliklarining yo’qolishi yetarlicha jiddiy afzallik bulib, buning evaziga tashqi qurilmalarning dastlabki o’rnatilishi va keyingi, zaruriyat tug’ilganda, joyini o’zgartirilishi anchagina osonlashadi.

Simsiz shaxsiy tarmoqlarning aksariyat uzatuvchi-qabul qiluvchilarining (transceiver) kam energiya iste’mol qilishi va ihchamligi katta bo’lmagan foydalanuvchi qurilmalarini samarali madadlashga hamda kompyuter qurilmasini uzoq vaqt mobaynida bitta batareyada (yoki akkumulyatorda) ishlashiga imkon beradi. Undan tashqari, kam quvvat iste’mol qilinishi simsiz shaxsiy tarmoqlarni uyali telefonlarga va naushniklarga tatbiq etishga imkon beradi.

Simsiz lokal tarmoqlar (WLAN) ofislarning ichida va tashqarisida, ishlab chiqarish binolarida uzatishlarning yuqori xarakteristikalarini ta’minlaydi. Bunday tarmoqlardan foydalanuvchilar odatda noutbuklarni, shaxsiy kompyuterlarni va katta resurslarni talab etuvchi ilovalarni bajarishga qodir prosessorli va katta ekranli shaxsiy raqamli yordamchilarni (PDA) ishlatishadi. Simsiz lokal tarmoqlar uzatishning 54 Mbit/s gacha tezlikda barcha ofis yoki maishiy ilovalar talabini qondirish imkoniga ega. Xarakteristikalari, komponentlari, narxi va bajaradigan

amallari bo’yicha bunday tarmoqlar ethernet xilidagi an’anaviy simli lokal tarmoqlarga o’xshash.

Simsiz shahar tarmoqlar (WMAN) maydoni bo’yicha shaharga teng bo’lgan hududga xizmat qiladi. Aksariyat hollarda ilovalarni bajarishda belgilangan ulanish talab etilsa, ba’zida mobillik zarur bo’ladi. Masalan, kasalxonada bunday tarmoq asosiy bino va masofadagi klinikalar orasida ma’lumotlarni uzatishni ta’minlaydi. Yoki energetik kompaniya bunday tarmoqdan shahar masshtabida foydalanib, tumanlardan beriladigan ish naryadlaridan foydalanishni bir erga to’playdi yoki mobil foydalanuvchilariga mavjud tarmoq infratuzilmalari bilan ulanishni o’rnatishga imkon beradi.

Simsiz Internet xizmatlari bilan ta’minlovchilar (Wireless Internet Service Provider, WISP) uyda foydalanuvchilar va kompaniyalar uchun doimiy simsiz ulanishlarni ta’minlash maqsadida shaharlarda va qishloq joylarida simsiz shahar tarmoqlarni mijozlar ixtiyoriga taqdim etadi. Bunday tarmoqlar, ko’pincha simli yotqizish bilan oddiy simli ulanishlarga nisbatan samarali hisoblanadi.

Simsiz shahar tarmoqlarning xarakteristikalari turlicha.

Ulanishlarda infraqizil texnologiyaning ishlatilishi ma’lumotlarni uzatish tezligining 100 Gbit/s va unda katta bo’lishini ta’minlaydi.

Simsiz global tarmoqlar (WWAN) mobil ilovalarning ishlanishini, mamlakat yoki xatto kontinent masshtabida foydalanish bilan, ta’minlaydi. Telekommunikatsiya kompaniyalari ko’pgina foydalanuvchilar uchun uzoq masofadan ulanishni ta’minlovchi simsiz global tarmoqning nisbatan qimmat infratuzilmasini yaratadilar. Bunday yechimning xarajati barcha forydalanuvchilar orasida taqsimlanadi, natijada abonent to’lovi unchalik yuqori bo’lmaydi.

Ko’pgina telekommunikatsiya kompaniyalarining kooperatsiyasi tufayli simsiz global tarmoqlarning ta’sir doirasi chegaralanmagan. Telekommunikatsiya xizmatini ta’minlovchilarning birida to’lab, simsiz global tarmoq orqali dunyoning ixtiyoriy nuqtasidan Internet xizmatlaridan foydalanish mumkin.

Simsiz global tarmoq xarakteristikalari nisbatan yuqori emas, ma’lumotlarni uzatish tezligi 56 Kbit/s ni, ba’zida 170 Kbit/s ni tashkil etadi.

Simsiz global tarmoqlarga xos ilovalar Internetdan foydalanishni, elektron pochta xabarlarini uzatish va qabul qilishni ta’minlovchi ilovalar

hisoblanadi. Umuman, simsiz tarmoqdan foydalanuvchilar hududiy chegaralanmaganlar.

Simsiz shaxsiy, lokal, shahar va global tarmoqlar bir-birini to'ldiruvchi bo'lib, turli talablarni qondiradi. Turli simsiz tarmoqlar orasidagi farqni aniqlashda ularda ishlatiladigan texnologiyalardan foydalanishadi.

3.2. Simsiz tarmoq texnologiyalari

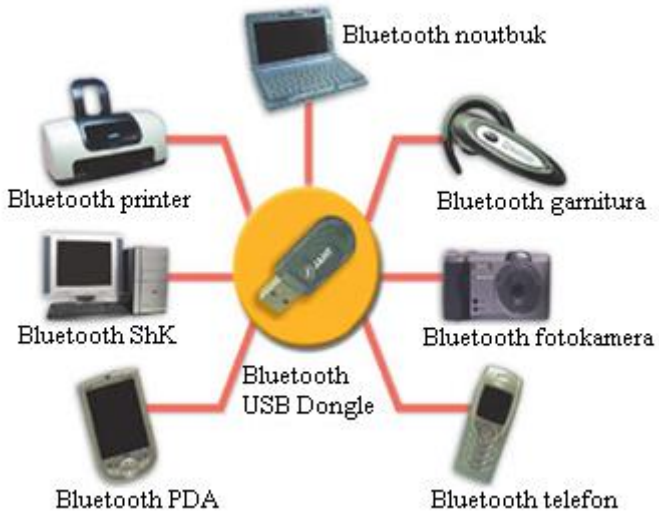
Simsiz shaxsiy tarmoqlariga Bluetooth, UWB, ZigBee texnologiyalari mansub.

Bluetooth texnologiyasida radioaloqa 2,4-2,48 GGs diapazonida amalga oshiriladi. Signal spektri FHSS (Frequency Hopping Spread Spectrum - chastotali sakrash bo'yicha keng polosali signal) usuli bo'yicha shakllantiriladi.

Universal qabul qilish/uzatish uskunalari bazasida ixtiyoriy Bluetooth-yechimlar bilan aloqa ta'minlanadi. Shu bilan birga ijroning asosan ikki varianti ishlatiladi:

- Bluetooth – kalit (Bluetooth-dongle) yoki
- Bluetooth-adapterlar.

Bluetooth shaxsiy kompyuter, noutbuk, PDA (Personal digital assisttanse), mobil telefon, printer va raqamli fotoapparat kabi qurilmalar orasida, bir-biridan 100 m doirasida va xatto turli binolarda, axborot almashinuvini ta'minlaydi (3.2 -rasm).



3.2-rasm. Turli Bluetooth-qurilmalar bilan aloqa

Bluetooth-qurilmalar notanish muhitda ishni boshqa Bluetooth-qurilmalarni qidirish bilan boshlaydi. Ushbu muolaja device discovery deb ataladi. Buning uchun so'rov jo'natiladi. So'rovga javob nafaqat aloqa doirasida faol Bluetooth-qurilmalarning mavjudligiga, balki ushbu qurilmalar mavjud bo'lgan rejimga bog'liq. Bu bosqichda uchta asosiy rejim bo'lishi mumkin:

- Discoverable mode. Ushbu rejimdagi qurilmalar olingan so'rovlarning barchasiga doim javob beradilar;
- Limited discoverable mode. Ushbu rejimdagi qurilmalar so'rovlarga faqat cheklangan vaqtda yoki ma'lum shartlarga rioya qilib javob berishlari lozim;
- Non-discoverable mode. Rejim nomidan ko'rinib turibdiki, ushbu rejimdagi mavjud qurilmalar yangi so'rovlarga javob bermaydilar.

Aniqlash, identifikatsiyalash va dastlabki sozlashning barcha muolajalaridan so'ng Bluetooth-qurilmalar foydalanuvchi axborot almashinuvini boshlashi mumkin.

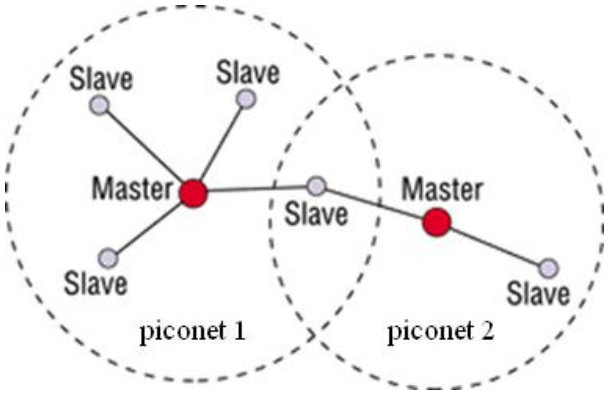
Bluetooth spetsifikatsiyasi axborotni vaqtli multiplekslashli paketli uzatish usulini tavsiflaydi. FHSS ishlashi prinsipiga binoan chastotalar polosasi 1 MGs kenglikdagi qismkanallarning ma'lum soniga ajratilgan. Kanal 79, 23 yoki 22 radiochastotali kanallar bo'yicha psevdotasodifiy sakrashlarning ketma-ketligidan iborat. Har bir kanal davomligi 625 mks bo'lgan vaqtiy segmentlarga bo'linadi. Har bir segmentga ma'lum eltuvchi chastota mos keladi. Peredatchik priyomnik bilan sinxron tarzda bir eltuvchidan ikkinchisiga to'g'rilanadi. Eltuvchi chastotaning bunday o'zgarishi hopping, kanalning o'zgarishi esa hopping channel deb yuritiladi. Ushbu usul uzatishning konfidensialligini va birmuncha xalallardan himoyalanganlikni ta'minlaydi. Agar qandaydir kanal bo'yicha uzatilgan paket qabul qilinmasa, priyomnik u xususida xabar beradi va paketni uzatish endi boshqa chastotada, keyingi qismkanallarning birida qaytariladi.

Bitta Bluetooth qurilmaning bir necha boshqa qurilmalarga ulanishida, bir necha ulanishlarga xizmat qiluvchi qurilma master ("etakchi"), ulangan qurilmalar esa slave ("etaklanuvchi") deb ataladi. Bitta master ga ettitacha aktiv slave larni ulash mumkin. Aktiv slave lardan (yani, ma'lumotlarni aktiv almashadigan qurilmalardan) tashqari, barcha kanallar band bo'lganida, *master* bilan ma'lumotlar almasha olmaydigan, ammo u bilan sinxronlashgan aktiv bo'lmagan slave lar to'plami mavjud bo'lishi mumkin. Bunday struktura *piconet deb yuritiladi. Piconet* lar bir

birlari bilan vaqt va chastota bo'yicha sinxronlanmagan. Ularning har biri o'zining chastota sakrashi ketma-ketligini ishlatadi. Bitta *piconet* doirasida barcha qurilmalar vaqt va chastota bo'yicha sinxronlangan. Har bir *piconet* uchun uning *master* qurilma adresi orqali aniqlanuvchi sakrashlarning psevdotasodifiy ketma-ketligi generatsiyalanadi.

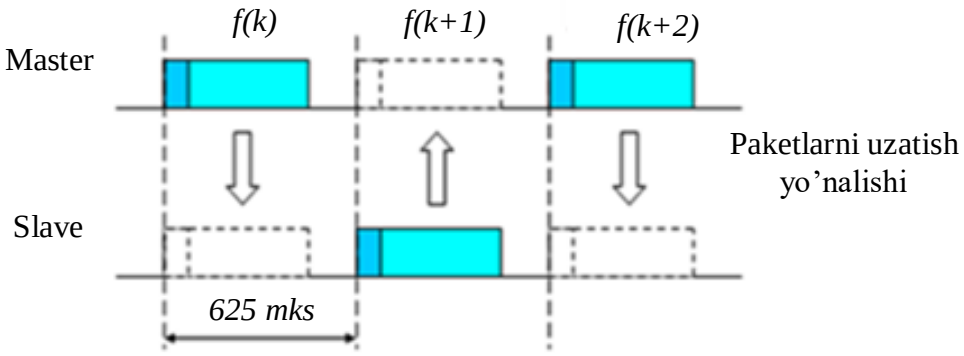
Bitta *piconet* da faqat bitta *master* bo'lishi mumkin, ammo har bir slave bir vaqtning o'zida boshqa qurilmalar uchun master bo'lishi va o'zining *piconet* ini hosil qilishi mumkin. Shu tariqa birlashgan bir necha *piconet scatternet* ni hosil qiladi. *Scatternet* doirasidagi turli qurilmalar turli *piconet* uchun bir vaqtning o'zida nafaqat *master* yoki *slave* bo'lishi, balki turli piconet lar uchun oddiy slave bo'lishi ham mumkin. 3.3-rasmda Bluetooth-qurilmalar bog'lanishlarini tashkil etish strukturasi keltirilgan.

Zaruriyat tug'ilganida *piconet* dagi ixtiyoriy *slave master* bo'lib qolishi mumkin. Tabiiyki, bu holda eski master slave bo'lib qoladi. Shunday qilib, scatternet da qancha kerak bo'lsa, shuncha bluetooth qurilmalar birlashtirilishi mumkin, mantiqiy bog'lanishlar talab qilinganiga binoan hosil qilinishi va zaruriyat tug'ilganida xohlagancha o'zgarishi mumkin.



3.3-rasm. Bluetooth qurilmalar bog'lanishlarini tashkil etish strukturasi

Bluetooth texnologiyasida vaqt bo'linishi - Time Division Duplexing (TDD) asosida dupleks uzatish ko'zda tutilgan. *Master* f(k) paketlarni toq vaqt segmentlaridi, *slave* esa juft vaqt segmentlarida uzatadi (3.4-rasm).



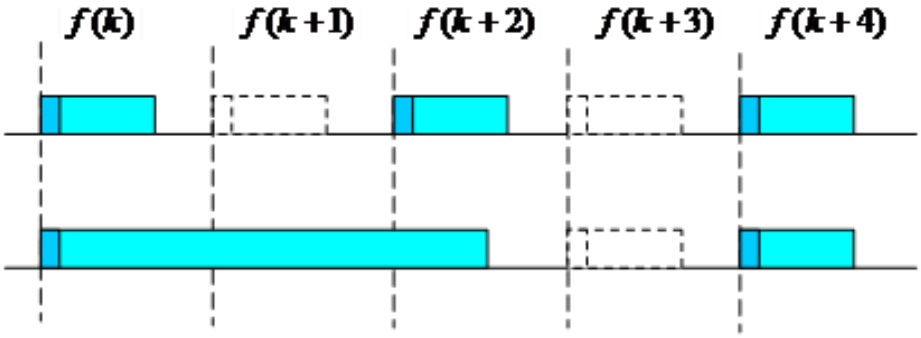
3.4-rasm. Qisqa xabar paketlarini uzatish tartibi

Paketlar, uzunligiga bog'liq holda, beshtagacha vaqt segmentlarini egallashi mumkin. Bunda kanal chastotasi paket uzatilishi tamom bo'lmaguncha o'zgarmaydi (3.5-rasm).

O'ta keng polosali texnologiya Ultra wideband (UWB) radiokanal orqali maishiy elektron qurilmalar, shaxsiy kompyuterning tashqi qurilmalari, va unchalik katta bo'lmagan masofada mobil qurilmalar orasida eng yuqori tezlikda va energiyaning kichik sarfi bilan ma'lumotlar almashinuvini ta'minlovchi, simsiz foydalanishga alternativ texnologiya hisoblanadi. Ushbu texnologiya qamrab olinuvchi zonaning katta bo'lmagan doirasida yuqori o'tkazish qobiliyatiga ega va ideal darajada yuqori sifatli multimedia kontentini simsiz uzatishga mos.

Haqiqatan, maishiy elektronika qurilmalari uchun tezligi yuqori simsiz interfeys kerak, ammo bluetooth kabi va boshqa simsiz texnologiyalaridan foydalanish qator cheklashlar orqali amalga oshiriladi. Ushbu texnologiyalarning asosiy kamchiligi ulardagi o'tkazish polosasining nisbatan katta emasligi. Videoni etkazish uchun odatda 3 dan 24 Mbit/s gacha o'tkazish qobiliyati talab etiladi.

Ta'sir doirasi qisqa simsiz tarmoq texnologiyasi (ZigBee) boshqa WPAN-texnologiyalariga, xususan bluetooth ga nisbatan arzonroq va kam energiya sarfini talab qiluvchi yechimni ta'minlash maqsadida ishlab chiqilgan: vaqtning katta qismida qurilmalar uxlash rejimida bo'ladi va onda-sonda ularga murojaat qilinganligi tekshiriladi. Ikkita apparat orasidagi aloqa uzunligi 75 metrgacha.

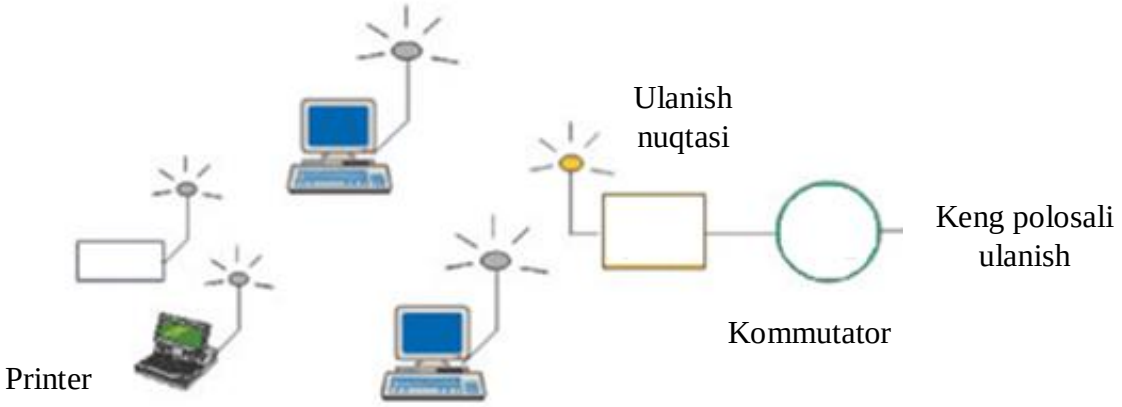


3.5-rasm. Uzun xabar paketlarini uzatish tartibi

Hozirda ushbu texnologiya asosan sensor tizimlarida ishlatiladi, ammo uning tarafdorlari texnologiyaning ixtiyoriy elektron qurilmalarni ulash uchun ishlatilishi mumkin deb hisoblaydilar. Xususan Pantech-Curitel firmasi ZigBee interfeysi bilan smartfon ishlab chiqargan. Ushbu texnologiyaning "aqlli" uy qurilmalarini boshqarish uchun, signalizatsiyaning turli simsiz vositalarida (tutash, xarorat, shovqun, namlik, harakat va h.) ishlatilishi kutilmoqda.

Lokal simsiz tarmoq (WLAN) texnologiyasi 802.11 standartlar oilasiga asoslanadi. 802.11 standartlar oilasiga mansub WLAN-texnologiyalari ko'pincha Wi-Fi atamasi orqali belgilanadi. Hozirda ushbu atama, simli lokal tarmoqlarga alternativa sifatida, 802.11 oilasidagi ixtiyoriy standartga mos barcha ma'lumotlarga qo'llaniladi.

Uy tarmog'i yoki kichik ofis tarmog'i uchun bitta foydalanish nuqtasining mavjudligi yetarli bo'lib, u orqali tarmoqning oxirgi qurilmalari kommutator yordamida keng polosali aloqada amalga oshiriladi (3.6-rasm).

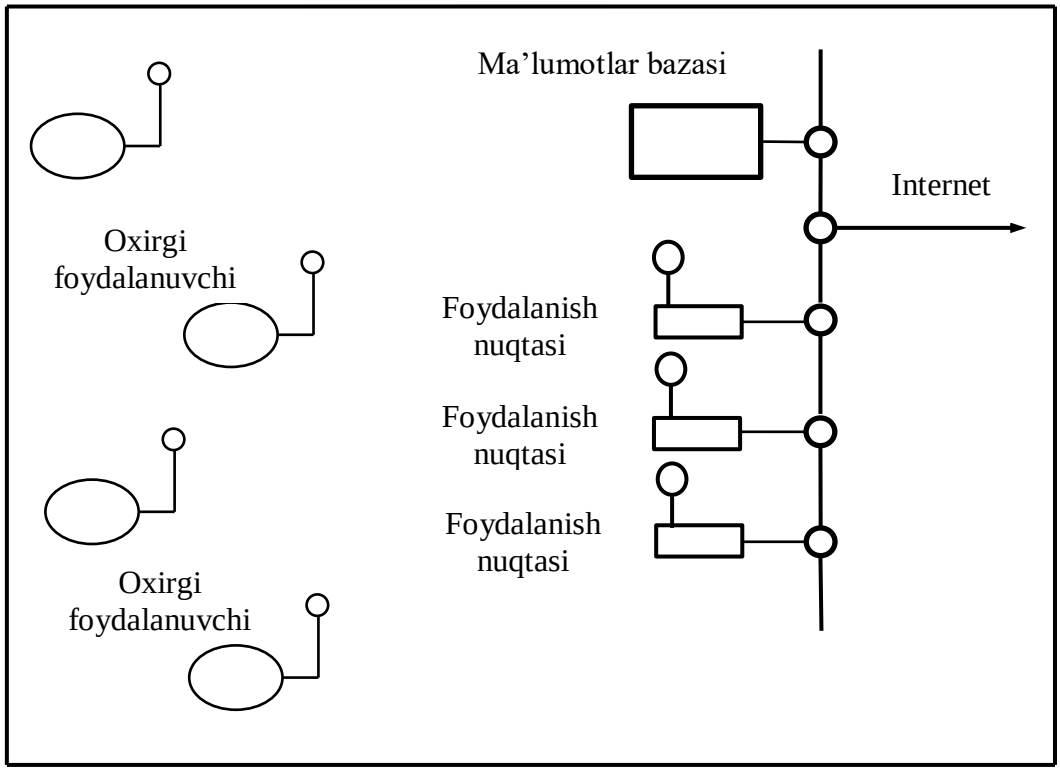


3.6-rasm. Uy yoki kichik ofisdagi WLAN sxemasi

Yirik ofis uchun WLAN ni tashkil etishda foydalanishning bitta nuqtasi yetarli bo’lmaydi. Oxirgi qurilmalar orasidagi masofalarning kattaligi sababli, ofis yoki tashkilot tarmog’ida foydalanishning bir necha nuqtasi tashkil etiladi (3.7-rasm).

Simsiz uy va ofis tarmoqlaridan tashqari Wi-Fi texnologiyasi Internetdan ommaviy foydalanishni tashkil etish sohasida keng qo’llaniladi.

Aksariyat aeroportlarda, mexmonxonalarda, restoranlarda Wi-Fi tarmoqlardan foydalanish (pulli yoki tekin) xot-spotlar (xot spot - "qaynoq nuqta") yordamida amalga oshirilgan (3.8-rasm).



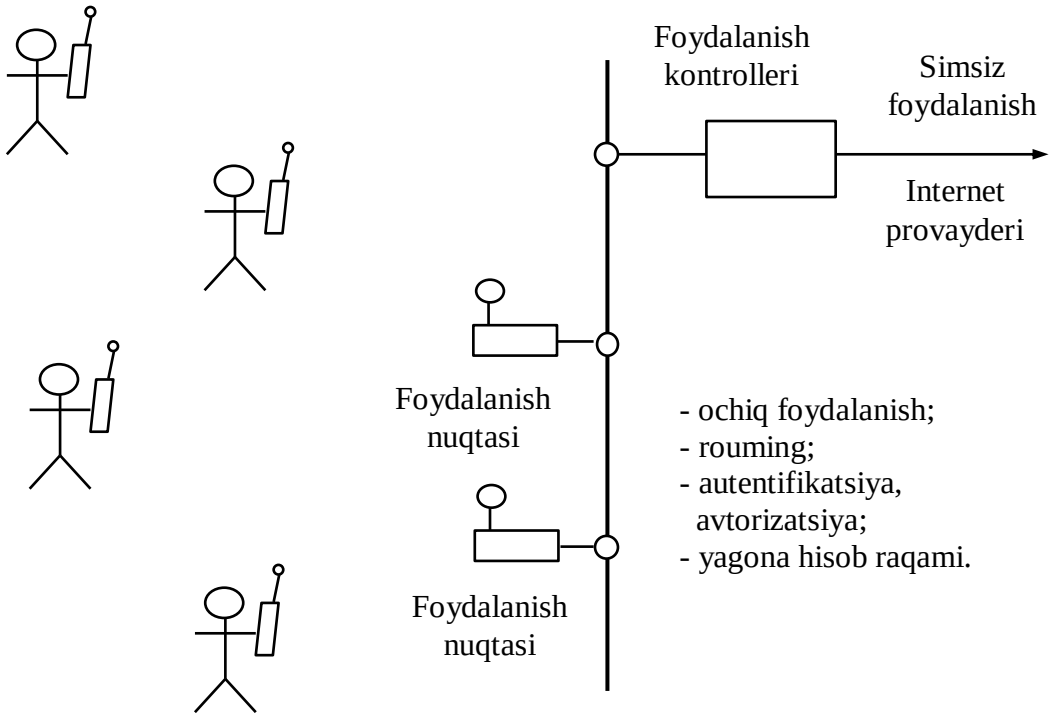
3.7-rasm. Yirik ofis uchun WLAN sxemasi

Xot-spotlari bo’lgan muassasaga har bir tashrif buyuruvchi o’zining noutbuki, cho’ntak shaxsiy kompyuteri yoki simsiz foydalanish standartini madadlovchi telefoni yordamida tarmoqqa mobil ulanish imkoniyatini oladi. Tarmoqning muayyan standartlariga bog’liq holda Wi-Fi lar 2,4 GGs yoki 5 GGs chastotalarda ishlaydi va ma’lumotlarni uzatish tezligini 54 Mbit/s gacha ta’minlaydi. Bir necha xot-spotlar bazasidagi simsiz foydalanish zona "xot-zona" deb ataladi.

O’tkazish qobiliyatining keskin o’zgarishiga 802.11n texnologiyasining paydo bo’lishi sabab bo’ldi. Mutaxassislarning fikri

bo’yicha yaqin orada 802.11n simsiz tarmoq texnologiyasini nafaqat noutbuklar, balki ko’pgina maishiy elektron asboblar madadlaydi va u barcha asosiy korporativ va uy ilovalari tomonidan ishlatiladi.

Simsiz personal va lokal tarmoqlarning istiqbolli rivoji sifatida mutaxassislar Cognitive Radios qurilmalarini ko'rsatmoqdalar. Bu qurilmalar turli diapazonda turli protokollar bo’yicha ishlay oladi hamda ularning joylashgan geografik hududini va ushbu hududda, mahalliy talablarga moslanib, qanday ishlashi lozimligini aniqlashi mumkin.



3.8-rasm. "Xot-spot" sxemasi

Shahar simsiz tarmoqlariga WiMAX (802.16) va MBWA-m (802.20) texnologiyalari mansub.

WiMAX texnologiyasi – qurilmalarning keng spektri (kompyuterlardan to mobil telefonlargacha) uchun katta masofada universal simsiz aloqani taqdim etish maqsadida yaratilgan telekommunikatsiya texnologiyasi. Texnologiyaning ishlashi Wireless MAN deb ham ataluvchi IEEE 802.16 standartga asoslangan.

WiMAX texnologiyasidan quyidagi masalalarni echishda foydalanish mumkin:

- Wi-Fi dan foydalanish nuqtalarini bir-biri bilan va Internetning boshqa segmentlari bilan ulash;

- ajratilgan (simli) liniyalarga alternativ sifatida simsiz keng polosali foydalanishni ta’minlash;

- ma’lumotlarni uzatishning tezkor servislarini va telekommunikatsiya xizmatlarini taqdim etish;

- geografik o’rniga bog’lanmagan foydalanish nuqtalarini yaratish;

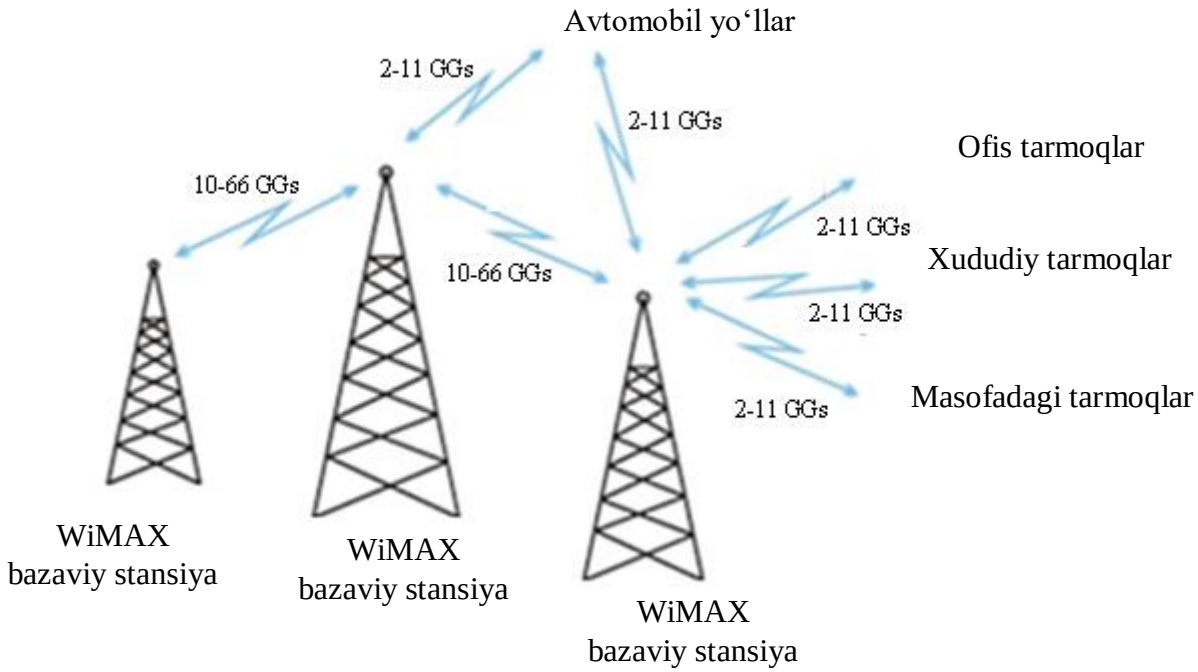
- masofaviy monitoring tizimlarini yaratish.

WiMAX Internetdan yuqori tezlikda, Wi-Fi tarmoqlarga nisbatan anchagina katta qoplash bilan foydalanishni amalga oshirishga imkon beradi. Bu texnologiyani "magistral kanal" sifatida ishlatishga imkon beradi. Bunday "magistral kanallar" an’anaviy ajratilgan (telefon) liniyalar bilan bog’lanishni amalga oshirishi mumkin.

Natijada bunday yondashish shahar doirasidagi masshtablanuvchi tezkor tarmoqlarni yaratishga imkon beradi.

Hozirda WiMAX texnologiyaning to’rtta standarti ma’lum: 802.16a, 802.16d, 802.16e va 802.16f. Bazisining bir xilligiga qaramay ushbu to’rtta standart bir-biriga mos kelmaydi.

WiMAX tarmog’i ikkita asosiy qismdan iborat (3.9-rasm):



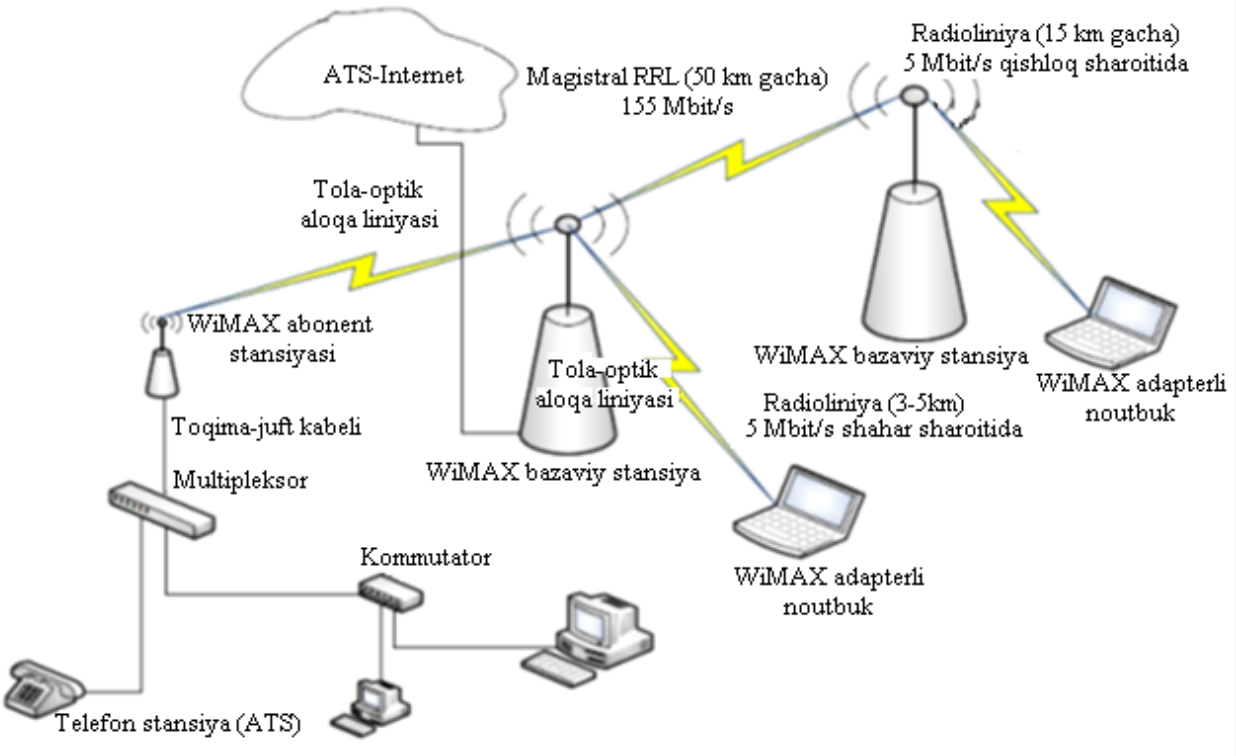
3.9-rasm. WiMAX tarmog’i strukturasi

- WiMAX ning bazaviy stansiyasi baland ob’ektda (binoda yoki minorada) joylashishi mumkin;

- WiMAX ning mijoz transiveri - priyomnik/peredatchikli antenna bilan.

Bazaviy stansiya bilan mijoz transiveri orasida ulanish 2-11 GGs diapazonida bajariladi. Ushbu ulanish ma’lumotlarni 20 Mbit/s tezlikda uzatishga imkon beradi va stansiya bilan foydalanuvchi orasida bevosita ko’rinish mavjudligini talab qilmaydi. WiMAX bazaviy stansiyasining ushbu ishlash rejimi keng ishlatiluvchi IEEE 802.11 (Wi-Fi) standartga yaqin. Bu esa WiMAX bilan ishlab chiqarilgan mijoz qurilmalarining mosligiga ishora qilinadi. WiMAX texnologiyasi provayder va foydalanuvchi orasidagi oxirgi qismda va shahar tarmoqlaridan foydalanishni taqdim etishda qo’llaniladi. Qo’shni bazaviy stansiyalar orasida 10-66 GGs chastotalar diapazonidan foydalanib doimiy ulanish o’rnatiladi. Bazaviy stansiyalardan biri keng polosali tezkor ulanish orqali provayder tarmog’i bilan doimiy bog’langan bo’lishi mumkin.

Tipik bazaviy stansiya 6 ta sektordan iborat. 802.16 standart asosida tashkil etilgan korporativ tarmog’ining strukturasi 3.10-rasmda keltirilgan.



3.10-rasm. Korporativ tarmoq strukturasi

Strukturasi bo’yicha WiMAX tarmoqlar mobil aloqaning an’anaviy tarmoqlariga juda o’xshash. WiMAX signallari standart ethernet-kabel orqali bevosita muayyan kompyuterga va Wi-Fi standartning foydalanish

nuqtasiga yoki ethernet standartining simli lokal tarmog'iga berilishi mumkin. Bu kabel foydalanishdan WiMAX ga o'tishda hudud yoki ofis lokal tarmoqlarning mavjud infrastrukturasining saqlanishiga imkon beradi.

Hozirgi vaqtda WiMAX texnologiya quyidagi ishlash rejimlarini madadlaydi:

- Fixed WiMAX –belgilangan foydalanish – ko'p polosali simli texnologiyalarga alternativa hisoblanadi. Bunda tarmoqning barcha uzellari harakatsiz qoladi;
- Nomadic WiMAX – seansli foydalanish – mavjud Fixed WiMAXga sessiyalar tushunchasi qo'shilgan. Sessiyalarning mavjudligi mijoz uskunalarini sessiyalar orasida bemalol ko'chirishga va ulanishni WiMAX ning boshqa minoralari yordamida tiklashga imkon beradi;
- Portable WiMAX – ko'chirish rejimida foydalanish. Ushbu rejim uchun mijozni WiMAX ning bir bazaviy stansiyasidan ikkinchisiga ulanishni yo'qotmay, avtomatik tarzda qayta ulash imkoniyati qo'shilgan.
- Mobile WiMAX – mobil foydalanish. Ushbu rejim mijoz uskunasini ko'chirish tezligini 120 km/soatgacha ko'paytirishga imkon beradi. Undan tashqari ushbu rejim signalning ko'p nurli tarqalishiga va ulanishni yo'qotmasdan shaxsiy xalallarga barqaror.

MBWA-m 802.20 texnologiyasi. Internetdan mobil simsiz foydalanish uchun yaratilgan. Shaharlarda, soni cheklangan bazaviy stansiyalarda ishlashga mo'ljallangan WiMAX dan farqli holda, ushbu texnologiya oddiy uyali tizimlarga juda uxshash va 1 Mbit/s dan yuqori tezlikda 3 GGs chastotalar diapazonidagi tezkor mobil ulanishlarga mo'ljallangan. Ushbu texnologiya boshqa texnologiyalar orasida g'alati o'rinni egallaydi. Bir tomondan uni WiMAX (802.16e)ning yaqin konkurenti deb atashadi, ikkinchi tomondan u GPRS yoki CDMA2000ni o'rniga uyali aloqa tizimida ishlatilishi mumkin. Bu endi WWAN. MBWA-m texnologiya abonent terminallarining katta tezlikda (250 km/soat), to'g'ri ko'rinish zonasidan tashqarida ko'chishida ham ishlashni ta'minlaydi.

MBWA-m ning uya doirasi 15 km gacha etishi mumkin. Radiokanal polosasining kengligi- 1,25 MGs dan 40 MGs gacha.

Global simsiz tarmoqlar (WWAN) texnologiyalari

WWAN tarmoq texnologiyalarini avlodlarga ajratish qabul qilingan (1G, 2G, 3G, 4G, …). G – Generation, ya'ni avlodni bildiradi.

Birinchi avlod texnologiyalariga (1G) analog texnologiyalari taalluqli. Analog texnologiyalari faqat ovoz chaqiriqlarini amalga oshirish

uchun yaratilgan bo’lib, ma’lumotlarni uzatish tezligi haddan tashqari past edi.

Ikkinchi avlod texnologiyalari (2G) analog texnologiyalariga nisbatan qator afzalliklarga ega, ya’ni ovozning yaxshilangan sifati, yuqori himoyalanganlik va unumdorlik. Ikkinchi avlod texnologiyalari xususida so’z borganida, avvalo, *GSM (Global Standard for Mobile Communications)* - "mobil uyali aloqa uchun global standart" texnologiyasini ko’rsatish lozim. Ushbu texnologiyada nafaqat raqamlashtirilgan nutq, balki raqamli ma’lumotlar uzatilishi mumkin. GSM tarmoq abonentlari mobil modem xizmatlaridan, kompyuter tizimlaridan foydalanishlari, elektron pochta xabarlarini yuborishlari va qabul qilishlari mumkin. Bunday tarmoqlarning asosiy kamchiliklaridan biri – uzatishning past tezligi. Internetdan mobil foydalanish imkoniyati GPRS (General Packet Radio Service) - ma’lumotlarni radiotarmoq orqali paketli uzatishga o’tish bilan anchagina kengaydi. GPRS texnologiyasi GSM texnologiyaga ustqurma bo’lib, ma’lumotlarni uzatish tezligi 171,2 Kbit/c gacha etadi.

Uchinchi avlod texnologiyalari (3G) yuqorida aytib o’tilgan ma’lumotlarni uzatish tezligiga talablarga qo’shimcha ikkinchi avlod tarmoqlari bilan osongina integratsiyasini ta’minlashga mo’ljallangan. Ushbu avlod texnologiyalariga CDMA texnologiyasining rivoji hisoblanuvchi *WCDMA (Wideband Code Division Multiple Access)* – kod ajratishli keng polosali ko’p miqdordagi foydalanish – radiointerfeys texnologiyasi mansub. Ushbu texnologiya har biri 5 MGs li radiochastotaning ikkita keng polosasidan foydalanadi. Mobil foydalanish texnologiyasi rivojining navbatdagi bosqichi EDGE (Enhanced Data rates for GSM evolution) – GPRS tarmoqlarga ustqurma hisoblanuvchi mobil aloqa uchun ma’lumotlarni simsiz uzatuvchi raqamli texnologiya. EDGE yordamida tarmoqqa ulanish GPRS ga nisbatan taxminan 3 marta tez, ma’lumotlarni uzatish tezligi esa 474 Kbit/s gacha tashkil etishi mumkin.

HSPA+ (Evolved High-Speed Packet Access) – uchinchi avlodning tezligi yuqori paketli foydalanish texnologiyasi bo’yicha ma’lumotlarni uzatish tezligi (bazaviy stansiyadan barcha lokal abonentlarga ma’lumotlarni uzatish tezligi) 10 - 20 Mbit/s gacha tashkil etadi.

To’rtinchi avlod texnologiyalarining (4G) uchinchi avlod texnologiyalaridan asosiy farqi, ushbu texnologiyalar ma’lumotlarni butunlay paketli uzatish protokollariga asoslangan. 3G texnologiyasi esa o’zida paketli kommutatsiya bilan kanalli kommutatsiyani birlashtiradi.

WiMAX va LTE (Long-Term evolution) texnologiyalari to’rtinchi avlod texnologiyalari hisoblanib, ularda multiplekslashning yangi, haddan tashqari samarali sxemalari ishlatiladi. Ularning ikkalasida ovozni uzatish kanali mavjud emas. LTE standartida tarmoqda abonentgacha tezlik 173 Mbit/s gacha va abonentdan tarmoqqacha tezlik 58 Mbit/s gacha belgilangan.

4 BOB. YERNING SUN’IY YO’LDOSHLI MOBIL ALOQA TIZIMLARI

4.1. Yerning sun’iy yo’ldoshli mobil aloqa tizimlarini qurishning umumiy prinsiplari

Yerning sun’iy yo’ldoshli mobil tizimlari mobil aloqaning nisbatan yangi, qudratli, moslanuvchan va tezlik bilan rivojlanuvchi turi hisoblanadi. Birinchi Yerning sun’iy yo’ldoshi (YSY) uchirilishi bilanoq u aloqa tizimlarida ishlatila boshlandi.

Hozirda Yerning sun’iy yo’ldoshli mobil aloqaning quyidagi sohalarda qo’llanishi dolzarb hisoblanadi:

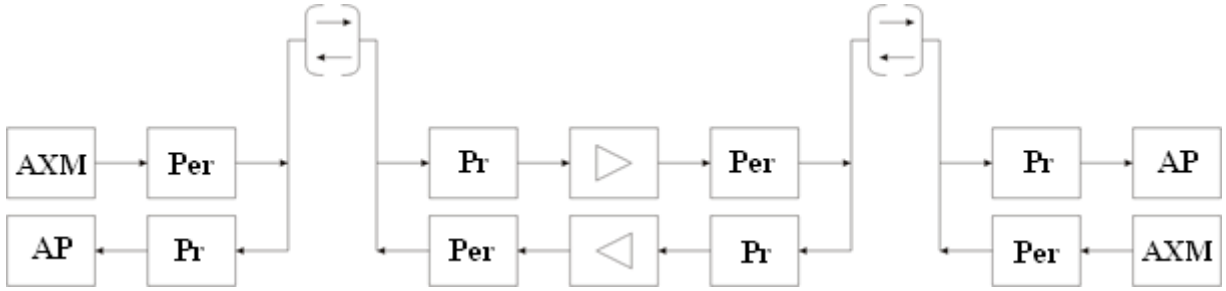
- uyali tarmoqlarni kengaytirish (cellular extension), ya’ni Yerning sun’iy yo’ldoshli aloqani uyali aloqa bo’lmagan hududlarda ishlatish;
- uyali tarmoqlarni to’ldirish (cellular complement), ya’ni Yerning sun’iy yo’ldoshli aloqani mavjud uyali aloqaga qo’shimcha tarzda ishlatish. Masalan, standartlarning bir-biriga mos kelmaganida yoki qandaydir favqulotdagi vaziyatlarda roumingni ta’minlash uchun;
- statsionar simsiz aloqa (fixed wireless), masalan, simli aloqa bo’lmagan kamaholi hududlarda.

Shunday qilib, Yerning sun’iy yo’ldoshli mobil aloqa uyali aloqaga raqib emas, balki u bilan yetarlicha uzviy bog’langan. Barcha Yerning sun’iy yo’ldoshli mobil aloqa tizimlarida uyali aloqa bilan integratsiyaning yetarlicha yuqori darajasi ko’zda tutilgan. Xususan, Yerning sun’iy yo’ldoshli mobil aloqa tizimlariga mo’ljallangan abonent terminallaridan tashqari ikkita rejimli terminallarni yaratish ko’zda tutilgan. Bu terminallar Yerning sun’iy yo’ldoshli mobil aloqa tizimida va ixtiyoriy uyali standartlarning birida ishlashga mo’ljallangan.

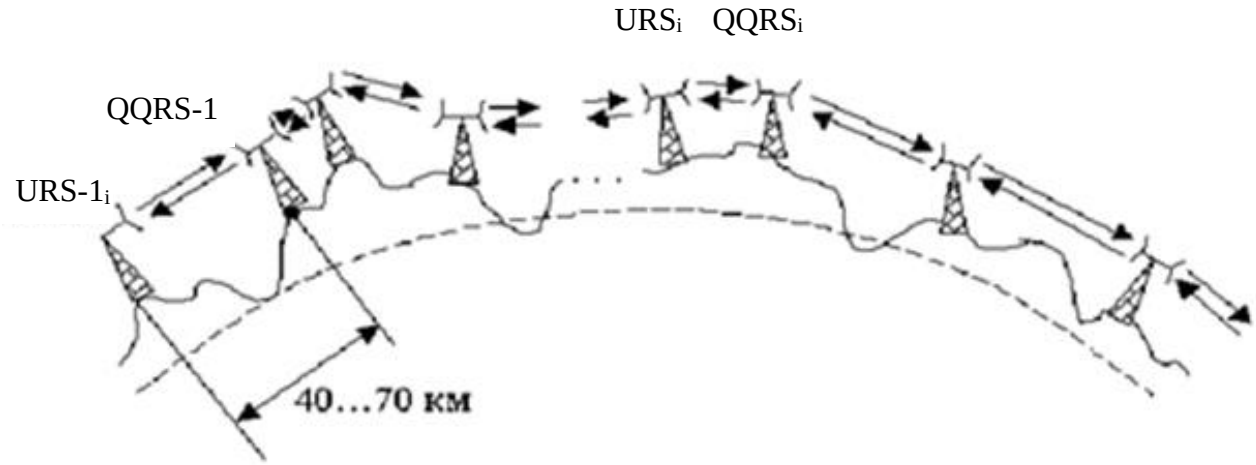
Yerning sun’iy yo’ldoshli mobil aloqa davrigacha katta masofaga radioaloqa qanday amalga oshirilar edi? Ayniqsa, iqtisodiy va texnik sabablarga ko’ra masofaga simli aloqani yaratish foydasiz, yoki qiyin edi. Bu hollarda olis aloqa radioreley tizimlari yordamida amalga oshirilar edi.

Radioaloqa liniyasi bir necha yoki ko’pgina bo’laklardan iborat bo’lishi mumkin va bo’laklar doirasida radiosignallarni uzatish qabul qiluvchi-uzatuvchi uskunalarning komplekti yordamida ta’minlanadi. Signallarni bir punktdan ikkinchi punkt qabul qiladi, kuchaytiradi va uchinchi punktga uzatadi, u erda kuchaytiriladi va to’rtinchi punktga uzatiladi va h. Radioaloqa liniyasining bunday qurilishi aloqaning

radioreleyli liniyasi deb ataladi. 4.1-rasmda aloqaning radioreleyli liniyasining struktura sxemasi, 4.2-rasmda esa shartli tasvirlanishi keltirilgan.

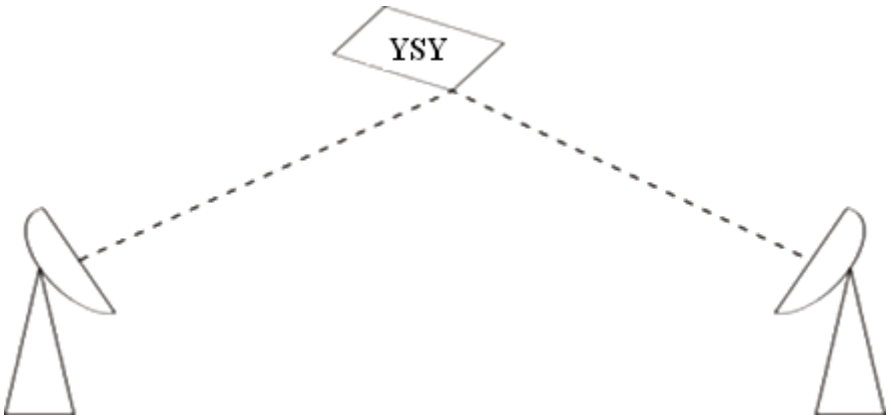


4.1-rasm. Aloqaning radioreleyli liniyasining struktura sxemasi (AXM - axborot manbai, AP - axborot priemnigi, Per - peredatchik, Pr - priyomnik)



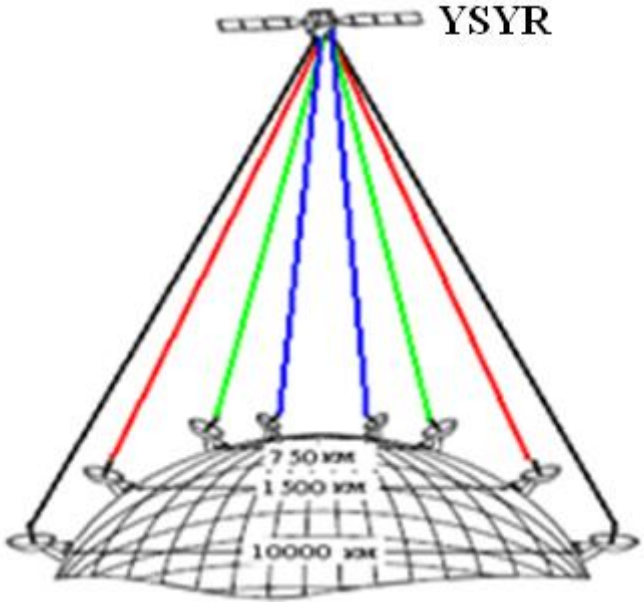
4.2-rasm. Aloqaning radioreleli liniyasining shartli tasvirlanishi (URS-1- birinchi uzatuvchi radioreley stansiyasi, QQRS-1 -birinchi qabul qiluvchi radioreley stansiyasi)

Yerning sun’iy yo’ldoshli mobil aloqa qanday ishlaydi? Yerdagi stansiyadan YSYga signal qabul qilinadi, kuchaytiriladi va Yerning sun’iy yo’ldoshi peredatchigi orqali, Yerdagi birinchi stansiyadan katta masofadagi Yerdagi boshqa stansiyaga uzatiladi (4.3-rasm).



4.3-rasm. Aloqaning Yerning sun’iy yo’ldoshli liniyasi

Yerning sun’iy yo’ldoshli aloqa tizimining (YSYAT) ishlash prinsipi Yerning sun’iy yo’ldosh retranslyatoridan (YSYR) foydalanishga asoslangan. YSYR orqali Yerdagi stansiyalar (YS) orasida aloqa ta’minlanadi (4.4-rasm).



4.4-rasm. Yerdagi stansiyalar orasida aloqaning ta’minlanishi

Yerning sun’iy yo’ldoshli aloqaning vazifasiga bog’liq holda Yerda, atmosferada yoki kosmosda joylashgan punktlar birlashtiriladi. Ushbu punktlarning har birida odatda qabul qiluvchi-uzatuvchi bog’langan radiostansiya (bir kanalli yoki ko’p kanalli) o’rnatiladi, Yerning sun’iy yo’ldoshlarida esa abonentlardan radiosignallarini oluvchi va bu signallarni boshqa abonentlarga retranslyasiyalovchi YSY translyatorlari o’rnatiladi. Oddiy holda retranslyasiya kirish signallari quvvatini

kuchaytirishdan va ular spektrlarini boshqa eltuvchi chastotalarga o’tkazishdan iborat bo’ladi. Ammo Yerning qator sun’iy yo’ldoshli aloqa tizimlarida YSYRlarida turli tizimlar orasidagi chaparastani kamaytirish va tizimning xalallarga bardoshligini oshirish maqsadida signallarning murakkab ishlanishi amalga oshiriladi. Umumiy holda, barcha punktlar (abonentlar) orasida sifatli aloqani ta’minlash uchun YSYRlarni turli orbitalarda aylanuvchi bir necha YSYlarida joylashtirishga to’g’ri keladi.

Yerning sun’iy yo’ldoshli aloqa tizimlari abonentlarga xizmat ko’rsatishning globallik va universallik darajasi bo’yicha farqlanadi. Bunday tizimlarning globallik darajasi xizmat ko’rsatish zonaning mansubligi va o’lchami orqali, tizim universalligi esa abonentlar kategoriyalari nabori va taqdim etiluvchi aloqa turlarining soni orqali xarakterlanadi.

Mansubligi bo’yicha Yerning sun’iy yo’ldoshli aloqa tizimlari xalqaro, milliy, korporativlarga bo’linadi. Xizmat ko’rsatish zonasi bo’yicha Yerning sun’iy yo’ldoshli aloqa tizimlari global, regional zonalarga bo’linadi.

Yerning sun’iy yo’ldoshli aloqa tizimlarida axborotning quyidagi turlarini uzatish amalga oshiriladi:

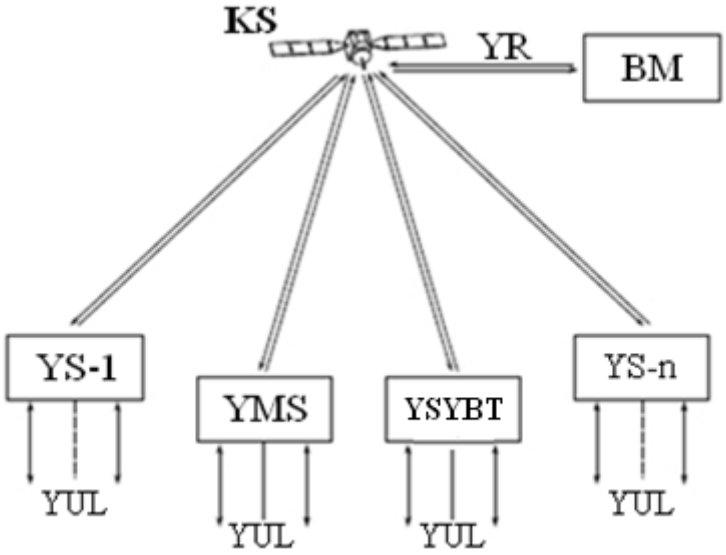
- televidenie va ovozli radioeshittrish dasturlari va davriy xarakterli simpleks xabarlarni;
- telefon, faksmil, telegraf xabarlarni, videokonferensiyalarni.

YS larning turi va Yerning sun’iy yo’ldoshli tizimning vazifalariga bog’liq holda radioaloqaning quyidagi xizmatlari farqlanadi:

- Yerning sun’iy yo’ldoshli tizimning belgilangan xizmati – Yerning bitta yoki bir necha sun’iy yo’ldoshi ishlatilganida belgilangan punktlarda joylashgan Yerdagi stansiyalar orasidagi radioaloqa rejimiga mos keladi;
- Yerning sun’iy yo’ldoshli ko’chma xizmati Yerning bitta yoki bir necha sun’iy yo’ldoshi ishlatilganida Yerdagi ko’chma stansiyalar orasidagi radioaloqa rejimiga mos keladi;
- Yerning sun’iy yo’ldoshli radioeshittirish xizmati - radioaloqaning sirkulyar rejimiga mos keladi.

4.2. Yerning sun’iy yo’ldoshli mobil aloqa tizimlari tarkibi va asosiy xarakteristikalari

Yerning sun’iy yo’ldoshli mobil aloqa tizimlari tarkibiga quyidagi komponentlar kiradi (4.5-rasm):



4.5-rasm. Yerning sun’iy yo’ldoshli mobil aloqa tizimi strukturasi

- kosmik stansiya (KS) – tarkibida qabul qiluvchi-uzatuvchi qurilma, radiosignallarni qabul qiluvchi va uzatuvchi antennalar, hamda energiya etkazib berishni, antennalar va quyosh batareyalarini orientatsiyalashni, orbitada Yerning sun’iy yo’ldoshi holatini korreksiyalashni va h. ta’minlovchi YSYRdan iborat;

- Yerdagi stansiyalar (YS) – axborotning dupleks almashishini ta’minlaydi;

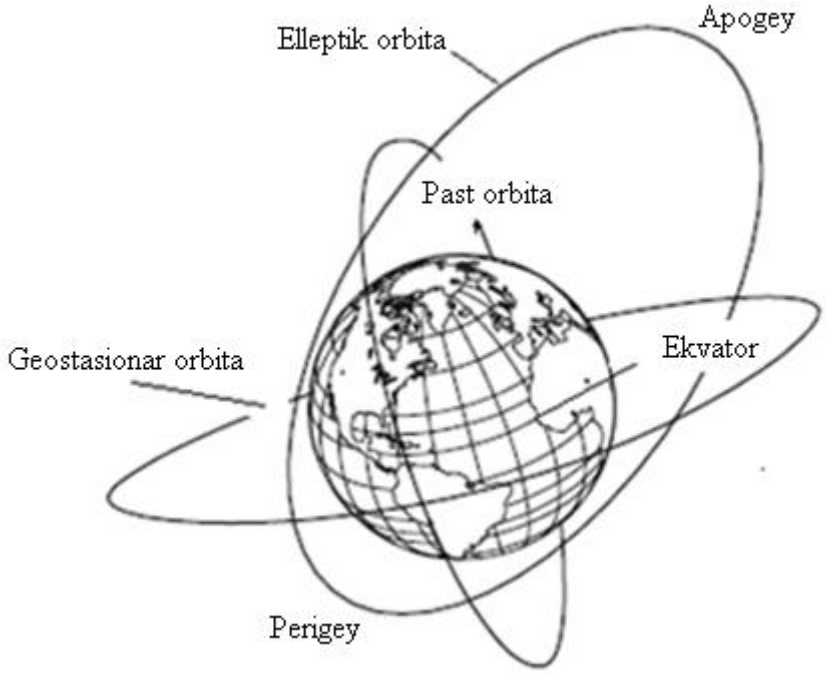
- Yerdagi markaziy (koordinatsiyalovchi) stansiya (YMS) – YSYR ishlash rejimini nazoratlashni va YSYAT ishlashi uchun muhim bo’lgan Yerdagi stansiyalar parametrlariga (nurlanuvchi energiya, eltuvchi chastotalar, modulyatsiyalovchi signal xarakteristikalarining qutblanish turlari va h.) rioya qilinishini ta’minlaydi;

- Yerning sun’iy yo’ldoshini boshqarishning markaziy tizimi - YSYBTda joylashgan barcha texnik vositalarni boshqarishni va ular holatini nazoratlashni ta’minlaydi;

- Yerdagi ulovchi liniyalar (YUL) – Yerdagi stansiyani uzatiluvchi axborot manbaiga va iste’molchiga ulashni ta’minlaydi;

- Yerning sun’iy yo’ldoshli aloqa tizimini boshqarish markazi (BM) – YSYATni ekspluatatsiyasiga va rivojiga rahbarlikni amalga oshiruvchi organ.

Mavjud va yaratiluvchi Yerning sun’iy yo’ldoshli aloqa tizimlarida balandligiga bog’liq holda geostatsionar, elliptik va past orbitalar ishlatiladi (4.6-rasm).



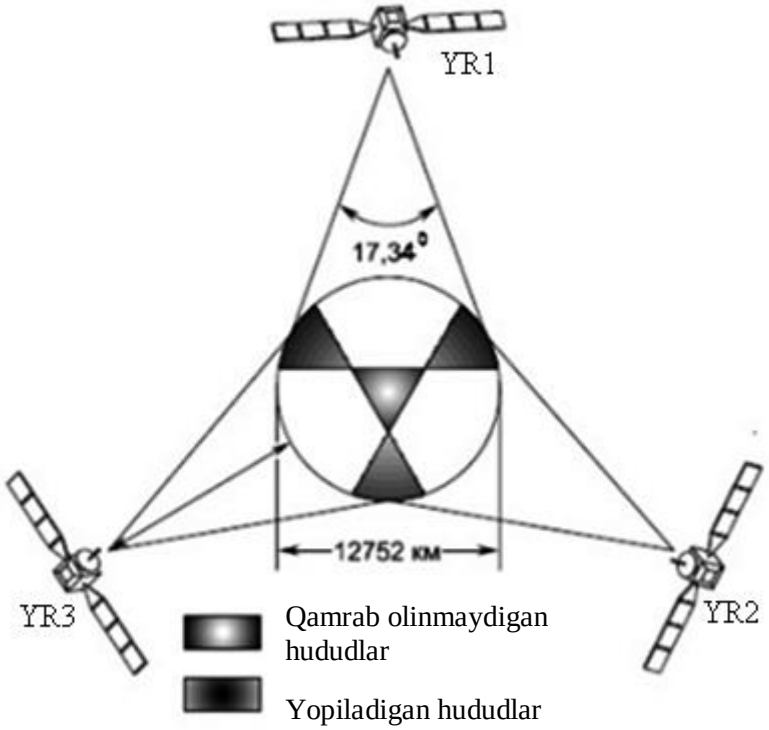
4.6-rasm. Yerning sun’iy yo’ldoshli aloqa
tizimlaridagi orbitalar turi

Yerning sun’iy yo’ldoshli mobil aloqa tizimlarida geostatsionar orbitalarning qo’llanishi quyidagi afzalliklarni ta’minlaydi:

- aloqa uzluksiz, kechayu kunduz, Yerning bir sun’iy yo’ldoshidan boshqasiga o’tmasdan va yo’ldosh holatini antennalar yordamida kuzatish zaruriyatisiz amalga oshiriladi;
- Yer stansiyasi va yo’ldosh retranslyatori orasidagi masofa stabil ahamiyatga ega bo’lganligi sababli, ular orasidagi trassada signal susayishining o’zgarmas qiymati ta’minlanadi;
- Yerning sun’iy yo’ldoshi tarqatadigan chastotaning dopler siljishining yo’qligi;
- geostatsionar yo’ldoshining ko’rinish zonasi yer ustining uchdan birini tashkil etganligi sababli, uchta yo’ldosh ishlatilganida aloqani global tizimini yaratish imkoniyati ta’minlanadi (4.7-rasm).

Geostatsionar orbita yuqorida keltirilgan afzalliklari tufayli, keng ishlatiladi. Hozirda geostatsionar orbita aloqa yo’ldoshlari bilan deyarli oxirgi chegaragacha to’ldirilgan. Buning ustiga eng katta to’yinishni fiksirlangan va qisman radio eshittirish xizmatlariga tegishli yo’ldoshlar vujudga keltiradi. Hozirda geostatsionar orbitada turli mamlakatlarning 300dan ortiq Yerning sun’iy yo’ldoshlari mavjud (ularning maksimal soni 360 atrofida bo’lishi mumkin). Yo’ldoshli aloqaning muayyan tizimlarida

yo’ldoshlarni joylashtirish uchun pozitsiyalarning hammasi ham qulay emasligi hisobga olinsa, yo’ldoshlar sonini ko’paytirish orqali orbita hajmini oshirish sezilarli natijalarni bermasligi ayon bo’ladi.



4.7-rasm. Yerni uchta geostatsionar yo’ldosh bilan qamrab olish sxemasi

Geostatsionar orbita resurslarining to’liqroq ishlatilishiga, ishchi chastotalarning ko’p marta takrorlanishi hamda yuqoriroq chastotali diapazonlarni o’zlashtirish yo’li bilan geostatsionar orbitalarda yo’ldoshli aloqa tizimining kelajakdagi rivoji yordam beradi.

Yerning sun’iy yo’ldoshli Internetda odatda, geostatsionar orbita ishlatiladi. Ushbu orbitadagi Yerning sun’iy yo’ldoshining asosiy vazifasi planetaning bir nuqtasidan (bazaviy stansiyadan) Yerning sun’iy yo’ldoshi qoplovchi zonada (bu juda katta hudud bo’lib, odatda, bir necha mamlakatlarni o’z ichiga oladi) joylashgan abonentlarga axborot uzatish hisoblanadi. Yerning sun’iy yo’ldoshli Internetni tashkil etish sxemasi 4.8-rasmda keltirilgan.

Qoplash maydoni - ushbu texnologiyaning asosiy afzalligi. Uyali operator bazaviy stansiyaning bitta vishkasi bitta kvartal yoki mikrorayonga teng hududni qoplaydi. Shunday bo’lsa ham, ma’lumotlar barcha foydalanuvchilarga birdaniga uzatiladi. Abonent unga atalgan

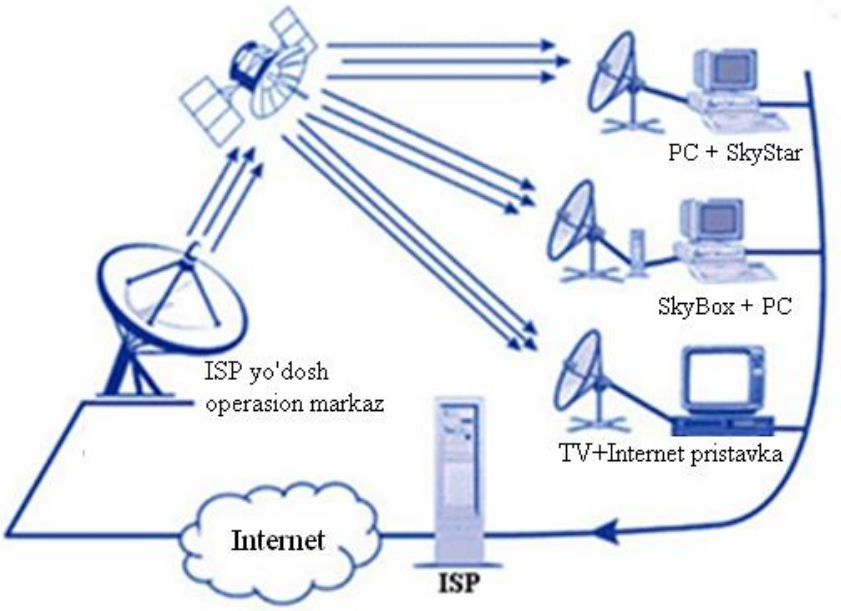
muayyan ma’lumotlar kanalidan foydalanish uchun o’zining elektromagnnit to’lqinini (eltuvchi to’lqinini) identifikatsiyalashi lozim.

Ushbu eltuvchi to’lqin parametrlarini Yerning sun’iy yo’ldoshli Internet provayderi taqdim etadi. Bu parametrlar quyidagilarni o’z ichiga oladi:

- eltuvchi chastotani (MGs);
- simvol tezligini (Kbit/s);
- elektromagnit to’lqinining qutblanish turini (o’ng/chap, vertikal/gorizontal).

Undan tashqari, bitta eltuvchi chastotada, odatda, bir necha foydalanuvchining ma’lumotlari bo’ladi. Ularni identifikatsiyalash uchun maxsus identifikatorlar (PID, LID) va qabul qilish kartasining (resiverning) MAC adresi ishlatiladi.

Yanada ishonchli bog’lanishni tashkil etish uchun maxsus dasturlar (akseleratorlar) ham ishlatiladi. Bu dasturlar trafikni shifrlash bilan bir qatorda uni zichlashtiradi. Natijada Yerning sun’iy yo’ldoshining chastota resurslari tejaladi va ma’lumotlarni uzatish tezligi oshadi.



4.8-rasm. Yerning sun’iy yo’ldoshli Internetni tashkil etish sxemasi

Mutaxassislar Yerning sun’iy yo’ldoshli Internetga ulanishning ikkita usulini ajratishadi: simmetrik va asimmetrik. Bunday farqlash, aavalo trafikni uzatishning kiruvchi (Internetdan) va chiquvchi (Internetga uzatish) kanallarini tashkil etish bilan bog’liq.

Internetdan *simmetrik* foydalanishda ma’lumotlar Yerning sun’iy yo’ldoshidan bitta antenna va ikkita (yoki bitta) peredatchik yordamida

uzatiladi. Ulanishning ushbu turi iqtisodiy nuqtai nazaridan ommaviy tus olmagan.

Internetdan *asimmetrik* foydalanishda Yerning sun’iy yo’ldoshi orqali faqat kiruvchi ulanish ishlatiladi (ya’ni, antenna uchun faqat arzon priyomnik talab etiladi), chiquvchi ulanish esa Yerdagi ixtiyoriy aloqa kanali orqali tashkil etiladi. Ulanishning ushbu turining samaradorligini foydalanuvchining Internetga tez-tez murojaati bilan tushuntirish mumkin, ya’ni oddiy foydalanuvchi Internetga ko’pincha qisqa so’rovlar yuboradi, Internetdan esa ma’lumotlarning katta hajmini oladi.

5 BOB. MOBIL TIZIMLARDA XAVFSIZLIK TAHDIDLARI

5.1. Axborot xavfsizligiga tahdidlar tasnifi

Axborot xavfsizligiga tahdidlar deganda tarmoq resurslarining, jumladan saqlanuvchi, uzatiluvchi va ishlanuvchi axborotning hamda dasturiy va apparat vositalarining buzilishiga, o'zgarishiga yoki ruxsatsiz foydalanishiga olib kelishi mumkin bo'lgan harakat yoki hodisa tushuniladi.

Tahdidlarni *tasodifiylariga (bilmasdan) va qasdan qilinadiganlariga (atayin)* ajratish qabul qilingan. Dasturiy ta'minotdagi xatoliklar, apparat vositalarining ishdan chiqishi, foydalanuvchilarning yoki tarmoq ma'muriyatining noto'g'ri harakatlari va h. tasodifiy tahdidlarning manbai bo'lishi mumkin. Qasdan qilinadigan tahdidlar tasodifiylaridan farqli holda tarmoq foydalanuvchilariga (abonentlarga) zarar etkazish maqsadini ko'zlaydi va, o'z navbatida *aktiv* va *passivlarga* bo'linadi.

Aktiv tahdidlarning maqsadi tarmoqning apparat, dasturiy va axborot resurslariga maqsadli ta'sir orqali uning me'yoriy ishlashi jarayonini buzish hisoblanadi. Aktiv tahdidlarga quyidagilar taalluqli:

- ma'lumotlarni uzatish tarmog'ining aloqa liniyalarini buzish yoki radioelektron bostirish;
- kompyuterni (serverni) yoki uning operatsion tizimini ishdan chiqarish;
- foydalaniluvchi ma'lumotlar bazasidagi yoki tarmoqning tizimli axborotidagi ma'lumotlarni o'zgartirish;
- tarmoq operatsion tizimini buzish yoki o'zgartirish va h.

Bunday tahdidlarning manbai niyati buzuqlarning bevosita harakatlari, dasturiy viruslar va h. bo'lishi mumkin.

Passiv tahdidlar, odatda, tarmoq ishlashiga ta'sir etmasdan, axborot resurslaridan ruxsatsiz foydalanishga mo'ljallangan. Misol tariqasida ma'lumotlarni uzatish kanallarini eshitish orqali ularda aylanuvchi axborotni olishga urinishni ko'rsatish mumkin.

Bo'lishi mumkin bo'lgan tahdid manbaining joylashgan joyiga bog'liq holda barcha tahdidlar *tashqi* va *ichki* lariga ajratiladi.

Axborot xavfsizligining tashqi tahdidlariga quyidagilar taalluqli:

- ajnabiy razvedka va maxsus xizmatlar faoliyati;
- raqobatlashuvchi iqtisodiy strukturalar faoliyati;

- jinoiy guruhlar va tuzilmalarning, hamda fuqarolar, davlat va umuman jamiyat manfaatlariga qarshi yo'naltirilgan mamlakat ichidagi ayrim shaxslar faoliyati;

- tabiiy ofat va falokat.

Axborot xavfsizligining ichki tahdidlariga quyidagilar taalluqli:

- mobil tizimlarga xizmat ko'rsatuvchi xodimlar va foydalanuvchilar tomonidan yo'l qo'yiluvchi axborot xavfsizligiga o'rnatilgan talablarning buzilishi (bilmasdan yoki atayin);

- xabarlarni (ma'lumotlarni) ishlovchi, saqlovchi va uzatuvchi texnik vositalarining, himoya vositalarining va himoyalash bo'yicha qayd qilingan choralar samaradorligini nazoratlash vositalarining ishlamay qolishi va nosozligi; dasturiy ta'minotning, axborotni himoyalashning dasturiy vositalarining va himoyalash bo'yicha qabul qilingan choralar samaradorligini nazoratlovchi dasturiy ta'minotning yanglishishi.

Amalga oshirilish usuli bo'yicha axborot xavfsizligi tahdidlari quyidagi turlarga ajratiladi:

- tashkiliy;
- dasturiy-matematik;
- radioelektron;
- fizik.

Axborot xavfsizligining tashkiliy tahdidlariga quyidagilar taalluqli:

- mobil tizimlarga hizmat ko'rsatuvchi xodimlar va foydalanuvchilar tomonidan yo'l qo'yiluvchi axborot xavfsizligiga o'rnatilgan talablarning buzilishi;

- axborotni manipulyasiyalash (dezinformatsiya, axborotni bekitish yoki o'zgartirish);

- mobil tizimlarda ma'lumotlarni ruxsatsiz nusxalash;

- mobil tizimlari ma'lumotlar bazasi va ma'lumotlar bankidan axborotni o'g'irlash;

- axborotning mashina eltuvchisini o'g'irlash;

- kriptografik himoya vositalarining muhim hujjatlarini o'g'irlash;

- mobil tizimlarida ma'lumotlarni yo'q qilish yoki modifikatsiyalash.

Axborot xavfsizligining dasturiy-matematik tahdidlariga quyidagilar taalluqli:

- virus-dasturlarni joriy etish;
- dasturiy zakladkalarni ishlatish.

Axborot xavfsizligining radioelektron tahdidlariga quyidagilar taalluqli:

- sirqib chiqishning texnik kanallarida axborotni ushlab qolish;

- apparat vositalariga va binolarga axborotni ushlab qolishning elektron vositalarini kiritish;

- ma’lumotlarni uzatish tarmoqlarida va aloqa liniyalarida yolg’on akxborotni majburan qabul qildirish;

- aloqa liniyasini radioelektron bostirish, mobil tizimlarini boshqarish tizimini izdan chiqarish.

Axborot xavfsizligining fizik tahdidlariga quyidagilar taalluqli:

- axborotni yig’ish, ishlash, uzatish, himoyalash vositalarini buzish, ularga maqsadli ravishda nosozliklarni kiritish;

- axborotning mashina eltuvchisini yo’q qilish yoki buzish;

- fizik, dasturiy-matematik yoki tashkiliy tahdidlarni amalga oshirish maqsadida mobil tizimga xizmat qiluvchilarga va foydalanuvchilarga ta’sir etish.

5.2. Mobil tizimlarda axborot xavfsizligiga asosiy tahdidlar

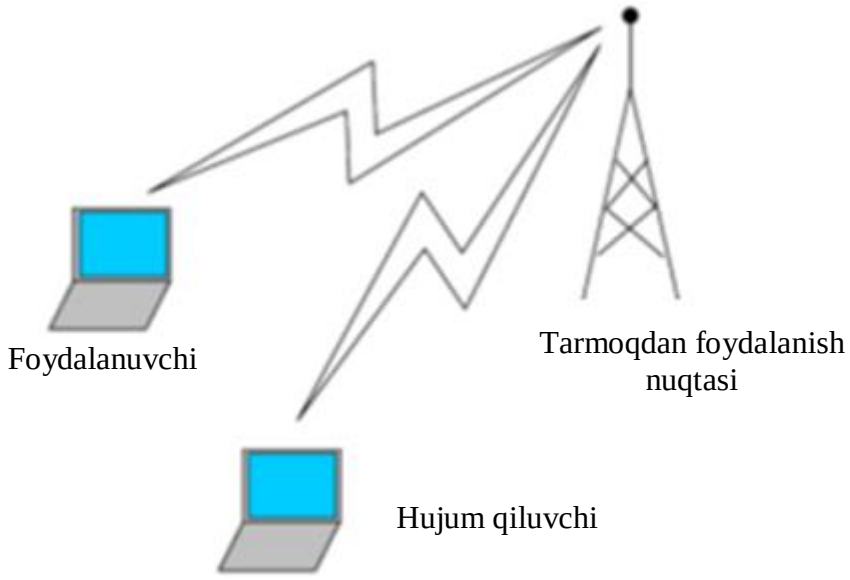
Simsiz texnologiyadan foydalanib juda katta afzalliklarga erishish mumkin. Bu texnologiya foydalanuvchilarga aloqani yo’qotmasdan bemalol harakatlanish hissiyotini bersa, tarmoq yaratuvchilariga bog’lanishlarni tashkil etish uchun katta imkoniyatlarni yaratadi. Undan tashqari tarmoqdan foydalanish uchun ko’pgina yangi qurilmalarni paydo bo’lishiga imkon beradi. Ammo simsiz texnologiya oddiy simli tarmoqlarga qaraganda o’zida ko’proq tahdidlarni eltadi. Xavfsiz simsiz ilovani yaratish uchun simsiz "hujumlar" o’tuvchi, bo’lishi mumkin bo’lgan barcha yo’nalishlarni aniqlash lozim. Afsuski, ilovalar hech qachon butunlay xavfsiz bo’lmaydi, ammo simsiz texnologiyalardagi xavf-xatarni sinchiklab o’rganish har holda himoyalanish darajasini oshishiga yordam beradi. Demak, mumkin bo’lgan tahdidlarni tahlillab, tarmoqni shunday qurish lozimki, hujumlarga xalaqit berish va nostandart "hujum"lardan himoyalanishga tayyor turish imkoni bo’lsin.

Nazoratlanmaydigan hudud. Simli va simsiz tarmoqlar orasidagi asosiy farq tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlanmaydigan zona bilan bog’liq. Uyali tarmoqlarning yetarlicha keng makonida simsiz muhit aslo nazoratlanmaydi. Zamonaviy simsiz texnologiyalar tarmoq makonini boshqarish vositalarining chegaralangan to’plamini taqdim etadi. Bu simsiz tuzilmalarning yaqinidagi hujum qiluvchilarga simli dunyoda mumkin bo’lmagan hujumlarni amalga oshirishga imkon beradi.

Yashirincha eshitish. Simsiz tarmoqlar kabi ochiq va boshqarilmaydigan muhitda eng tarqalgan muammo - anonim hujumlarning mumkinligi. Anonim zararkunandalar 5.1-rasmda ko’rsatilganidek radio-signallarni ushlab qolib, uzatiluvchi ma’lumotlarni rasshifrovka qilishi mumkin.

Uzatishni ushlab qolish uchun niyati buzuq peredatchik oldida bo’lishi lozim. Ushlab qolishning bunday turlarini umuman qaydlash mumkin emas va ularga xalaqit berish undan ham qiyin. Antennalar va kuchaytirgichlardan foydalanish, ushlab qolish jarayonida niyati buzuqning nishondan aytarlicha uzoq masofada bo’lishlariga imkon beradi.

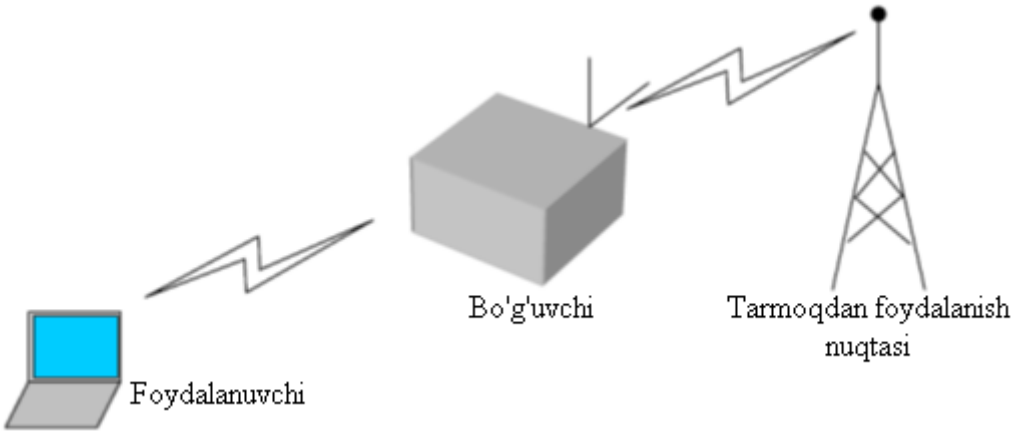
Yashirincha eshitishning yana bir usuli - simsiz tarmoqqa ulanish. Lokal simsiz tarmoqda yashirincha faol eshitish odatda *Adress Resolution Protocol (ARP)* protokolidan noto’g’ri foydalanishga asoslangan. Boshida bu texnologiya tarmoqni "eshitish" maqsadida yaratilgan edi. Aslida, ma’lumotlar bog’lanishi sathida *"man in the middle" (MITM* - "o’rtada odam", pastroqqa qaralsin) xilidagi hujum bilan ish ko’riladi. Hujum qiluvchi lokal simsiz tarmoqning nishon stansiyasiga so’ralmagan ARP-javoblarni yuboradi, nishon stansiyasi esa hujum qiluvchiga o’zidan o’tayotgan barcha trafikni jo’natadi. So’ngra niyati buzuq paketlarni ko’rsatilgan adresatlarga yo’llaydi. Shunday qilib, simsiz stansiya boshqa simsiz mijozning (yoki lokal tarmoqdagi simli mijozning) trafigini ushlab qolishi mumkin.



5.1-rasm. Simsiz kommunikatsiyalarda yashirincha eshitish

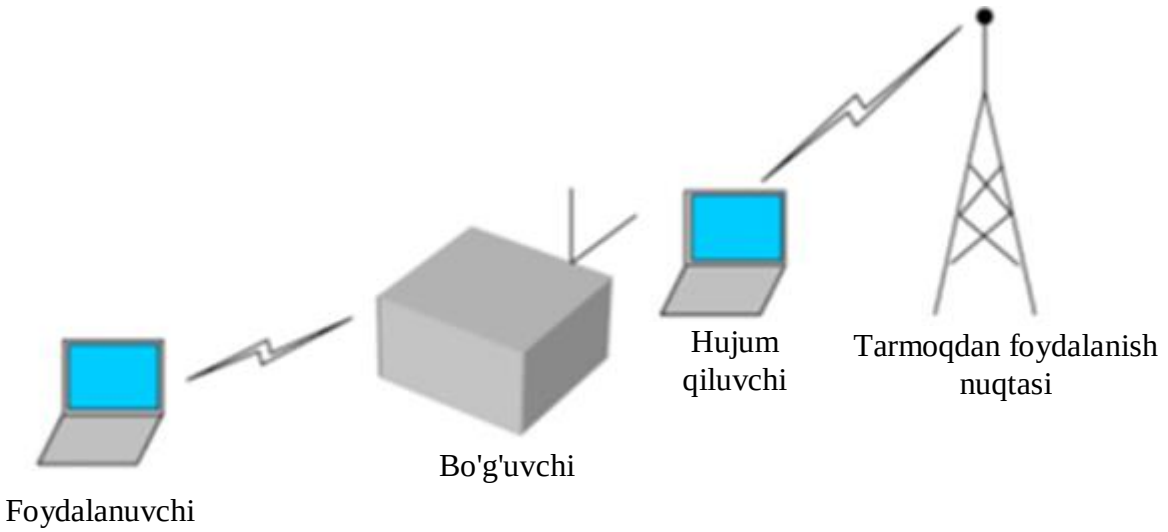
Bo'g'ish. Tarmoqlarda bo'g'ish atayin yoki atayin bo'lmagan interferensiyaning aloqa kanalidagi jo'natuvchi va qabul qiluvchi imkoniyatidan oshganida sodir bo'ladi. Natijada, bu kanal ishdan chiqariladi. Hujum qiluvchi bo'g'ishning quyidagi usullaridan foydalanishi mumkin.

Xizmat kursatishdan voz kechishga undash. DoS (Denial of Service - xizmat ko'rsatishdan voz kechishga undash) xilidagi hujum tarmoqni butunlay ishdan chiqarishi mumkin. Butun tarmoqda, jumladan bazaviy stansiyalarda va mijoz terminallarida, shunday kuchli interferensiya paydo bo'ladiki, stansiyalar bir-birlari bilan bog'lana olmaydilar (5.2-rasm). Bu hujum ma'lum doiradagi barcha kommunikatsiyani o'chiradi. Simsiz tarmoqqa bo'ladigan DoS hujumni oldini olish yoki tuxtatish qiyin. Simsiz tarmoq texnologiyalarining aksariyati litsenziyalanmagan chastotalardan foydalanadi, demak, bir qancha elektron qurilmalardan interferensiya bo'lishi mumkin.



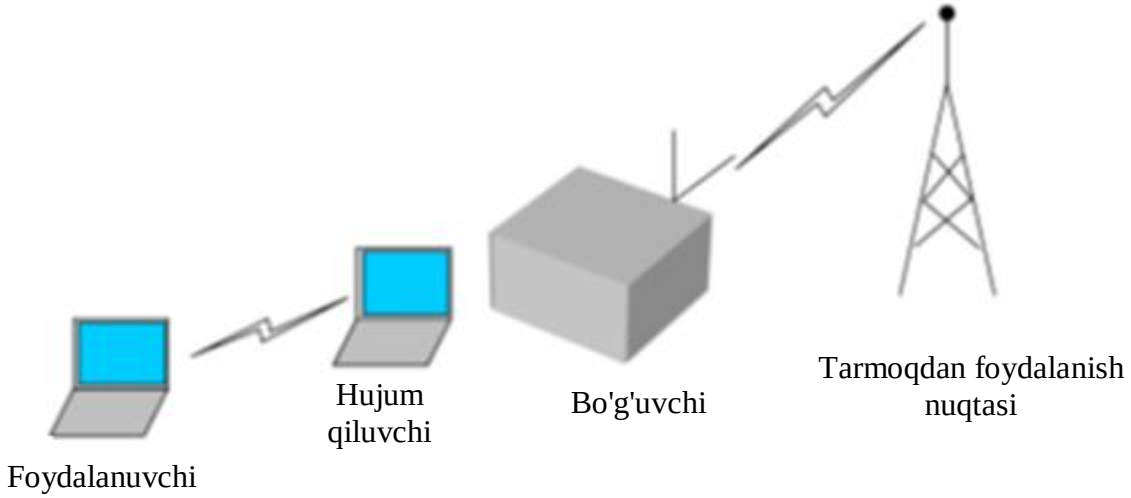
5.2-rasm. Simsiz kommunikatsiyalarda bo'g'ish hujumlari

Mijozlarni bo'g'ish. Mijoz stansiyasini bo'g'ish firibgarga o'zini bo'g'ilgan mijoz o'rniga qo'yishiga imkon beradi (5.3-rasm). Mijoz ulanishni amalga oshira olmasin degan maqsadda unga xizmat ko'rsatishdan voz kechishga undash uchun ham bo'g'ishdan foydalaniladi. Juda mohirlik bilan qilingan hujumlar niyati buzuq stansiyasini bazaviy stansiyaga ulash maqsadida mavjud ulanishni uzadi.



5.3-rasm. Ulanishni ushlab qolish maqsadida mijozni bo’g’ish hujumi

Bazaviy stansiyani bo’g’ish. Bazaviy stansiyani bo’g’ish uni hujum qiluvchi stansiyasi bilan almashtirishga imkon beradi (5.4-rasm).



5.4-rasm. Ulanishni ushlab qolish maqsadida
bazaviy stansiyani bo’g’ish hujumi

Bunday bo’g’ish foydalanuvchilarni xizmatlardan foydalanishdan, telekommunikatsiya kompaniyalarini esa foydadan mahrum qiladi.

Yuqorida qayd etilganidek, aksariyat simsiz texnologiyalar litsenziyalanmagan chastotalardan foydalanadi. Shu sababli ko’pgina qurilmalar – radiotelefonlar, kuzatish tizimlari va mikroto’lqinli o’choqlar - simsiz tarmoq ishiga ta’sir etishi va simsiz ulanishni bo’g’ishi mumkin. Bunday atayin bo’lmagan bo’g’ish hollarini oldini olish uchun,

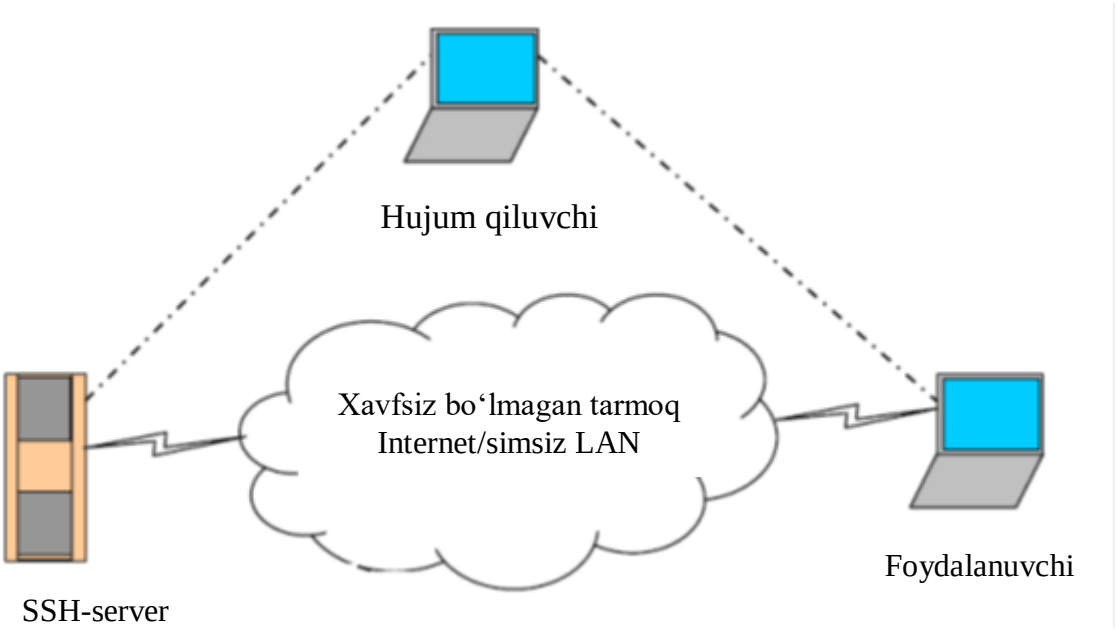
qimmatbaho simsiz asbob-uskunani sotib olishdan avval u o’rnatiladigan joyni sinchiklab tahlillash lozim. Bunday tahlil kommunikatsiyalarga begona qurilmalarning ta’sir etmasligiga ishonch hosil qilishga imkon beradi va ma’nosiz xarajatlardan asraydi.

Bostirib kirish va ma’lumotlarni modifikatsiyalash. Niyati buzuq ulanishni ushlab qolish, ma’lumotlarni yoki komandalarni uzatish maqsadida ma’lumotlarning mavjud oqimiga axborotni qo’shganida bostirib kirish sodir bo’ladi. Hujum qiluvchi paketlarni bazaviy stansiyaga yuborib, boshqarish komandalari va axborot oqimlari ustida manipulyasiyani amalga oshirishi mumkin. Boshqarish komandalarini kerakli boshqarish kanaliga yuborish orqali foydalanuvchini tarmoqdan uzishga erishish mumkin.

Bostirib kirish xizmat ko’rsatishdan voz kechishga undash uchun ishlatilishi mumkin. Hujum qiluvchi tarmoqdan foydalanish nuqtalarini ulanish komandalari bilan to’lib-toshtiradi. Natijada boshqa foydalanuvchilarga tarmoqdan foydalanishga ruxsat berilmaydi.

MITM (man in the middle) hujumi. MITM hujumi yuqorida tavsiflangan bostirib kirishlarga o’xshash. Ular turli shakllarni olishlari mumkin va aloqa seansining konfidensialligini va yaxlitligini buzish uchun ishlatiladi. MITM hujumlar anchagina murakkab, chunki ularni amalga oshirish uchun tarmoq xususida batafsil axborot talab etiladi. Niyati buzuq, odatda, tarmoq resurslaridan birining identifikatsiyasini bajaradi. Hujum qurboni ulanishni boshlaganida, firibgar uni ushlab qoladi va istalgan resurs bilan ulanishni tugallaydi, so’ngra ushbu resurs bilan barcha ulanishlarni o’zining stansiyasi orqali o’tkazadi (5.5-rasm). Bunda hujum qiluvchi axborotni jo’natishi, jo’natilganini o’zgartirishi yoki barcha muzokaralarni yashirincha eshitishi va so’ngra rasshifrovka qilishi mumkin.

Abonent-firibgar. Tarmoq abonentining ishini sinchiklab o’rganib chiqqan hujum qiluvchi o’zini "tarmoq abonenti" qilib ko’rsatib, tarmoq va uning xizmatlaridan foydalanishga urinadi. Undan tashqari foydalanishda qo’llaniladigan qurilmaning o’g’irlanishi tarmoqqa kirishga yetarli bo’ladi. Barcha simsiz qurilmalarning xavfsizligini ta’minlash oson ish emas, chunki ular foydalanuvchilarning harakatlanishida qulaylik tug’dirish maqsadida atayin kichkina qilib yaratiladi.

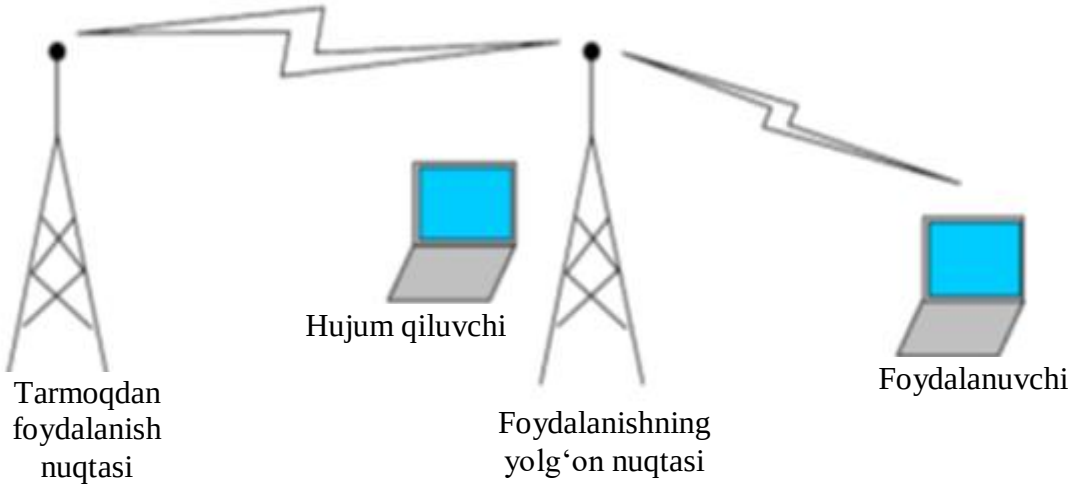


5.5-rasm. MITM xilidagi hujum

Tarmoqdan foydalanishning yolg’on nuqtalari. Tajribali hujum qiluvchi tarmoq resurslarini imitatsiya qilish bilan foydalanishning yolg’on nuqtalarini tashkil etishi mumkin. Abonentlar, hech shubhalanmasdan foydalanishning ushbu yolg’on nuqtasiga murojaat etadilar va uni o’zining muhim rekvizitlaridan, masalan, autentifikatsiya axborotidan xabardor qiladilar. Hujumning bu xili tarmoqdan foydalanishning haqiqiy nuqtasini "bo’g’ish" maqsadida ba’zida to’g’ridan-to’g’ri bo’g’ish bilan birgalikda amalga oshiriladi (5.6-rasm).

Simli tarmoqdan foydalanuvchilar ham, bilmasdan tarmoqni hujumga ochib berib foydalanishning yolg'on nuqtalarining o’rnatilishiga sababchi bo’lishlari mumkin. Ba’zida foydalanuvchi, qulaylikka intilib, simsiz aloqa taqdim etuvchi foydalanishning simsiz nuqtalarini o’rnatadi, ammo xavfsizlik muammosini o’ylamaydi. Bu nuqtalar simli tarmoqqa kirish uchun "orqa eshik" vazifasini bajarishi mumkin, chunki ular turli hujumlarga duchor bo’ladigan konfiguratsiyada o’rnatiladi.

Hujumlarnnng anonimligi. Simsiz foydalanish hujumning to’liq anonimligini ta’minlaydi. O’rnatilgan joyni aniqlovchi mos tarmoq asbob-uskunasi bo’lmasa, hujum qiluvchi anonimlikni osongina saqlashi va simsiz tarmoq ta’siri hududidagi har qanday joyda bekinishi mumkin. Bunday holda niyati buzuqni tutish qiyin, ishni sudga oshirish esa undan ham qiyin.



5.6-rasm. Foydalanishning yolg’on nuqtasi

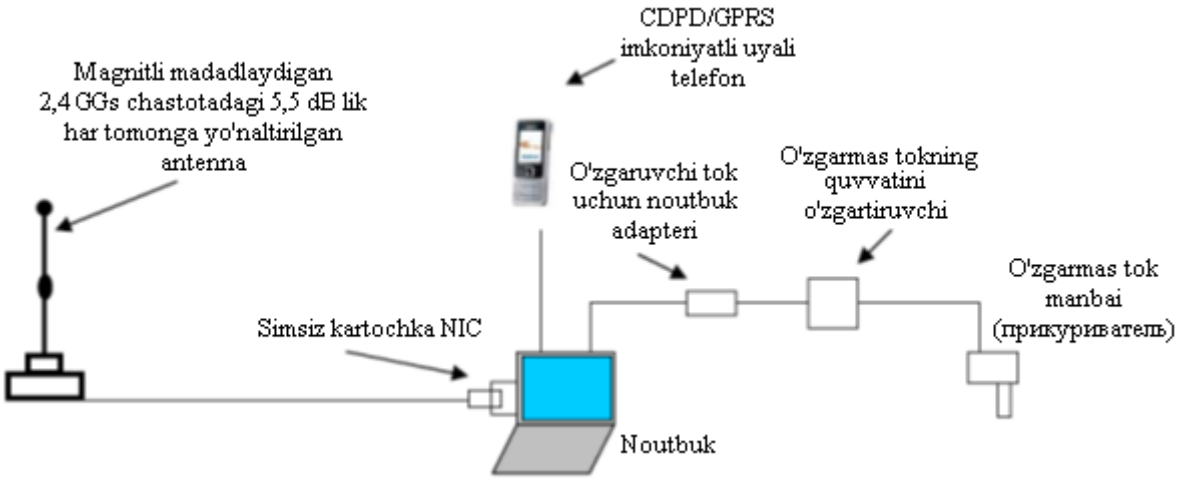
Ta’kidlash lozimki, aksariyat firibgarlar tarmoqni, ularning ichki resurslariga hujum qilish uchun emas, balki Internetdan tekin anonim foydalanish uchun o’rganadilar va Internet himoyasida boshqa tarmoqlarni hujumlaydilar.

"Mijoz-mijoz" xilidagi hujumlar. Tarmoqning barcha abonentlari hujumlanishi mumkin. Birinchi muvaffakiyatdan so’ng hujum qiluvchi korporativ yoki telekommunikatsiya tarmog’idan foydalanish huquqiga ega bo’ladi. Aksariyat tarmoq ma’murlari xavfsizlik rejimiga talabni oshirishga yoki shaxsiy tarmoqlararo ekranlarni (brandmauerlarni) o’rnatishga yetarlicha e’tibor bermaydilar. Shu sababli, simsiz tarmoq mijozlariga muvaffaqiyatli hujumlar niyati buzuqga foydalanuvchilarning ismini va parolini ochish, demak, boshqa tarmoq resurslaridan foydalanish imkonini berishi mumkin.

Tarmoq asbob-uskunalariga hujumlar. Noto’gri konfiguratsiyalangan asbob-uskunalar hujum qiluvchilar uchun birinchi "xo’rak" hisoblanadi va tarmoqqa keyingi suqilib kirishga yo’l ochadi. Hujumlarning asosiy ob’ektlari - marshrutizatorlar, uzib-ulagichlar, arxivlarni saqlovchi serverlar va foydalanish serverlari.

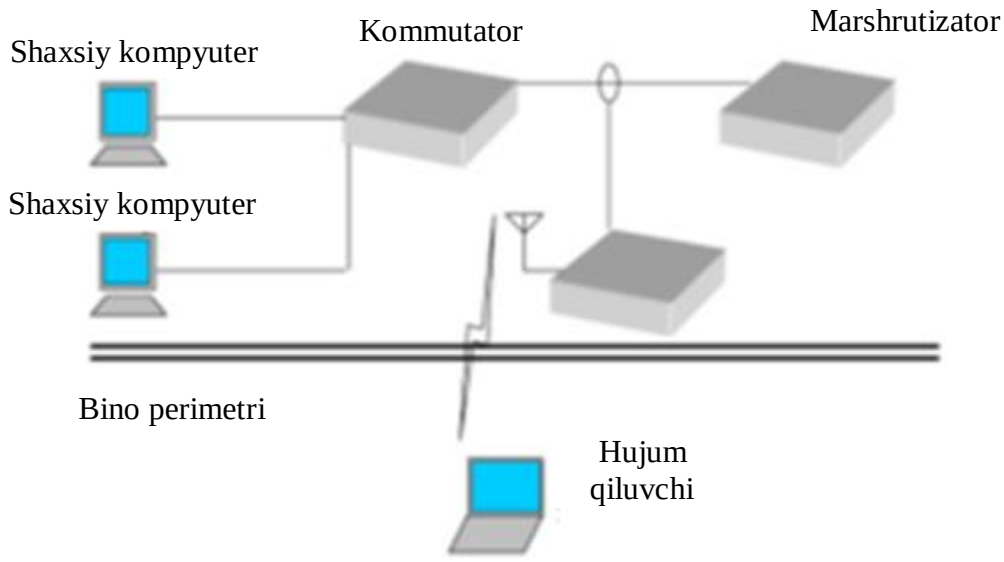
Maxfiy simsiz kanallar. Simsiz tarmoq foydalanuvchilari tarmoqni yaratish yoki baholash jarayonida yana bir omilni hisobga olishlari zarur. Simsiz foydalanish nuqtasining narxi past hamda dasturiy ta'minot, standart noutbuk va NIC-kartalar asosida foydalanish nuqtasini yaratish yetarlicha oson bo’lganligi sababli, nokorrekt konfiguratsiyalangan yoki simli tarmoqda o’ylamasdan joylashtirilgan simsiz asbob-uskunani ziyraklik bilan kuzatish talab etiladi. Bu asbob-uskuna (5.7-rasm) simli

infratuzilmada juda sezilarli "raxnalar" hosil qilishi mumkinki, ular tarmoqdan bir necha kilometr uzoqdagi hujum qiluvchilar diqqatini tortishi mumkin.



5.7-rasm. "Simsiz urushni" olib borish asbob-uskunasi

Xuddi shunga o’xshash konstruksiya yordamida o’ziga xos "simsiz ko’prik" o’tkazish va foydalanish nuqtalarining butun zanjirini tashkil qilgan holda tarmoqdan ma’lumotlarni himoyalangan bino tashqarisida chiqarib olish mumkin (5.8-rasm).



5.8-rasm. "Orqa eshik" ko’rinishidagi tarmoqdan foydalanish

Rouming muammosi. Simsiz tarmoqning simli tarmoqdan yana bir muhim farqi foydalanuvchining tarmoq bilan aloqani uzmasdan joyini o'zgartirish qobiliyatidir. Rouming konsepsiyasi turli simsiz aloqa standartlari SDMA (Code Division Multiple Access), GSM (Global System for Mobile Communications) va simsiz Ethernet uchun bir xil. TSR/IRning ko'pgina tarmoq ilovalari server va mijoz IP-adreslarining o'zgarmasligini talab etadi, ammo tarmoqdagi rouming jarayonida abonent albatta uning bir joyini tark etib, boshqa joyiga qo'shiladi. Simsiz tarmoqlarda mobil IP-adreslarning va boshqa rouming mexanizmlarining ishlatilishi ushbu talabga asoslangan.

Mobil IP-aloqaning asosiy g'oyasi - foydalanuvchining turgan joyini qaydlash va trafikni qayta yo'naltirish. Abonent turgan joyiga bog'liq bo'lmagan adres TCP/IP - ulanishni madadlaydi, foydalanuvchi turgan joyiga bog'liq bo'lgan vaqtincha adres esa lokal tarmoq resurslari bilan ulanishni ta'minlaydi. IP mobil tizimi uchun uchta tartibga soluvchi talablar mavjud: mobil uzeli (foydalanuvchining simsiz qurilmasi), uy agenti (uy tarmog'ida joylashgan server) va ajnabiy agent (rouming uzatuvchi tarmoqda joylashgan server). Mobil uzeli yangi tarmoqqa o'tganida, u turgan joyiga bog'liq bo'lgan vaqtincha IP-adres olinadi va ajnabiy agentda qaydlanadi. So'ngra ajnabiy agent uy agenti bilan bog'lanib mobil agentning o'ziga bog'langanligini xabar qiladi. Shu ondan boshlab barcha paketlar ajnabiy agent - rouming orqali uy agentiga yo'naltiriladi.

Kriptohimoyalash tahdidlari. CDMA, GSM uyali tarmoqlarda va simsiz Ethernet-tarmoqda axborotning konfidensialligini va yaxlitligini taminlash maqsadida kriptografik vositalar ishlatiladi. Ammo xatoliklarga yo'l qo'yish kommunikatsiyaning buzilishiga va axborotning yomon niyatda ishlatilishiga olib keladi.

WEP (Wired Equivalent Privacy - simsiz tarmoq darajasidagi maxfiylik) - 802.11 xilidagi tarmoq xavfsizligini ta'minlash uchun yaratilgan kriptografik mexanizm. WEPni tatbiq etishdagi xatoliklar va boshqarish muammolari uni befoyda qilib qo'ydi. Ushbu mexanizm barcha foydalanuvchilar ishlatadigan yagona statik kalitga ega. Ethernet tarmoqda niyati buzuq odamga bir necha soat mobaynida kalitni tiklashga imkon beruvchi vositalar mavjud. Shu sababli, WEPga autentifikatsiya va konfidensiallik vositasi sifatida ishonish mumkin emas. Tavsiflangan kriptografik usullarni ishlatilgani, umuman ishlatilmaganiga qaraganda

yaxshiroq, ammo yuqorida keltirilgan hujumlardan himoyalashning boshqa usullari zarur.

5.3. Axborot xavfsizligini buzuvchining modeli

Bo'lishi mumkin bo'lgan tahdidlarni oldini olish uchun nafaqat operatsion tizimlarni, dasturiy taminotni himoyalash va foydalanishni nazorat qilish, balki buzuvchilar turkumini va ular foydalanadigan usullarni aniqlash lozim.

Sabablar, maqsadlar va usullarga bog'liq holda axborot xavfsizligini buzuvchilarni to'rtta kategoriyaga ajratish mumkin:

- sarguzasht qidiruvchilar;
- g'oyali xakerlar;
- xakerlar-professionallar;
- ishonchsiz xodimlar.

Sarguzasht qidiruvchi, odatda, yosh, ko'pincha talaba yoki yuqori sinf o'quvchisi va unda o'ylab qilingan hujum rejasi kamdan-kam bo'ladi. U nishonini tasodifan tanlaydi, qiyinchiliklarga duch kelsa chekinadi. Xavfsizlik tizimida nuqsonli joyni topib, u maxfiy axborotni yig'ishga tirishadi, ammo hech qachon uni yashirincha o'zgartirishga urinmaydi. Bunday sarguzasht qidiruvchi muvaffaqiyatlarini faqat yaqin do'stlari-kasbdoshlari bilan o'rtoqlashadi.

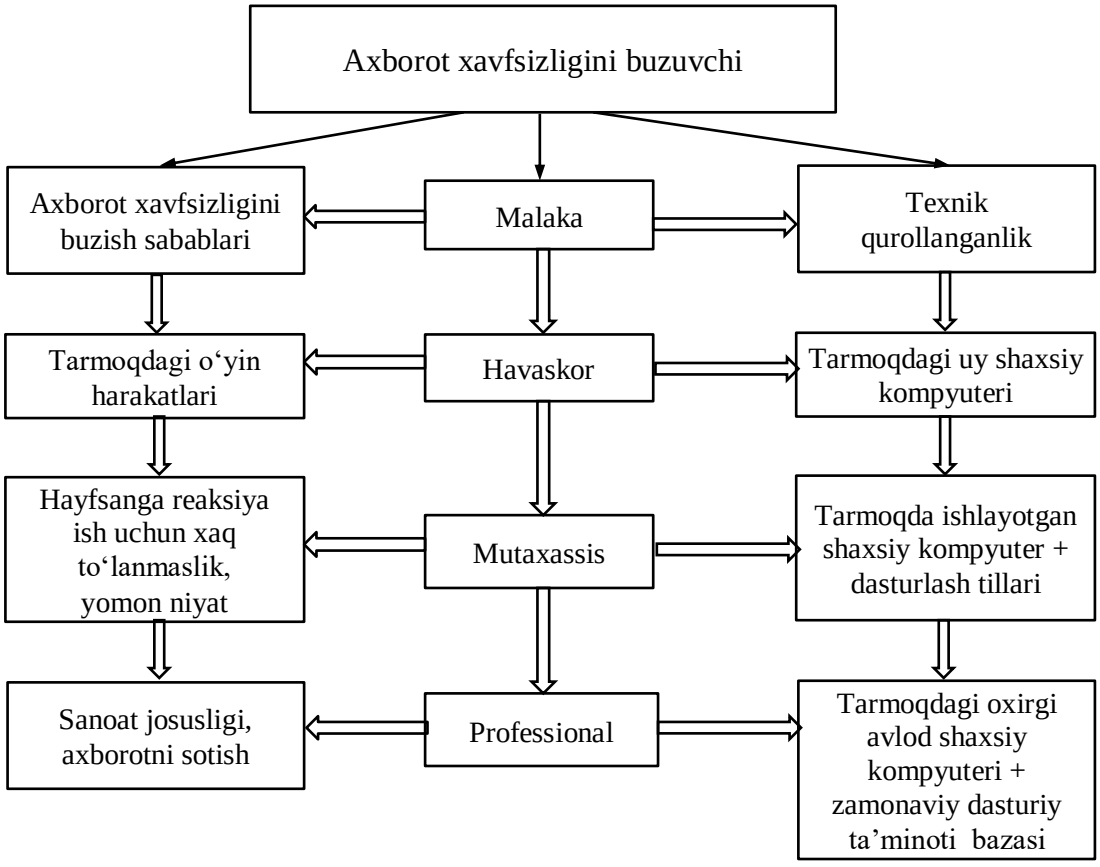
G'oyali xaker - bu ham sarguzasht qiduruvchi, ammo mohirroq. U o'zining etiqodi asosida muayyan nishonlarni (xostlar va resurslarni) tanlaydi. Uning yaxshi ko'rgan hujum turi Web-serverning axborotini o'zgartirishi yoki, juda kam hollarda, hujum qilinuvchi resurslar ishini blokirovka qilish. Sarguzasht qidiruvchilarga nisbatan g'oyali xakerlar muvaffaqiyatlarini kengroq auditoriyada, odatda axborotni xaker Web-uzelda yoki Usenet anjumanida joylashtirilgan holda e'lon qiladilar.

Xaker-professional harakatlarning aniq rejasiga ega va ma'lum resurslarni mo'ljallaydi. Uning hujumlari yaxshi o'ylangan va odatda bir necha bosqichda amalga oshiriladi. Avval u dastlabki axborotni yig'adi (operatsion tizim turi, taqdim etiladigan servislar va qo'llaniladigan himoya choralari). So'ngra u yig'ilgan ma'lumotlarni hisobga olgan holda hujum rejasini tuzadi va mos instrumentlarni tanlaydi (yoki hatto ishlab chiqadi). Keyin, hujumni amalga oshirib, maxfiy axborotni oladi va nihoyat harakatlarining barcha izlarini yo'q qiladi. Bunday hujum qiluvchi

professional, odatda, yaxshi moliyalanadi va yakka yoki professionallar komandasida ishlashi mumkin.

Ishonchsiz xodim o'zining harakatlari bilan sanoat josusi etkazadigan muammoga teng (undan ham ko'p bo'lishi mumkin) muammoni tug'diradi. Buning ustiga uning borligini aniqlash murakkabroq. Undan tashqari unga tarmoqning tashqi himoyasinn emas, balki faqat, odatda, unchalik qatiy bo'lmagan tarmoqning ichki himoyasini bartaraf qilishiga to'g'ri keladi. Ammo, bu holda uning korporativ ma'lumotlardan ruxsatsiz foydalanishi xavfi boshqa har qanday niyati buzuqnikidan yuqori bo'ladi.

Yuqorida keltirilgan axborot xavfsizligini buzuvchilar kategoriyalarini ularni malakalari bo'yicha guruhlash mumkin: xavaskor (sarguzasht kidiruvchi), mutaxassis (g'oyali xaker, ishonchsiz xodim), professional (xaker-professional). Agar bu guruhlar bilan xavfsizlikning buzilishi sabablari va har bir guruhnnng texnik qurollanganligi taqqoslansa, axborot xavfsizligini buzuvchnnnng umumlashtirilgan modelini olish mumkin (5.9-rasm).



5.9-rasm. Axborot xavfsizligini buzuvchining modeli

Axborot xavfsizligini buzuvchi, odatda ma'lum malakali mutaxassis bo’lgan holda kompyuter tizimlari va tarmoqlari xususan, ularni himoyalash vositalari xususida barcha narsalarni bilishga urinadi. Shu sababli buzuvchining modeli quyidagilarni aniqlaydi:

- buzuvchi bo’lishi mumkin bo’lgan shaxslar kategoriyasi;
- buzuvchining bo’lishi mumkin bo’lgan nishonlari va ularnnng muhimlik va xavfsizlik darajasi bo’yicha rutbalanishi;
- buzuvchining malakasi xususidagi taxminlar va uning texnik qurollanganligining bahosi;
- buzuvchining harakat xarakteri bo’yicha cheklashlar va taxminlar.

Tizimdan ruxsatsiz foydalanishga majbur etish sabablarining diapazoni yetarlicha keng: kompyuter bilan o’ynaganidagi hayajon ko’tarinkiligidan to "jirkanch" menejer ustidan hokimlik hissiyotigacha. Bu bilan nafaqat ko’ngil ochishni xohlovchi havaskorlar, balki professional dasturchilar ham shug’ullanadi. Ular parolni tanlash, faraz qilish natijasida yoki boshqa xakerlar bilan almashish yo’li orqali ko’lga kiritadilar. Ularning bir qismi nafaqat fayllarni ko’rib chiqadi, balki fayllarning mazmuni bilan qiziqa boshlaydi. Bu jiddiy tahdid hisoblanadi, chunki bu holda beozor sho’xlikni yomon niyat bilan qilingan harakatdan ajratish qiyin bo’ladi.

Yaqin vaqtgacha rahbarlardan norozi xizmatchilarning o’z mavqelarini suiiste’mol qilgan holda tizimni buzishlari, undan begonalarning foydalanishlariga yo’l qo’yishlari yoki tizimni ish holatida qarovsiz qoldirishlari tashvishlantirar edi. Bunday harakatlarga majbur etish sabablari quyidagilar:

- hayfsanga yoki rahbar tomonidan tanbehga reaksiya;
- ish vaqtidan tashqari bajarilgan ishga firma haq to’lamaganidan norozilik;
- firmani qandaydir yangi tuzilayotgan firmaga raqib sifatida zaiflashtirish maqsadida qasos olish kabi yomon niyat.

Rahbardan norozi xodim jamoa foydalanuvchi hisoblash tizimlariga eng katta tahdidlardan birini tug’diradi. Shuning uchun ham xakerlar bilan kurashish agentligi individual kompyuter sohiblariga jon deb xizmat ko’rsatadilar.

Professional xakerlar hisoblash texnikasini va aloqa tizimini juda yaxshi biladigan kompyuter fanatlari (mutaassiblari) hisoblanadi. Tizimga kirish uchun professionallar omadga va farazga tayanmaydilar, balki qandaydir tartibni va tajribani ishlatadilar. Ularning maqsadi - himoyani

aniqlash va yo’qotish, hisoblash qurilmasining imkoniyatlarini o’rganish va maqsadiga erishish mumkinligi to’g’risida qarorga kelish.

Bunday professional xakerlar kategoriyasiga quyidagi shaxslar kiradi:

- siyosiy maqsadni ko’zlovchi jinoiy guruhlarga kiruvchilar;
- sanoat josuslik maqsadlarida axborotni olishga urinuvchilar;
- tekin daromadga intiluvchi xakerlar guruhi.

Umuman, professional xakerlar xavf-xatarni minimallashtirishga urinadilar. Buning uchun ular birga ishlashga firmada ishlaydigan yoki firmadan yaqinda ishdan bo’shatilgan xodimlarni jalb etadilar, chunki begona uchun bank tizimiga kirishda oshkor bo’lish xavfi juda katta. Haqiqatan, bank hisoblash tizimlarining murakkabligi va yuqori tezkorligi, hujjatlarni yurg’izish va tekshirish usullarining muntazam takomillashtirilishi begona shaxs uchun xabarlarni ushlab qolish yoki ma’lumotlarni o’g’irlash maqsadida tizimga o’rnashishiga imkon bermaydi. Professional xakerlar uchun yana bir qo’shimcha xavotir - tizimdagi bir komponentning o’zgarishi boshqa bir komponentning buzilishiga olib kelishi va xatardan darak beruvchi signalga sabab bo’lishi mumkin.

Xakerlar xavf-xatarni kamaytirish maqsadida odatda moliyaviy va oilaviy muammolarga ega bo’lgan xodimlar bilan kontaktga kiradilar. Ko’pgina odamlar hayotida xakerlar bilan to’qnashmasliklari mumkin, ammo alkagolga yoki qimorga ruju qo’ygan xodimlar bilmasdan jinoiy guruh bilan bog’langan qandaydir bir bukmekerdan qarzdor bo’lib qolishlari mumkin. Bunday xodim qandaydir o’yin-kulgi kechasida suhbatdoshining professional agent ekanligiga shubha qilmagan holda ortiqcha gapirib yuborishi mumkin.

6 BOB. MOBIL OPERATSION TIZIM XAVFSIZLIGI

6.1. 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.

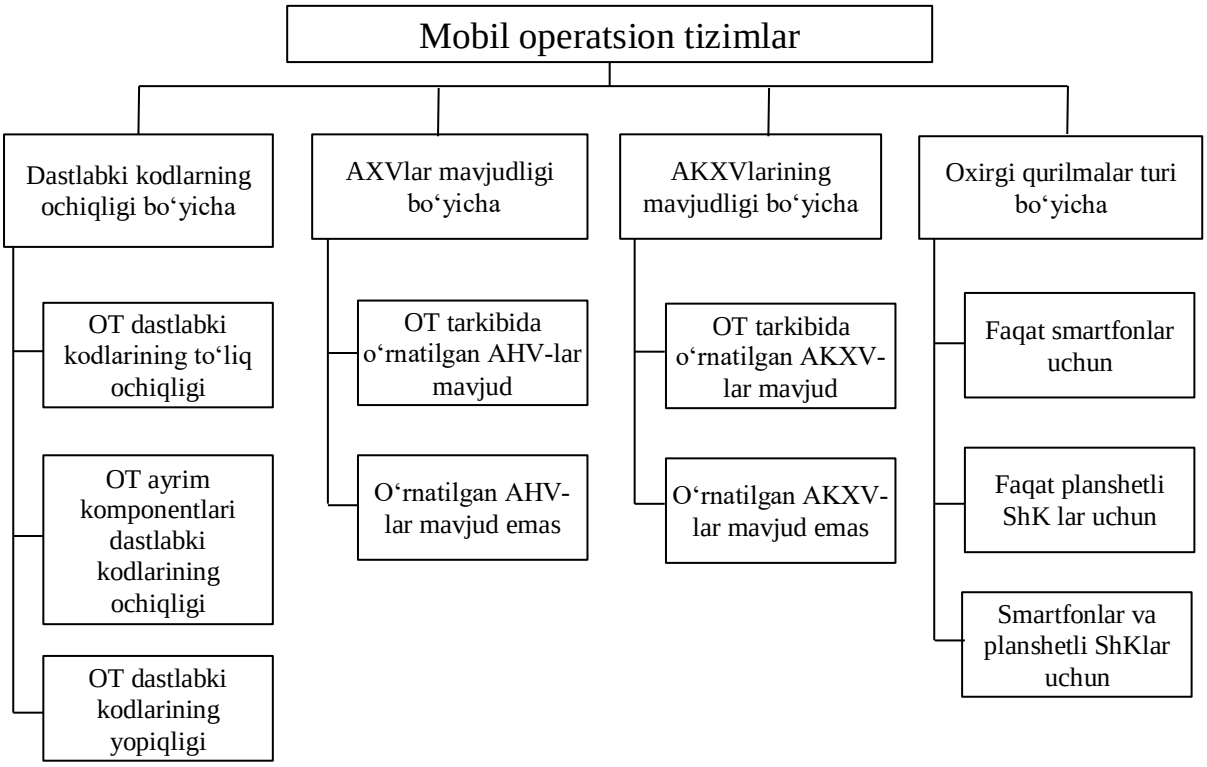
Mobil operatsion tizimlarni quyidagi alomatlari bo'yicha tasniflash mumkin (6.1-rasm):

- 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.

6.2. 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).

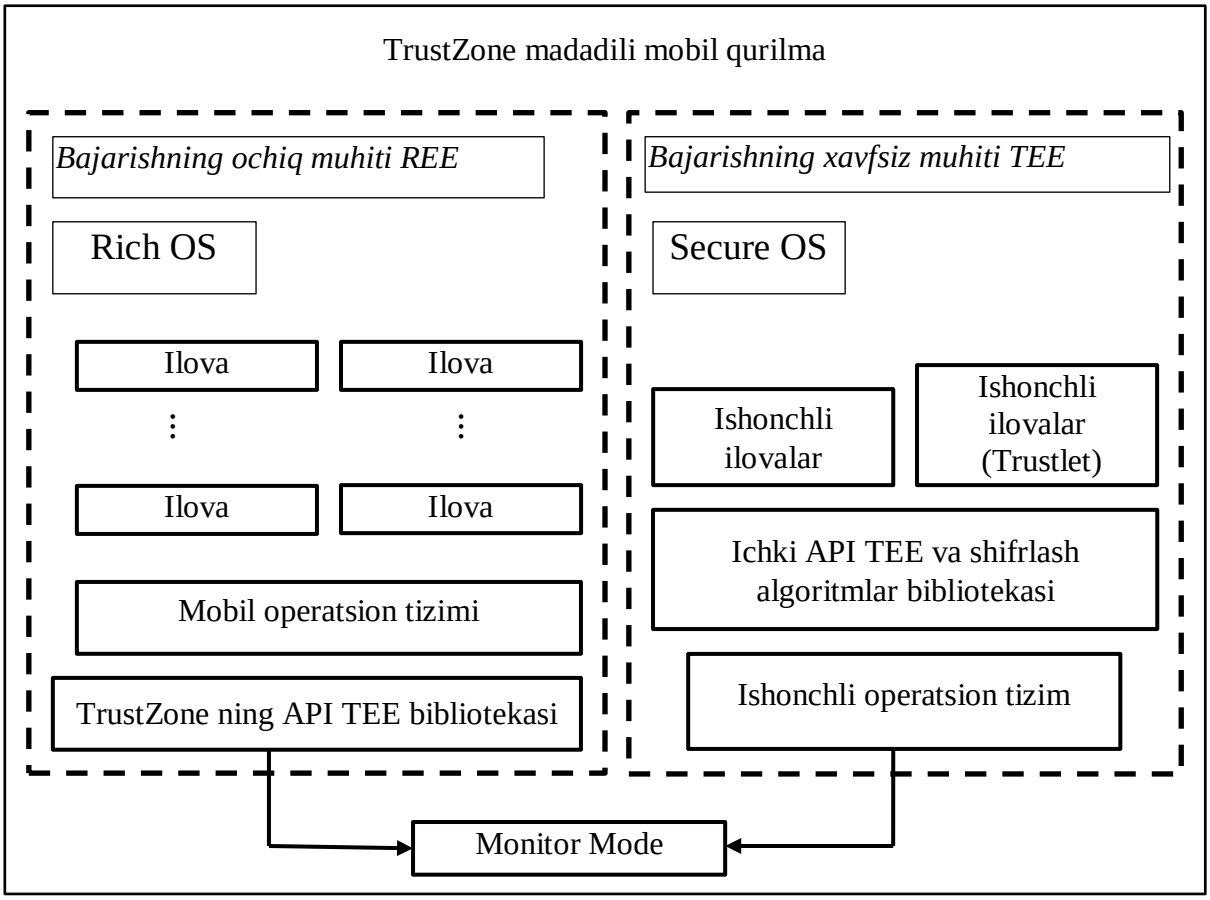
Rich OS - to’liq funksional operatsion tizim, ya’ni bibliotekalar, servislar va xizmatlar nabori. Bular tizim komponentlarini (ichki va chetki ilovalarni) boshqarishning umumiy funksiyalarini ta’minlaydi.

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:

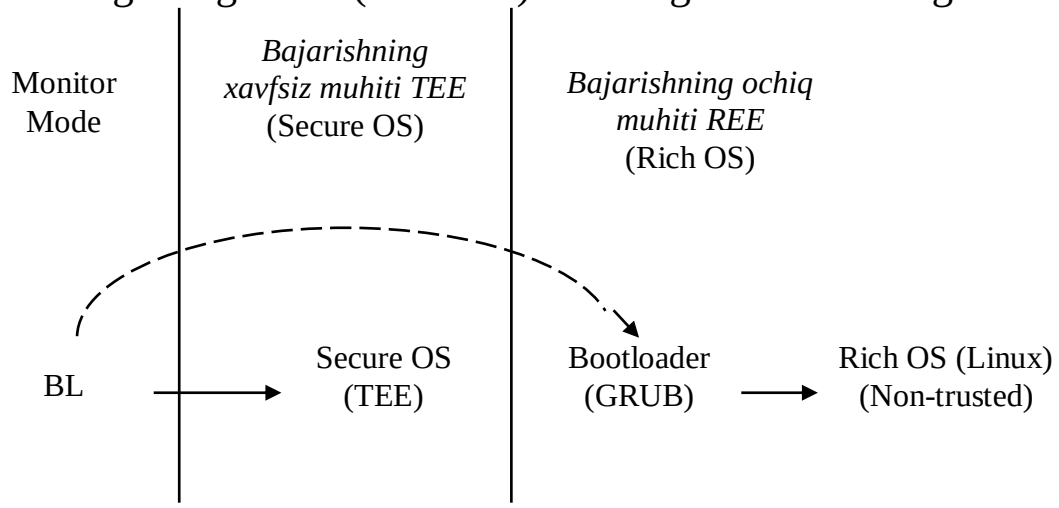
- jarayonlarni nazoratlash, ya’ni keraksizini tezda to’xtatish imkoniyati bilan barcha ishga solingan jarayonlarni kuzatish;
- tarmoq interfeyslari monitoringini amalga oshirish, ya’ni ishlatiluvchi tarmoq interfeyslarini kuzatish;

- 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

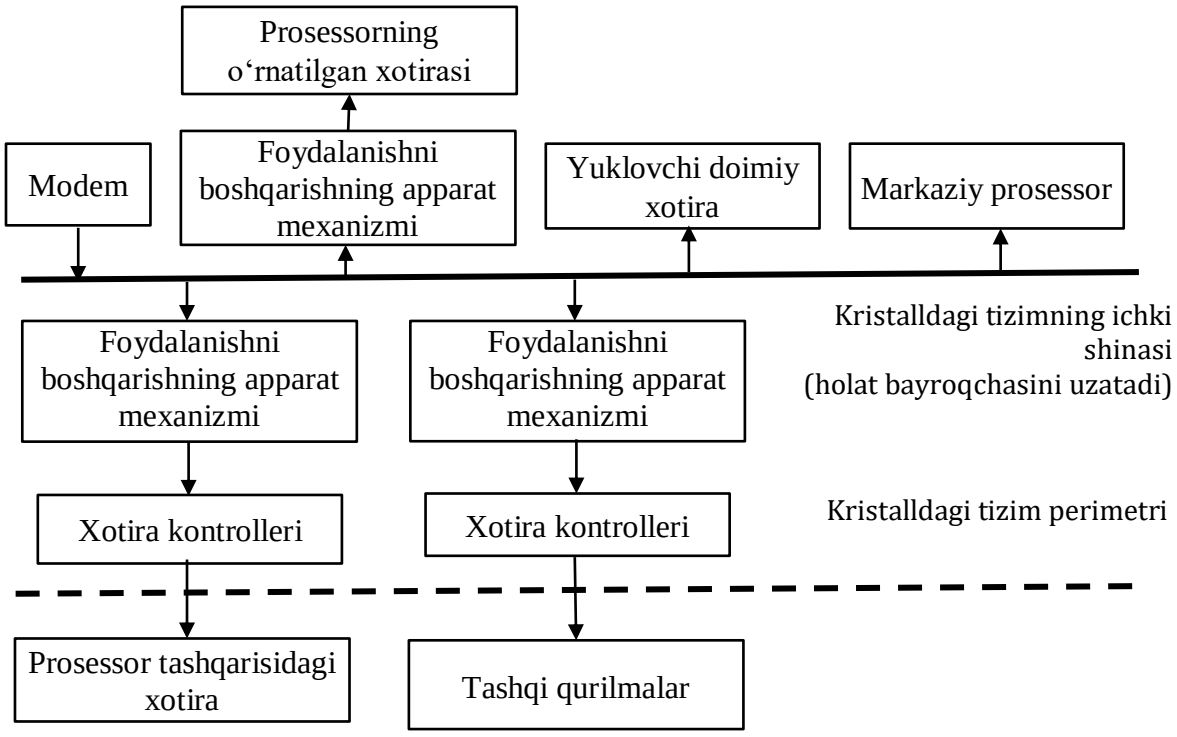
Prosessor Monitor Mode rejimida ish boshlaydi, ya’ni bajarishning xavfsiz muhiti TEEda bo’ladi va TEEning asosi hisoblanuvchi Secure OS ga bootloader ni yuklashni boshlab beradi. (BL-yuklovchi - Bootloader – yuklash jarayonining normal rejimda amalga oshirilishi uchun operatsion tizim yadrosini nazoratlovchi 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.

6.3. Android va iOS operatsion tizimlar xavfsizligini ta’minlash mexanizmlarining qiyosiy tahlili

Hozirda Android va iOS operatsion tizimlar (platformalar) keng tarqalgan. Quyida ularning xavfsizligi masalalari va ushbu masalalarni amalga oshirish mexanizmlarining qiyosiy tahlili yoritilgan.

1. Ishlab chiqaruvchi kompaniyalar nuqtai nazaridan xavfsizlikning asosiy riski – ular ilovalarining buzib ochilishi natijasidagi mijozlarning va biznesning yuqotilishi. Agar mobil ilovalarning lokal va veb-hujumlarga qarshi tura olish qobiliyati ko’rilsa, ikkala Android va iOS operatsion tizimlar taxminan teng sharoitdadurlar.

2. Android uchun ilovalar, Objective-C tilida iOS uchun yozilgan dasturlardan farqli holda, buferning to’lib-toshishi hujumidan qo’rqmaydigan Java tilida yozilgan dasturlardir. Objective-C tilida yozilgan ilovalar buferning to’lib-toshishi hujumiga zaif, ammo iOS-yaratuvchilari zahirasida bunday zaifliklarni bartaraf etuvchi kerakli mexanizmlar mavjud. Bunday mexanizmlarga, avvalo PIE (Position Independent Executable), SSP (Stack Smashing Protection) va ARC (Automatic Reference Counting) kabi kompilyasiyalar parametrlari taalluqli. Ushbu parametrlar xotirani samarali boshqarishni, buferning to’lib-toshishiga olib keluvchi xatoliklarning bo’lmasligini ta’minlaydi.

Undan tashqari, iOS ning sakkizinchi versiyasining taqdimotida Objective-C tili o’rniga yangi dasturlash tili Swift taqdim etildi. Apple kompaniyasining aytishicha yangi til oldingisiga qaraganda o’rganishga oson va xavfsizliroq.

Shunday qilib, Android va iOS-ilovalar bir xil yahshi himoyalanishi mumkin va ushbu ilovalarni buzib kirish ehtimolligi bevosita ishlab chiqaruvchilar mahoratiga bog’liq.

3. Mobil qurilmalardan oddiy foydalanuvchilarning xavfsizligi ular foydalanadigan mobil operatsion tizim xavfsizligiga bog’liq. Xatto smartfonda faqat yaxshi himoyalangan ilovalar o’rnatilgan bo’lsa ham, oxirgi foydalanuvchilar operatsion tizimning raxnalari orqali muvaffaqiyatli hujumga duchor bo’lishlari mumkin. Agar mobil ilovalarning himoyalanganlik alomati bo’yicha ikkala operatsion tizim bir xil sathda bo’lsa, Android va iOS operatsion tizimlar, o’zlarining xavfsizligi nuqtai nazaridan, o’zaro anchagina farqlanadi.

4. Ikkala operatsion tizim himoyasining mexanizmlarida tizimli qismning faqat o’qish uchun foydalanuvchanligi va yadro sathida bajariluvchi jarayonlarning farqlanishi kabi xavfsizlikning bazaviy prinsiplarining mavjudligini aytish lozim. Ikkala operatsion tizimda tizimli qismning yozish uchun foydalanuvchan emasligi tizim fayllarining tasodifiy yoki maqsadli o’zgarishini bartaraf etadi. Ikkala operatsion tizimda "qumdon" (sandbox) prinsipi ham amalga oshirilgan. Bu degani, har bir ilova alohida konteynerda ishlaydi va tizimli fayllardan yoki boshqa ilovalar resurslaridan foydalana olmaydi.

5. Android va iOS operatsion tizimlarning asosiy farqlari yadro sathida foydalanishning farqlanishi prinsiplariga, magazinlarga yuklanuvchi operatsion tizimni verifikatsiyalash jarayoniga va o’rnatiluvchi ilovalardan foydalanish huquqlarini nazoratlash prinsiplariga taalluqli.

6. Ishlab chiqaruvchilar tomonidan zararli dasturiy ta’minotning mavjud emasligini ta’minlash bo’yicha ko’riluvchi zarur choralar:

- iOS-ilovalar zaiflikka va Apple ishlanmalar standartlariga mosligiga sinchiklab tekshiriladi. iOS ga o’rnatiluvchi har bir ilova, faqat ishlab chiqaruvchini kerakli verifikatsiyalashdan so’ng Apple kompaniyasi tomonidan beriladigan "iOS Developer Program" dasturning noyob sertifikati bilan imzolanadi. iOS da ilovalardan foydalanish huquqlarini moslanuvchan taqsimlash amalga oshirilgan. Har bir foydalanish

kategoriyasi, kameradan yoki GPS dan foydalanish bo’lsin, foydalanuvchi tomonidan tasdiqlanishi yoki rad etilishi lozim;

- Google Play da yuklashdan oldin ilovalar tekshirilmaydi, ammo o’zining magazinini bo’lishi mumkin bo’lgan zararli dastur ta’minotining mavjudligiga muntazam skanerlaydi. Android boshqaruvida qurilmaga yangi ilovani o’rnatishda foydalanuvchiga ushbu ilovaga kerakli foydalanish huquqlarining to’liq ro’yxati ko’rsatiladi. Ushbu ro’yxat bo’yicha foydalanuvchi bo’lishi mumkin bo’lgan zararli dasturiy ta’minotni aniqlashi va uning o’rnatilishini bekor qilishi mumkin.

7. Operatsion tizimlarning zaifliklari:

- iOS, to’la ochiq operatsion tizim bo’lishiga qaramasdan, ma’lum zaifliklar (CVE) soni bo’yicha Android dan ilgarilab ketgan. Buning ustiga afzallik yetarlicha aytarli darajada: 2014 yil o’rtasida iOS ning barcha versiyalarining jami 335ta, Android esa faqat 36ta zaifliklarni tashkil etadi.

Apple operatsion tizimda iOS-8 ning beta versiyasining taqdimoti tufayli hujum uchun yangi vektorlar paydo bo’ldi: begona klaviaturalar, yangi SDK da, yangi API chaqiruvlari to’plami va "aqlli uyni" boshqarish tizimi. Zaifliklarning bunday katta miqdoriga qaramay, iOS foydalanuvchilari o’zlarining himoyalanganliklari xususida xavotir olmasliklari kerak, chunki Apple, odatda, yangi zaifliklarni tezda yopadi;

- Google ham, o’z navbatida, o’zining operatsion tizimi xavfsizligini kuchaytirishga tayanadi. Android ning 4.4 versiyasida yadro sathida foydalanishni majburiy rejimda nazoratlovchi SELinux moduli paydo bo’ldi. Ushbu modul Linux xavfsizligining bazaviy modeliga bog’liq bo’lmagan holda ishlaydi.

Shunday qilib, operatsion tizimning shaxsiy xavfsizligi nuqtai nazaridan ikkala operatsion tizimdan birortasi ham g’olib hisoblanmaydi. Android ham, iOS ham xaker hujumlaridan himoyalanishning quvvatli mexanizmlariga ega va ikkala Google va Apple kompaniyalari o’zlarining tizimlari xavfsizligiga yuqori e’tibor beradilar.

8. Oxirgi yillarda ishchi masalalarni echishda o’zlarining shaxsiy mobil qurilmalarini ishlatuvchi foydalanuvchilar soni ko’paymoqda. BYOD (Bring Your Own Device) nomini olgan ushbu tendensiya o’zida korporatsiya uchun xavfsizlikning ma’lum riskini eltadi. Niyati buzuqlar zaif yoki yo’qolgan smartfon yoki planshet yordamida kompaniyaning maxfiy hujjatlaridan yoki ichki resurslaridan, masalan pochtadan, ruxsatsiz foydalanishlari mumkin. Shu sababli, kompaniya tarmog’ida ishlovchi mobil qurilmalar xavfsizligi siyosatini markazlashgan boshqarishga imkon

beruvchi MDM (Mobile Device Management) xilidagi yechimlardan foydalanishga ehtiyoj paydo bo'ladi.

Korporatsiya darajasidagi xavfsizlik nuqtai nazaridan Apple ning operatsion tizimi Android ga nisbatan qator afzalliklarga ega. iOS o'zining zahirasida konfiguratsiya profillari, masofaviy to'liq dastlabki holatiga tiklash va begona MDM-yechimlarni o'rnatilgan madadlash kabi qurilmalarni markazlashgan quvvatli vositalarga ega. Android asli ko'rinishida bunday imkoniyatlarga ega emas. MDM-tizimlarga integrallash uchun Android ga oldindan maxsus dasturiy ta'minotni o'rnatish kerak.

Alohida aytib o'tish lozimki, Samsung kompaniyasi Android dagi qurilmalar ishlab chiqaruvchilariga nisbatan korporativ xavfsizlik masalalarida oldinga qarab ilgarilab ketdi. So'z SAFE (Samsung For Enterprise) dasturi va KNOX (Samsung konteyneri) ustqurmasi xususida boradi.

Android va iOS operatsion tizimlarning xavfsizlik nuqtai nazaridan afzalliklari va kamchiliklari:

Android

Afzalliklari:

- xavfsizlik tadqiqotchilari uchun ochiqligi;
- buferning to'lib-toshishiga immunitetligi;
- yadro sathida SELinux foydalanishning qat'iy nazorati.

Kamchiliklari:

- Google Play magazinida bo'lishi mumkin bo'lgan zararli dasturiy ta'minotning katta miqdori;
- korporativ xavfsizlikni ta'minlash imkoniyatining kuchsizligi;
- himoya usullarini standartlashni murakkablashtiruvchi turli ishlab chiqaruvchilardan operatsion tizim versiyalari va qurilmalar modellari sonining ko'pligi.

iOS

Afzalliklari:

- App Store ga yuklanuvchi ilovalarning sinchiklab tekshirilishi natijasida ilovalar magazinida zararli dasturiy ta'minot deyarli mavjud emasligi;
- xavfsizlik insidentlariga Apple ning tezkor reaksiyasi;
- korporativ xavfsizlik tizimini madadlash bo'yicha imkoniyatlarining kattaligi.

Kamchiliklari:

- operatsion tizimning o’zida ma’lum zaifliklar sonining kattaligi;
- hujum uchun mumkin bo’lgan vektorlar sonining o’sishi.

Xulosa sifatida aytish mumkinki, amalda telefon tanlanganida uning himoyalanishi asosiy kriteriy deb hisoblovchilar topilmasa kerak. Bu to’g’ri, chunki Android va iOS tizimlar o’zlarining foydalanuvchilarini himoya qilish imkoniyatlari bo’yicha bir darajada.

7 BOB. MOBIL ILOVALARDAGI ZAIFLIKLAR

7.1. Mobil ilovalar tasnifi

Mobil ilovalar deganda u yoki bu masalani yechishga mo'ljallangan, mobil telefonda, smartfonda yoki kommunikatsiyada ishlatilishi uchun maxsus yaratilgan kompyuter dasturlari tushuniladi.

Mobil ilovalarni tasniflashda bir necha yondashishlar mavjud.

O'rnatish usuli bo'yicha: pulli va bepul.

Kontent turi bo'yicha: ko'ngil ocharli (multimediali), kommunikatsiyali, navigatsiyali, ma'lumot beradigan va tatbiqiy.

Ishlab chiqarish usuli bo'yicha: nativ ilovalar, mobil saytlar/veb-ilovalar, gibrid ilovalar.

Nativ ilovalar (Native Apps) – o'rnatilishini talab etuvchi ilovalar. Bunday ilovalardan smartfon ekranida ikonkalar orqali foydalanish mumkin. Ular ilovalar magazini (Google Play yoki App Store) orqali o'rnatiladi va muayyan platforma uchun ishlab chiqarilib qurilmalarning (fotokakmera, GPS, akselerometr, kompas, va h.) barcha funksiyalaridan foydalanadi. Bunday ilovalar bildirish xatini jo'natish tizimidan foydalanishlari mumkin va avtonom rejimda (Internetdan foydalanmay) ishlashlari mumkin. Bu ilovalarning, resurslarning katta hajmini talab qiluvchi turi, ammo taklif etilgan muayyan operatsion tizim imkoniyatlaridan maksimal foydalanishga imkon beradi. Nativ ilovalar funksionallik va ishlash tezligi bo'yicha mobil ilovalarning boshqa turlaridan afzal hisoblanadi.

Mobil saytlar/web-ilovalar eng ko'p tarqalgan bo'lib, birmuncha nativ ilovalarga o'xshash mini saytlardan iborat. Ular HTML5 va Java Script tillarida yozilgan va brauzer orqali ishga tushiriladi. Foydalanuvchilar ulardan, ixtiyoriy *web*-saytdan qanday foydalanishsa, shunday foydalanadilar. Web-ilovalar kam pul sarfi va qisqa muddat evaziga katta natijalarga erishishga imkon beradi. Mobil saytning yana bir afzalligi – uning universalligi, ya'ni barcha operatsion tizimlarda ishlatilishi mumkin.

Gibrid ilovalar qisman nativ, qisman veb-ilovalardan iborat. Nativ ilovalarga o'xshab, ular ilovalar magazinida joylashgan va qurilmaning ko'pgina funksiyalaridan foydalana oladilar. Web-ilovalarga o'xshab, ular HTML ga asoslanadilar, brauzer esa ilovada o'rnatilgan bo'ladi.

Ilovaning joylashgan joyi bo'yicha:

- *SIM-ilovalar* - SIM Application Toolkit (STK) standartga muvofiq yozilgan SIM-kartadagi ilovalar;
- *Web-ilovalar* – Web-saytlar uchun maxsus versiyalar;
- *muayyan operatsion tizim uchun ishlab chiqilgan mobil ilovalar.*

Muayyan operatsion tizim uchun mobil ilovalar API (application programming interface) tatbiqiy dasturlash interfeysidan foydalanib ishlab chiqiladi. API – smartfonga o'rnatiluvchi ilovalar (biblioteka, servis) taqdim etuvchi tayyor muolajalar, funksiyalar, strukturalar va konstantalar nabori.

Ma'lumotlarni uzatishda ishlatiluvchi texnologiyalarning turi bo'yicha:

- *tarmoq ilovalari* - TCP/IP protokoli ustidan aloqaning xususiy aloqa protokolini, masalan HTTP ni ishlatadi;
- *SIM-ilovalar* - SMS (Short Messaging Service) asosidagi ilovalar;
- *server bilan almashish uchun ilovalar* (qisqa matnli xabarlar ko'rinishida);
- *USSD-ilovalar* - USSD (Unstructured Supplementary Service Data) asosidagi ilovalar. Servis SMS ga o'xshash, ammo qator farqlanishga ega, qisqa xabarlarni uzatishga asoslanadi;
- *IVR-ilovalar* – IVR (Interactive Voice Response) texnologiyasiga asoslanuvchi ilovalar. Texnologiya oldindan yozilgan tovushli xabarlarga va tovush naboriga asoslangan.

7.2. Mobil ilovalarning namunaviy zaifliklari va ulardan himoyalanish choralari

Kompaniyalar va tashkilotlar mobil texnologiyalardan xodimlar ishining unumdorligini va korporativ tizim samaradorligini oshirish maqsadida foydalanadilar. Ammo, xakerlar suqilib kirishning va mobil ilovalar orqali konfidensial axborotdan foydalanishning yangi usullarini topadilar. Ilovalarni ishlab chiqaruvchilari va foydalanuvchilari, mobil ilovalarni noto'g'ri konfiguratsiyalash natijasidagi, mobil qurilmalar xavfsizligining buzilishini bilib qoladilar. So'z, mobil tizimlarining umumiy xavfsizligining jiddiy kamaytiruvchi ilova himoyasidagi bo'shliqlar to'plami xususida boradi. Bu kodni va xavfsizlik konfiguratsiyasi to'liq tekshirmasdan mobil ilovalarning bozorga chiqarilishi tufayli sodir bo'ladi. Shuning uchun, ishlab chiqaruvchilar va

foydalanuvchilar mobil qurilmalarning eng ko’p tarqalgan zaifliklari va ular bilan doimiy kurashishning eng mukammal usullarini bilishlari muhim hisoblanadi.

Quyida mobil ilovalar va qurilmalar moyil 10 ta asosiy zaifliklar va ulardan himoyalanish choralari bo’yicha takliflar bayon etilgan.

1. Arxitekturaviy cheklashlarni chetlab o’tish (Improper Platform Usage).

Zaifliklarning ushbu kategoriyasi operatsion tizim (platforma) va platforma xavfsizligini boshqarishni nazoratlash tizimida o’rnatilgan cheklashlarni chetlab o’tishning o’ziga xos xususiyatlaridan foydalanadi. Ushbu zaiflik Android va iOS platformalariga va boshqa mobil operatsion tizimlarga xos.

Takliflar. Mobil ilovaning server qismida dasturiy kodni qurishning va konfiguratsiyalashning xavfsiz usullaridan foydalanish lozim. Xususan, API-interfeys uni chaqiruvchi shaxsning identifikatsiyasini va vakolatini ishonarli tekshirishi lozim.

2. Ma’lumotlarni xavfli saqlash (Insecure Data Storage).

Ishlab chiqaruvchilar jamoasi, foydalanuvchilar yoki zararli kod konfidensial axborot saqlanuvchi mobil qurilmalarning fayl tizimidan foydalana olmaydilar deb hisoblaydilar. Ammo, fayl tizimini chetlab o’tish va unga suqilib kirishning ko’pgina usullari mavjud:

- ilova yaratuvchi fayllar uchun foydalanish huquqlarini noto’g’ri belgilash. Testlash bosqichida (ishlab chiqaruvchilar) foydalanish huquqlarini ko’pincha belgilaydilar va ularni dasturiy mahsulotni yakuniy chiqarishda tahrirlashni unutadilar. Natijada niyati buzuqlarda ruhsatsiz foydalanishga imkoniyat paydo bo’ladi;

- SD-kartada muhim ma’lumotlarni saqlash. Foydalanuvchilar ko’pincha muhim ma’lumotlarni SD-kartada saqlaydilar. Bunday ma’lumotlardan barcha ilovalar foydalanishlari mumkinligini unutadilar;

- jurnallashtirish. Jurnallar mobil operatsion tizimda sodir bo’ladigan barcha hodisalar xususidagi yozuvlarni ro’yxatga oluvchi fayllardan iborat. Android da har qanday ilova o’rnatilishida jurnallarni o’qish huquqini talab etishi mumkin. Foydalanuvchilarning ko’pchiligi bunga e’tibor bermaydilar. Xavflilik shundan iboratki, foydalanuvchi tomonidan jurnallarni o’qish huquqini olgan har qanday o’rnatiluvchi ilova barcha axborotni o’qish huquqini oladi. Ko’pincha jurnallarga shifrlanmagan sozlash axboroti va shaxsiy ma’lumotlar tushib qoladi;

- superfoydalanuvchi (ma’mur) huquqlarini olish. Smartfon foydalanuvchilari, begona ilovalarni o’rnatish imkoniyatini ta’minlash

maqsadida, ko’pincha qurilmaning fayl tizimidan to’laqonli foydalanishga intiladilar. Apple kompaniyasining mobil qurilmalarida ushbu muolaja Jail Break, Android-cmartfonlarda esa Root-huquqlarni (yoki superfoydalanuvchi huquqlarini) olish deb ataladi. Ta’kidlash lozimki, Jail Break root oddiy opsiya bo’lmay, qurilmaning barcha xavfsizlik tizimining kompрometatsiyasi hisoblanadi.

Takliflar. Mobil qurilma ma’lumotlarini ruxsatsiz foydalanishdan himoyalash choralari:

- muhim ma’lumotlarni SD-kartada saqlamaslik;
- ilovalar o’rnatilishidan avval jurnallashtirishni to’xtatish;
- ilovalarni ishlab chiqarishda foydalanish huquqlarini, foydalanuvchining mobil qurilmasi root-huquqlar orqali kompрometatsiyalangan bo’lishi mumkinligini hisobga olgan holda, sozlash lozim;
- agar tijorat konfidensial axborotning saqlanishini talab etsa, shifrlashdan kengroq foydalanish zarur.

3. Ma’lumotlarning xavfli uzatilishi (transport sathidagi himoyaning yetarli emasligi) (Insecure Communication)

Aloqa manbalari ishonchligi tasdig’ining yetarli emasligi, SSLning noto’g’ri versiyalari, nozik ma’lumotlarni ochiq holda uzatish va h.

Asosiy muammolar:

- ma’lumotlarni uzatishda shifrlash ishlatilmaydi (masalan https o’rniga http protokolining ishlatilishi);
- ma’lumotlarni uzatishda soxta sertifikatlarning ishlatilishi.

Takliflar. Axborot xavfsizligini ta’minlash bo’yicha choralar:

- mobil ilova trafigini tekshirish;
- web-snifferning ishlatilishi. Natijada mobil ilovalar trafigi tahlillanadi va muhim ma’lumotlar https protokoli bo’yicha shifrlangan holda uzatilganligi tekshiriladi;
- ishonchli markazlar tomonidan imzolangan sertifikatlarning ishlatilishi;
- kontent-provayderlardan foydalanilganda tekshirish va foydalanish huquqlarini qo’shish.

4. Xavfli autentifikatsiya (Insecure Authentication)

Ma’lumotlarni himoyalash, odatda, mobil ilovalarning ishlatilishining tipik hollariga nisbatan amalga oshiriladi. Ammo, ko’pgina boshqa vaziyatlar mavjudki, ma’lumotlar kuzatiladi, nusxalanadi, keshlanadi, ro’yxatga olinadi, ekran tasviri va rezerv nusxa yaratiladi.

Ushbu kategoriya oxirgi foydalanuvchinining autentifikatsiyasiga yoki seanslarni noto’g’ri boshqarishga taalluqli. Quyidagilarni o’z ichiga oladi:

- ilova bilan anonim ishlash. Mobil ilovaning himoyalanganligiga talablar web-ilovalar himoyalanganligiga qo’yilgan talablardan farqlanadi. Faraz qilinadiki, foydalanuvchi oflayn rejimida ishlashi mumkin. Shu sababli, ko’pincha ma’lumotlarni keyinchalik sessiyali cookie-fayllarda saqlash orqali onlayn-avtorizatsiya ishlatiladi. Identifikatsiya ma’lumotlari (login va parol) kiritilganidan va ilova foydalanuvchini avtorizatsiyalaganidan so’ng, maxsus identifikatorni saqlaydi. Ushbu identifikator ilova tomonidan keluvchi har bir so’rovda serverga taqdim etiladi. Agar niyati buzuq foydalanuvchi identifikatorini olgan va tizimda sessiyaning IP-adresini yoki sessiya doirasida bittadan ortiq ulanish mavjudligini tekshirish muolajasi amalga oshirilmagan bo’lsa, niyati buzuq foydalanuvchi akkaunti huquqlari bilan tizimdan foydalanishi mumkin;

- kuchsiz parollar. Mobil ilovalarda parollar uzun bo’lishi kerak emas va aksariyat ilovalar to’rt simvolli parollarni yaratishga ruhsat beradi. Bunda parollar aksariyat hollarda shifrlanmay xeshlangan ko’rinishda bazaga joylashtiriladi. Agar niyati buzuq ma’lumotlar bazasidan foydalanishga ruxsat olgan bo’lsa, tayyor xesh-jadval yordamida parolni deshifrlash uning uchun qiyinchilik tug’dirmaydi.

Takliflar. Ushbu tur zaifliklar uchun xavfsizlikni ta’minlash bo’yicha choralar:

- mobil ilovadagi autentifikatsiya web-versiyaga mos bo’lishi lozim;
- uzunligi 6 simvoldan ortiq murakkab parollarni yaratish;
- qurilmani mobil qurilmani boshqarish qurilmasi (mobile-device management, MDM) yoki mobil ilovalar (mobile-application management, MAM) yordamida nazoratlash.

5. Kuchsiz kriptografik bardoshlik (Insufficient Cryptography)

Mobil ilova kuchsiz va g’animlar echa oladigan algoritmdan foydalanishlari mumkin. Chunki ishlab chiqilgan arxitektura jiddiy nuqsonlarga ega yoki kalitlarni boshqarish jarayoni yomon tashkil etilgan.

Taklif. Axborotni himoyalashda murakkab kriptografik muolajalardan foydalanish kerak.

6. Xavfli avtorizatsiya (Insecure Authorization)

Ushbu kategoriya avtorizatsiyaning kamchiligini tavsiflaydi (mijoz tomonidagi tekshiruv, majburiy ko’zdan kechirish va h.).

Takliflar. Ilova foydalanuvchilarning haqiqiyligini tekshirishdan o’tishi lozim (masalan, haqiqiylikni tekshirmasdan va ruxsatsiz foydalanishni taqiqlamasdan ba’zi resurslarga yoki xizmatlarga anonim foydalanishni taqdim etmaslik).

7. Mijoz ilovalari tarkibining nazorati (Client Code Quality)

Muammo server-sayt ilovalarda kodni yozish va uni amalga oshirishdan farqlanuvchi mijoz-sayt ilovalarda dasturiy kodni yozish texnologiyasini amalga oshirishning o’ziga xos xususiyatidan iborat. Bularga quyidagilar taalluqli: buferning to’lib-toshishi, format string zaifliklar, hamda kod darajasidagi xatoliklar. Mobil qurilmalarda ishlovchi kodni qayta yozish masalaning yechimi hisoblanadi. Zararli kod mobil ilovalarni o’zgartira olmaydi degan xato fikr keng tarqalgan.

Takliflar. Ilovalarni turg’un holatida va bajarilishi davrida suqilib kirishdan himoyalash. Ilovalarning kirish ma’lumotlarini va API-interfeyslarni tekshirish, konfidensial axborotning yaxlitligini tekshirish. WebView dan foydalanishda ehtiyot bo’lish lozim, chunki u saytlararo skriping (XSS) kabi zaifliklarni yaratishi mumkin.

8. Ma’lumotlarning modifikatsiyasi (Code Tampering)

Ushbu kategoriya bajariluvchi fayllarning, lokal resurslarning o’zgarishini, begona jarayon chaqiruvlarini ushlab qolishni, runtime usullarni almashtirishini va xotirani dinamik modifikatsiyasini tavsiflaydi.

Ilova o’rnatilganidan so’ng, uning kodi qurilma xotirasida rezident bo’lib qoladi. Bu zararli ilovaga kodni, xotira tarkibini o’zgartirishga APIning tizimli usullarini o’zgartirishga yoki almashtirishga, ilova ma’lumotlarini va resurslarini o’zgartirishga imkon beradi. Bularning hammasi niyati buzuqqa noqonuniy harakatlar qilish, ma’lumotlarni o’g’irlash yoki boshqa moliyaviy foydani olish uchun begona ilovalarni manipulyasiyalash imkonini ta’minlaydi.

Takliflar. Ma’lumotlar manbalariga hech qachon ishonish kerak emas. Ularni yetarli darajada, xususan autentifikatsiya, avtorizatsiya, yaxlitlikni tekshirish, shifrlash va boshqa mexanizmlardan foydalanib, soxtalashtirilishidan va suiiste’mol qilinishidan himoyalash zarur.

9. Dastlabki kodning tahlili (Reverse engineering)

Hujumchilar server servislaridan foydalanish uchun autentifikatsiyalashda sessiyaning hisob ma’lumotlarini ishlatishlari va muayyan foydalanuvchi nomidan harakatlarni amalga oshirishlari mumkin.

Takliflar. Serverda va mijozdagi sessiyalar uchun cookie harakatlari vaqtini cheklash mexanizmini ishlatish lozim. Umumiy holda vaqtni bir soatga yoki undan qisqaga cheklash taklif etiladi. Autentifikatsiya talab qilinganida har bir foydalanuvchi uchun server yangi sessiyani ochishi zarur. Takroran ishlatilishini bartaraf etish uchun serverdagi oldingi sessiyalar yo'q qilinishi yoki bekor qilinishi lozim.

10. Yashirin funksional (Extraneous Functionality)

Ishlab chiqaruvchilar ko'pincha ilovalar kodiga, funksionalligi umumfoydalanishga mo'ljallangan, yashirin funksional imkoniyatlarni, bekdorlarni yoki boshqa mexanizmlarni kiritishadi. Ushbu kategoriyaga ma'lum ta'rif "security through obscurity" (noaniqlik orqali xavfsizlik) to'g'ri keladi. Xaker iborasi bilan aytganda, bu operatsion tizim sotuvchilarining aksariyati xavfsizlik tizimini tuynuklar bilan sotishidan iborat. Tabiiyki, ushbu tuynuklar xususida hujjatlarda so'z bo'lmaydi. Ushbu tuynuklar uzoq vaqt sezilmasdan qolmaydi. Ushbu tuynuklardan foydalanuvchi xakerlar doim topiladi.

Takliflar. Ilovalarni himoyalashning o'ziga xos xususiyati tahdid xarakteriga va mobil platformasiga bog'liq. Ilovalar ishlatilishi jarayonida himoyalangan bo'lishi uchun, resurslarning va dastlabki kodning modifikatsiyalanishini bartaraf etishi mumkin bo'lgan yaxlitlikni tekshirish lozim.

8 BOB. SIMSIZ VA MOBIL TARMOQLAR XAVFSIZLIGINI TA’MINLOVCHI TEXNOLOGIYALAR

8.1. Simsiz va mobil tarmoqlar uchun bazaviy standart

Tarmoq xavfsizligini oshirishga mo’ljallangan ko’pgina texnologiyalar mavjud bo’lib, ularning barchasi ma’lumotlarni himoyalash sohasidagi siyosatning muhim komponentlari, ya’ni autentifikatsiya, ma’lumotlar yaxlitligini madadlash va aktiv tekshirish uchun yechimlarni taklif etadi.

Autentifikatsiya deganda keyingi avtorizatsiyalash maqsadida, foydalanuvchi yoki oxirgi qurilmani (mijoz xostini, serverni, kompyuterni, tarmoqlararo ekranni va h.) va uning joylashgan joyini autentifikatsiyasi tushuniladi.

Ma’lumotlar yaxlitligi tarmoq infrastrukturasi xavfsizligi, perimetr xavfsizligi va ma’lumotlar konfidensialligi kabi strukturalarni o’z ichiga oladi.

Aktiv tekshirish xavfsizlik sohasida o’rnatilgan siyosatning amalda rioya qilinishiga ishonishga va barcha anomal hodisalarni va ruxsatsiz foydalanishga urinishlarini kuzatishga yordam beradi.

Simsiz va mobil tarmoqlarda axborotni uzatishni ta’minlovchi bazaviy standart, ma’lumotlarni uzatish uchun protokollar naboridan tashkil topgan IEEE 802.11 (Wi-Fi 802.11) standarti hisoblanadi. Uning asosiy vazifasi - autentifikatsiya.

An’anaviy xavfsizlik (Tradition Security Network, TSN) IEEE 802.11 standarti simsiz mijozlarni autentifikatsiyasining ikkita mexanizmini ko’zda tutadi:

- ochiq autentifikatsiyani (Open Authentication);
- umumiy kalitli autentifikatsiyani (Shared Key Authentication).

Ochiq autentifikatsiya foydalanish nuqtasining mijozga tarmoqdan foydalanishga ruxsat berilganligini yoki berilmaganligini aniqlashga imkon bermaydi. Bu, agar simsiz yoki mobil tarmoqda WEP-shifrlash ishlatilmasa, xavfsizlik tizimidagi zaif joyi bo’lib qoladi. WEP-shifrlash xususida ma’lumot pastroqda keltirilgan.

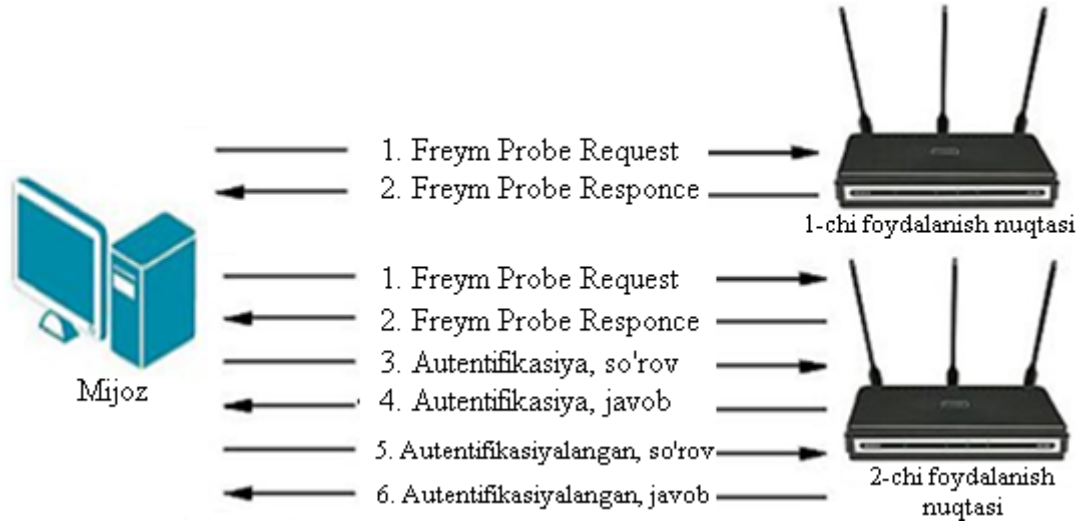
IEEE 802.11 standarti mijozning MAC-adresini va radiofoydalanish nuqtalarini ochiq ko’rinishda uzatishni talab qiladi. Natijada, MAC-adres bo’yicha autentifikatsiyani ishlatuvchi simsiz tarmoqda niyati buzuq

o’zining MAC-adresini ruxsat etilganiga almashtirish yo’li bilan autentifikatsiya usulini aldashi mumkin.

Umumiy kalitli autentifikatsiya ochiq autentifikatsiyaga o’xshash, ammo undan farqli holda WEP-shifrlashning statik kalitini sozlashni talab etadi.

IEEE 802.11 standarti bo’yicha autentifikatsiya, simli tarmoqdan farqli holda, tarmoq resurslaridan foydalanuvchi muayyan mijozga emas, balki mijozning radiofoydalanish qurilmasini autentifikatsiyasiga mo’ljallangan.

Autentifikatsiya jarayoni quyidagi bosqichlardan iborat (8.1-rasm).



8.1-rasm. 802.11 standarti bo’yicha autentifikatsiya

1. Mijoz *Probe Request* so’rovi kadrini (freymini) barcha radiokanallarga jo’natadi.

2. Ta’sir doirasida mijoz bo’lgan radiofoydalanishning har bir nuqtasi javob tariqasida *Probe Response* freymini jo’natadi.

3. Mijoz o’ziga maqul radiofoydalanish nuqtasini tanlaydi va unga xizmat qiluvchi radiokanalga *Authentication Request* (autentifikatsiyaga so’rov) jo’natadi.

4. Radiofoydalanish nuqtasi *Authentication Reply* (autentifikatsiya javobini) jo’natadi.

5. Muvaffaqiyatli autentifikatsiya holida mijoz foydalanish nuqtasiga ulanishga *Association Request* (assotsiyalangan so’rovni) jo’natadi.

6. Foydalanish nuqtasi javob tariqasida *Association Response* (assotsiyalangan javob) assotsiatsiya tasdig’i freymini jo’natadi.

7. Endi mijoz radiofoydalanish nuqtasi bilan foydalanish trafigini almashishi mumkin.

Hozirda IEEE 802.11 ma’lumotlarni turli tezlikda, turli chastota diapazonida va tarmoq xavfsizligining turli darajasida uzatishga imkon beruvchi standartlar guruhidan iborat.

IEEE 802.11a - 802.11b ga uzatishning nisbatan yuqori tezligini tavsiflaydi. 5 GGs chastota spektridagi chastota kanallaridan foydalaniladi. Protokol 802.11b bilan qushilishmaydi.

IEEE 802.11b - uzatishning katta tezligini tavsiflaydi va katta texnologik cheklashlarni kiritadi. Ushbu standart dastlab Wi-Fi deb atalar edi. 2.4 GGs chastota spektridagi chastota kanallaridan foydalaniladi.

IEEE 802.11g - IEEE 802.11a ga ekvivalent ma’lumotlarni uzatish tezligini tavsiflaydi. Protokol IEEE 802.11b bilan qo’shilishadi.

IEEE 802.11n - eng ilg’or tijoriy Wi-Fi-standart. 2.4 GGs va 5 GGs chastota spektrlaridagi chastota kanallaridan foydalaniladi. 11b/11a/11g bilan qo’shilishadi.

802.11i - IEEE 802.11 standartining eng himoyalangan varianti.

802.11as yangi Wi-Fi-standart. Faqat 5 GGs chastota polosasida ishlaydi va nisbatan yuqori tezlikni ta’minlaydi.

Wi-Fi 802.11a, b, g, n asosiy standartlardan bir qatorda turli servis funksiyalarini amalga oshirish uchun qo’shimcha standartlar ishlatiladi (802.11d, 802.11e, 802.11f, 802.11h, 802.11k, 802.11m, 802.11p, 802.11r, 802.11s, 802.11t, 802.11u, 802.11v, 802.11y, 802.11w).

IEEE 802.11i standarti tarkibida autentifikatsiya, har bir sessiya uchun yangi kalitlarni yaratish, kalitlarni boshqarish (Remote Access Dial-In User Service, RADIUS texnologiyasi asosida), paketlar haqiqiyligini tekshirish va h. qismtizimlari mavjud.

Ishlab chiqarilgan IEEE 802.11i standarti, uzatiluvchi ma’lumotlarni shifrlash vositalarini, hamda foydalanuvchilarni va ishchi stansiyalarni markazlashgan autentifikatsiyasini ko’zda tutgan holda, IEEE 802.11 standarti imkoniyatlarini kengaytirishga mo’ljallangan.

Wi-Fi (Wi-Fi Alliance i IEEE) standartlarni ishlab chiqishda va ilgari surishda ishtirok etuvchi tashkilotlar IEEE 802.11i standartning tarkibiy qismi bo’lib qolgan WPA (Wi-Fi Protected Access, Wi-Fi dan himoyalangan foydalanish) standartni tarqatdi. Ushbu standart turli ishlab chiqaruvchilar uskunalarining qo’shiluvchanligini ham ta’minlaydi.

Xavfsizlikning yangi standarti WPA xavfsizlik darajasini WEP ga qaraganda yuqoriroq ta’minlaydi va eski uskunaning dasturiy ta’minotini apparat o’zgarishisiz yangisiga almashtirishga imkon beradi.

Keyinroq WPA ning birinchi versiyasiga nisbatan xavfsizlikning yanada yuqoriroq darajasini ta’minlovchi WPA2 standarti ishlab chiqildi va tasdiqlandi. WPA/WPA2 simsiz aloqa qurilmalarini sertifikatsiyalovchi yangilangan dastur hisoblanadi. WPA ning afzalligi - ma’lumotlarning kuchaytirilgan xavfsizligi va simsiz tarmoqlardan foydalanishdagi nazoratning talabchanligi.

WPA azaldan RC4 shifrlash usulini ishlatuvchi TKIP (Temporal Key Integrity Protocol) protokolga asoslangan. Shu orada WPA2 standarti RC4 ga nisbatan shifrlashning quvvatliroq yangi usuli CCMP ga (Counter-Mode with CBC-MAC Protocol ga) asoslangan AES (Advanced encryption Standard) shifrlash algoritmidan foydalanadi. Undan tashqari WPA/WPA2 da IEEE 802.1x standartini, EAP protokolini va xabarlar yaxlitligini tekshirish MIC (Message Integrity Check) ni madadlash ta’minlangan. Wi-Fi Alliance WPA mohiyatini quyidagi formula orqali aniqlaydi:

$$WPA = IEEE\ 802.1x + TKIP + EAP + MIC$$

Ushbu formuladan ko’rinib turibdiki, WPA mohiyatan, bir necha texnologiyalarning yig’indisidan iborat.

WPA ikkita rejimda ishlashi mumkin: enterprise (korporativ) va Pre-Shared Key (shahsiy).

Birinchi holda, katta tarmoqlarda ma’lumotlar bazasini saqlash va IEEE 802.1x standart bo’yicha autentitlikni tekshirish, odatda, maxsus server, ko’pincha RADIUS orqali amalga oshiriladi.

Ikkinchi holda WPA ni simsiz tarmoqlarning barcha kategoriyali foydalanuvchilari tomonidan ishlatilishi ko’zda tutiladi, ya’ni murakkab mexanizmlarni talab qilmaydigan soddalashtirilgan rejimga ega. Ushbu rejim WPA-PSK (Pre-Shared Key) deb ataladi va simsiz tarmoqning har bir uzeliga (foydalanish nuqtasiga, simsiz marshrutizatorga, mijoz adapteriga, ko’prikka) bitta parol kiritilishi ko’zda tutiladi.

Parollar mos kelgan vaqtgacha, mijoz tarmoqdan foydalana oladi. Payqash mumkinki, paroldan foydalanib yondashish WPA-PSK ni saralash usuli orqali hujumga zaif qilib qo’yadi. Ammo ushbu rejim WEP kalitlar bilan chalkashliklardan qutqaradi. Ularni raqam-xarfli parol asosidagi yaxlit va aniq tizim bilan almashtiriladi.

Xabarlar yaxlitligini tekshirish MIC (Message Integrity Check) autentifikatsiyaning yana bir muhim mexanizmi hisoblanadi. Undan

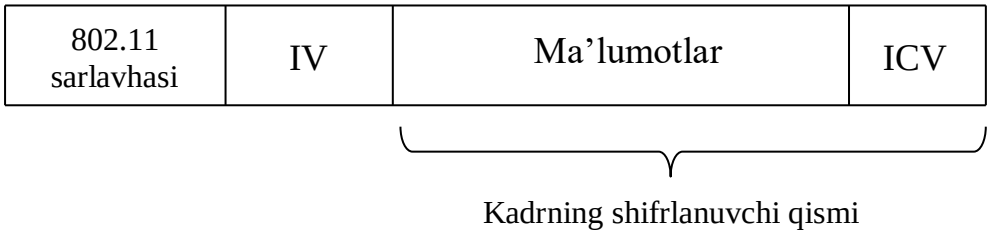
ma’lumotlar paketini tutib olishini bartaraf etishda foydalaniladi. Chunki tutib olingan paket mazmuni o’zgartirilishi va modifikatsiyalangan paket yana tarmoq orqali uzatilishi mumkin.

802.11i (WPA2) - eng barqaror va xavfsiz yechim bo’lib, birinchi navbatda kalitlarni boshqarish va ma’murlash asosiy bosh og’rig’i hisoblanuvchi katta tashkilotlarga mo’ljallangan. WPA2 barcha sertifikatsiyalangan Wi-Fi qurilmalar uchun majburiy hisoblanadi.

Yuqorida tilga olingan WEP protokol ma’lumotlarni shifrlashning birinchi standarti hisoblanadi.

WEP-shifrlashning muolajasi quyidagicha. Uzatiluvchi paketdagi ma’lumotlar avvalo, dastlabki xabar oxiriga qo’shiluvchi yaxlitlik nazorati qiymatini (Integrity Check Value, ICV) olish uchun, yaxlitlikka tekshiriladi (CRC-32 algoritmi). So’ngra 24-bitli initsializatsiya vektori generatsiyalanadi, unga esa statik (40 yoki 104 bitli) maxfiy kalit qo’shiladi. Shu tariqa olingan 64 yoki 128-bitli kalit ma’lumotlarni shifrlashda ishlatiluvchi psevdotasodifiy sonni generatsiyalash uchun dastlabki kalit hisoblanadi. So’ngra ma’lumotlar XOR mantiqiy amali yordamida psevdotasodifiy kalit ketma-ketligi bilan aralashtiriladi (shifrlanadi) va initsializatsiya vektori kadrning xizmatchi hoshiyasiga qo’shiladi. 8.2-rasmda WEP-kadrning formati keltirilgan.

Parollarga asoslangan har qanday xavfsizlik tizimiga o’xshab, WEP ishonchligi kalitning uzunligiga va tarkibiga hamda uning almashtirilish chastotasiga bog’liq. Birinchi jiddiy kamchiligi - statik kalitning ishlatilishi bo’lib, uni nisbatan kichik vaqt mobaynida saralash yo’li bilan topish mumkin. WEP-shifrlashning ikkinchi kamchiligi - initsializatsiya vektori har bir paket bilan shifrlanmagan matn orqali uzatiladi va vaqtning katta bo’lmagan oralig’ida qaytariladi.



8.2-rasm. WEP -kadr formati

Simsiz tarmoqlarda autentifikatsiya uchun 802.11 standartning qismi hisoblanmaydigan ikkita boshqa mexanizmlar ham keng ishlatiladi:

- simsiz lokal tarmoqning identifikatorini belgilash (Service Set Identifier, SSID);

- mijozning, uning MAC-adresi bo'yicha, autentifikatsiyasi (MAC Address Authentication).

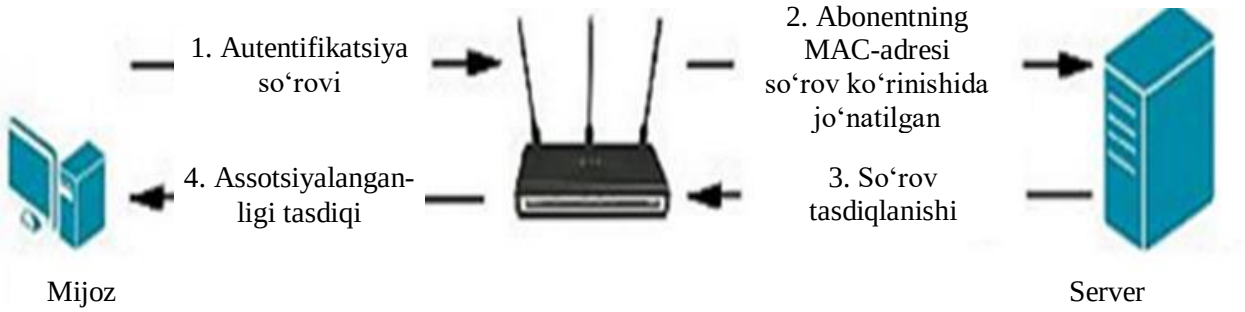
Simsiz lokal tarmoqning identifikatorini belgilash (SSID) tarmoqlarni bir-biridan mantiqiy farqlashga imkon beruvchi simsiz tarmoqning atributidan (tarmoq nomidan) iborat. Foydalanuvchi tarmoqqa kirishga urinishida simsiz adapter makonni, unda simsiz tarmoq mavjudligini aniqlash maqsadida, skanerlaydi. Yashirin identifikator rejimida skanerlashda tarmoq foydalaniluvchi tarmoqlar ro'yxatida ko'rsatilmaydi. Unga faqat, birinchidan uning SSID si aniq bo'lsa, ikkinchidan ushbu tarmoqqa ulanishning profili oldindan yaratilgan bo'lsa, ulanish mumkin.

SSID identifikator maxsus freymlarda - bikonlarda (beacon) - boshqarishning eng muhim freymlarining birining signal kadrlarida radiofoydalanishning nuqtalari yordamida muntazam uzatiladi. Radiofoydalanuvchi nuqta u qamrab olgan zonadagi barcha qurilmalarga o'zining borligini va kerakli axborotni (SSID, kanal chastotasi, qurilmalarni sinxronlash uchun vaqt markerlarini, madadlanuvchi tezliklarni, xizmat ko'rsatish sifatini ta'minlash funksiyasining imkoniyatini va h.) afisha qilish uchun vaqti-vaqti bilan bikonlarni jo'natadi.

Ta'sir doirasida joylashgan va 802.11 standartni madadlovchi har qanday qabul qiluvchi-uzatuvchi stansiya SSID ni 802.11 protokolining trafikni tahlillagichi yordamida aniqlashi mumkin. Radiofoydalanishning ba'zi nuqtalari freymlar-bikonlar ichida SSID ni keng ommaga eshittirishni ma'muriy taqiqlashga imkon beradi. Ammo bu holda SSID ni Probe response frame freymlarni freym-so'rovga olingan freym-javoblarni egallash yo'li bilan osongina aniqlash mumkin. Freym-javob tarkibida radiofoydalanish nuqtalari jo'natuvchi funksionallik, ma'lumotlarni uzatishning madadlanuvchi tezliklari va h. xususidagi axborot mavjud. SSID ma'lumotlarning konfidensialligini ta'minlamaydi. Undan tashqari, radiofoydalanish nuqtasi tomonidan SSID ni keng ommaga eshittirishning to'xtatib qo'yilishi bitta simsiz tarmoqda ishlatiluvchi turli ishlab chiqaruvchilarining simsiz tarmoqlari uskunalarining qo'shilishiga jiddiy ta'sir ko'rsatishi mumkin.

Mijozning, uning MAC-adresi bo'yicha autentifikatsiyasi. Begona foydalanuvchilarning foydalanishlari ehtimolligini kamaytirish uchun,

ochiq autentifikatsiyaga qo’shimcha ravishda, mijozning MAC-adresi bo’yicha autentifikatsiyasi ishlatiladi (8.3-rasm).



8.3-rasm. Mijozning, uning MAC-adresi bo’yicha autentifikatsiyasi

MAC-adres bo’yicha autentifikatsiyalashda mijozning MAC-adresi foydalanish nuqtalarining MAC-jadvaliga kiritilgan mijozlarning ruxsat etilgan (yoki taqiqlangan) ro’yxati bilan yoki autentifikatsiyaning tashqi serveri yordamida taqqoslash ro’y beradi.

8.2. EAP, IEEE 802.1x va IPSec standartlari

IEEE 802.11 standart asosida tarmoqlarni ishlab chiqaruvchilari va ulardan foydalanuvchilari to’qnashgan muammolari simsiz tarmoqlarni himoyalashning yangi yechimlarini qidirishga majbur etdi.

Simsiz tarmoq xavfsizligi tizimiga ta’sir etuvchi komponentlar aniqlandi:

- autentifikatsiya arxitekturasi;
- autentifikatsiya mexanizmi;
- ma’lumotlarning konfidensialligini va yaxlitligini ta’minlovchi mexanizmlar.

Shu sababli, autentifikatsiyaning kengayuvchi protokoli EAP ishlab chiqilgan.

Autentifikatsiya algoritmi EAP (Extensible Authentication Protocol - autentifikatsiyaning kengayuvchi protokoli) - ko’pgina tekshirish usullarini madadlovchi autentifikatsiya modeli. EAP, odatda, bevosita PPP yoki IEEE 802 xillaridagi kanal sathidagi protokollar bazasida ishlaydi va IP protokolini ishlatishni talab qilmaydi.

EAP simsiz tarmoq elementlarining va tarmoqdan foydalanuvchilarning markazlashgan autentifikatsiyasini, shifrlash kalitlarini dinamik generatsiyalash imkoni bilan, madadlaydi.

EAP simli va simsiz muhitlardagi ajratilgan va kommutatsiyalanuvchi qurilmalarda ishlatilishi mumkin. Hozirda EAP protokoli xostlarda va marshrutizatorlarda amalga oshirilgan. Protokol IEEE 802 protokollarini ishlatuvchi kommutatorlarda va foydalanish nuqtalarida ham amalga oshirilishi mumkin. IEEE 802 simli muhitlarda EAP ning inkapsulyasiyasi IEEE-802.1x standartda, simsiz muhitlarda esa - IEEE 802.11i standartda tavsiflangan.

EAP arxitekturasining afzalliklaridan biri uning moslanuvchanligi. EAP autentifikatsiyaning muayyan mexanizmini tanlashga xizmat qiladi.

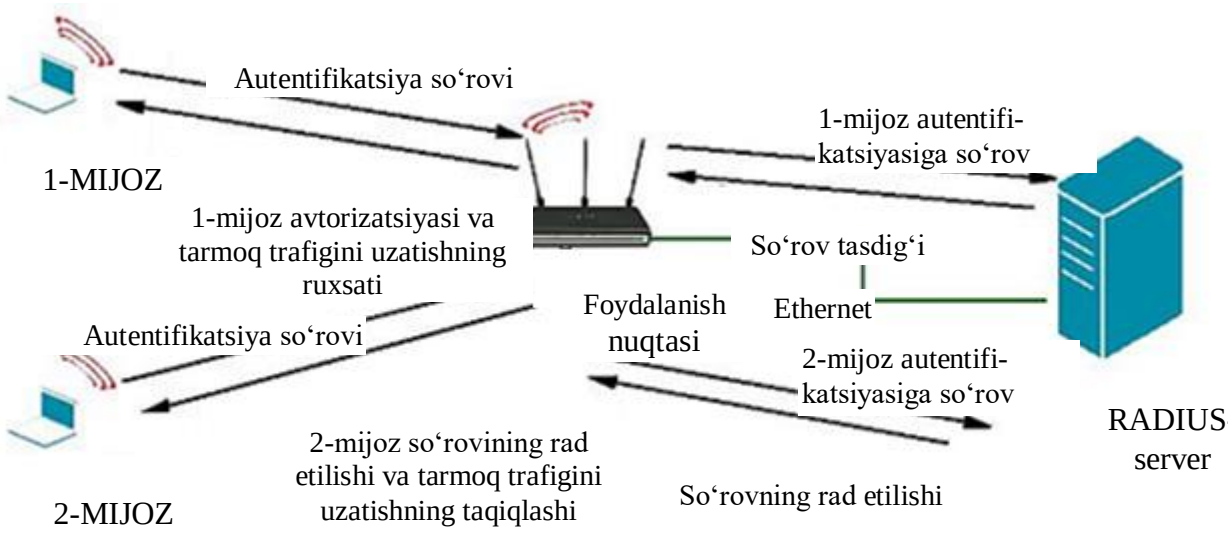
Autentifikatsiya mexanizmiga binoan foydalanuvchi autentifikatsiyalanuvchi tomonga (masalan RADIUS-serverga) autentifikatsiya so'rovini jo'natadi. So'ngra autentifikatsiyalanuvchi tomon qo'llanuvchi muayyan autentifikatsiya usulini aniqlash uchun qo'shimcha axborotni so'raydi. Foydalanuvchi tomonidan javob olinganidan so'ng autentifikatsiyalovchi tomon avtorizatsiyalash va tarmoq trafigini uzatish huquqini olishga ruhsat beradi.

IEEE 802.1x standart ma'lumotlarni uzatish tarmog'idan foydalanuvchilarni va ishchi stansiyalarni autentifikatsiyalash va avtorizatsiyalash uchun ishlatiladi. IEEE 802.1x standart foydalanuvchiga, u tegishli guruhga bog'liq holda, tarmoqdan va uning servislaridan foydalanish huquqini taqdim etadi.

Simsiz tarmoqlar uchun IEEE 802.1x standart autentifikatsiyasi uchta komponentdan iborat (8.4-rasm):

- simsiz mijoz (mijoz qurilmasining dasturiy ta'minoti);
- autentifikator (foydalanish nuqtasi);
- autentifikatsiya serveri (RADIUS).

IEEE 802.1x standartning autentifikatsiya himoyasi simsiz tarmoq mijozidan foydalanish nuqtasiga so'rovni boshlab beradi. Foydalanish nuqtasi mijozning haqiqiyligini mos RADIUS serverida EAP protokoli orqali aniqlaydi. RADIUS serveri foydalanuvchi autentifikatsiyasini (parol yoki sertifikat yordamida) yoki kompyuter autentifikatsiyasini (MAC-adres yordamida) bajarishi mumkin. Nazariy jihatdan, simsiz tarmoq mijozi tarmoqqa tranzaksiya tugamasdan oldin kira olmaydi.



8.4-rasm. 802.1x/EAP da autentifikatsiya jarayoni

IEEE 802.1x simsiz lokal tarmoq mijoziga faqat autentifikatsiya serveriga atributlarni uzatish vositalarini taqdim etadi va autentifikatsiyaning turli usullari va algoritmlarining ishlatilishiga yo’l quyadi. Autentifikatsiya serverining vazifasi tarmoq xavfsizligi siyosati talab etuvchi autentifikatsiya usullarini madadlash hisoblanadi.

Autentifikator (foydalanish nuqtasi) har bir mijoz uchun, uning assotsiyalangan identifikatori asosida mantiqiy port yaratadi. Mantiqiy port ma’lumotlarni almashish uchun ikkita kanalga ega - nazoratlanuvchi va nazoratlanmaydigan kanallar. Nazoratlanmaydigan kanal trafikni simsiz segmentdan simliligiga va aksincha qarshiliksiz o’tkazadi, nazoratlanuvchi kanal esa tarmoq trafigining qarshiliksiz o’tkazilishi uchun muvaffaqiyatli autentifikatsiyani talab etadi.

Mijoz aktivlashadi va foydalanish nuqtasi bilan assotsiyalanadi (yoki simli lokal tarmoq xolida segmentga fizik ulanadi). Autentifikator ulanish faktini aniqlaydi va mijoz uchun mantiqiy portni, uni darhol "avtorizatsiyalanmagan" holiga o’tkazib, aktivlashtiradi. Natijada mijoz porti orqali faqat IEEE 802.1x protokol trafigi almashishi mumkin, barcha boshqa trafik uchun port blokirovka qilingan. IEEE 802.11 ning lokal tarmoqlarda fizik portlarning mavjud emasligi sababli, simsiz mijoz qurilmasi va foydalanish nuqtasi orasidagi assotsiatsiya foydalanishning tarmoq porti hisoblanadi. Mijoz ham autentifikatsiya jarayonini ishga tushirish uchun EAP Start (EAP autentifikatsiyaning boshlanishi) xabarini jo’natishi mumkin (majbur emas).

Autentifikatsiya tugaganidan so’ng server autentifikatorga RADIUS-ACCEPT (qabul qilish) xabarini yoki RADIUS-REJECT (rad etish) xabarini jo’natadi. RADIUS-ACCEPT xabari olinganida autentifikator mijoz portini "avtorizatsiyalangan" holatiga o’tkazadi va foydalanuvchining barcha trafigini uzatish boshlanadi.

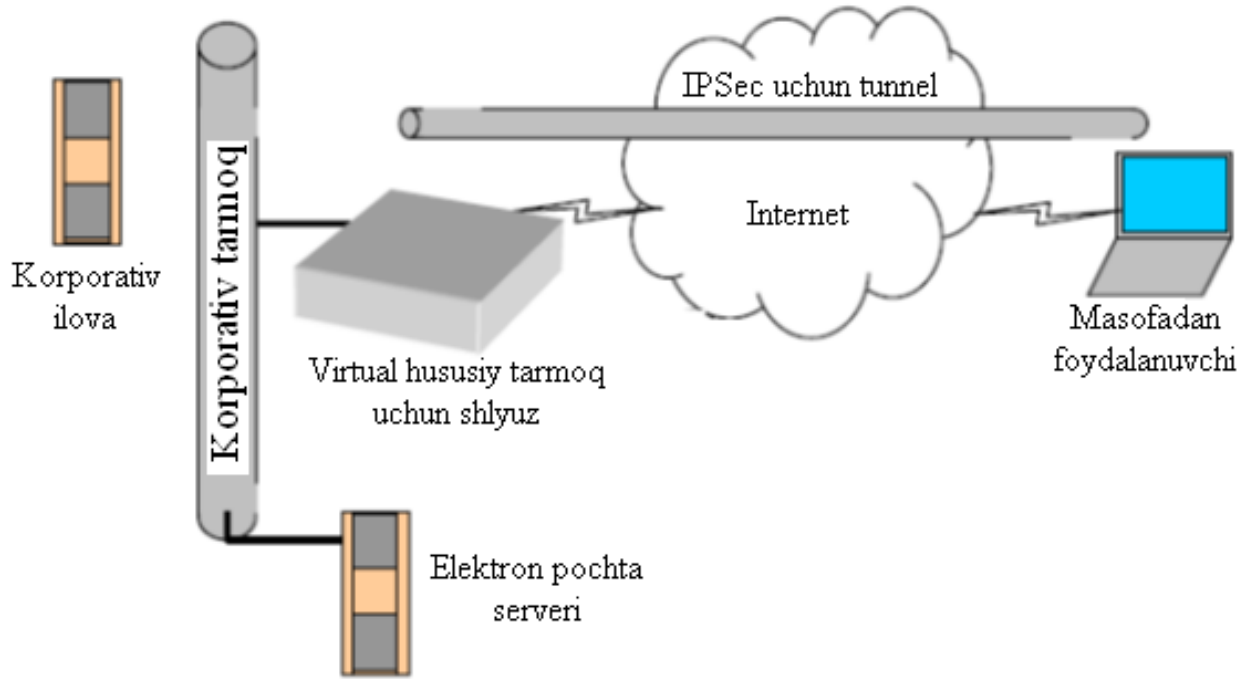
IEEE 802.1x standartda kanal sathidagi foydalanuvchilarning autentifikatsiyasi EAP protokoli bo’yicha bajariladi. EAP protokoli ChAP (Challenge Handshake Authentication Protocol - o’zaro autentifikatsiya protokoli) ga o’xshash. ChAP protokoli PPP da (Point to Point Protocol - "nuqta-nuqta" ulanish protokolida) ishlatiladi.

EAP autentifikatsiyaning turli usullarini ta’minlovchi autentifikatsiya, avtorizatsiya va ro’yxatga olish (authentication, authorization and accounting - AAA) tizimida "umumlashgan" protokol hisoblanadi.

AAA-mijoz (simsiz tarmoqda foydalanish serveri AAA atamalarida foydalanish nuqtasi orqali ifodalangan) EAP ni madadlaydi. EAP autentifikatsiya jarayonida mijoz va tarmoq tomonidan ishlatiluvchi muayyan usullarni tushunmasligi mumkin. Foydalanish serveri (AAA-mijoz) mijoz va server almashuvchi autentifikatsiya protokoli xabarlarini tunnellaydi. Foydalanish serverini faqat autentifikatsiya jarayonining boshlanishi va tugallanishi fakti qiziqtiradi.

Turli kompaniya - ishlab chiqaruvchilari ishtirokida loyixalangan EAP ning bir necha variantlari mavjud (EAP-MD5, EAP-TLS, EAP-LEAP, PEAP). Bunday xilma-xillik qo’shiluvchanlikka qo’shimcha muammolarni kelib chiqaradi, ya’ni simsiz tarmoq uchun munosib uskunani va dasturiy ta’minotni tanlash murakkab masala bo’lib qoladi.

IPSec protokoli simli va simsiz (mobil) tarmoqlarda muvaffaqiyatli ishlatiladi. Xavfsizlikni ta’minlash IP-sathida va Internet-modelda amalga oshiriladi. IPSec ni tatbiq etish usullaridan ko’p tarqalgani tunnellash bo’lib, u bitta sessiyada IP-trafikni shifrlash va autentifikatsiyalash imkonini beradi. IPSec hozirda Internetda ishlatiluvchi aksariyat virtual xususiy tarmoqlardagi (VPN - Virtual Private Network) asosiy texnologiya hisoblanadi (8.5-rasm). IPSec ning moslanuvchanligi va ilovalar tanlanishining kengligi sababli, ko’pchilik aynan bu sxemadan simsiz ilovalar xavfsizligini ta’minlashda foydalanadi.



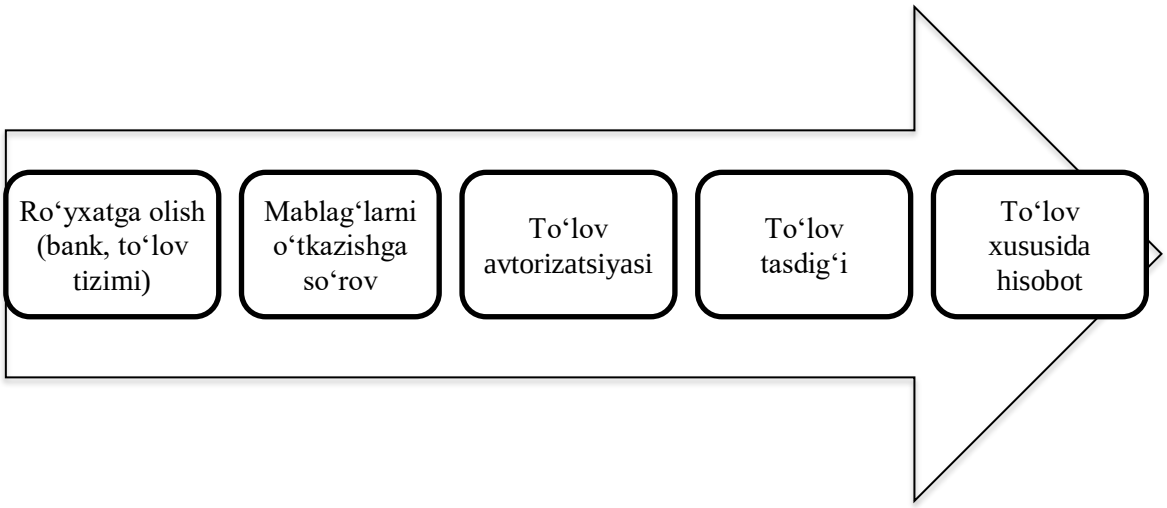
8.5-rasm. IPSec VPN-tunnel

IPSec ni ilovalarga asoslangan qo'llanilishining juda ko'p imkoniyatlari mavjud. Xavfsiz kommunikatsiyalar uchun IPSec ning qo'llanilishi ko'pgina Internet orqali masofadan foydalanuvchi virtual xususiy tarmoq VPN bilan bog'liq. Qachonki, umumfoydalanuvchi tarmoq xususiy tarmoq funksiyalarini amalga oshirish uchun ishlatilsa, uni VPN deb atash mumkin. Bunday ta'rifga ATM (uzatishning asinxron usuli), Frame Relay va x.25 kabi tarmoq texnologiyalari ham tushadi, ammo aksariyat odamlar Internet orqali shifrlangan kanalni tashkil etish xususida gap ketganida VPN atamasini ishlatishadi. Korporativ tarmoq perimetri bo'yicha shlyuzlar o'rnatiladi va IPSec-tunneli orqali shlyuzdan masofadan foydalanish amalga oshiriladi.

9 BOB. MOBIL KOMMERSIYADA XAVFSIZLIKNI TA’MINLASH

9.1. Mobil moliya xizmatlari modeli

Zamonaviy mobil moliya xizmatlari tizimi, asosan 9.1-rasmda keltirilgan sxema bo’yicha quriladi:



9.1-rasm. Mobil moliya xizmatini amalga oshirish sxemasi

Hozirda quyidagi mobil moliya xizmatlari modellari mavjud:

- Premium-SMS - asosida to’lov;
- mobil kommersiya.

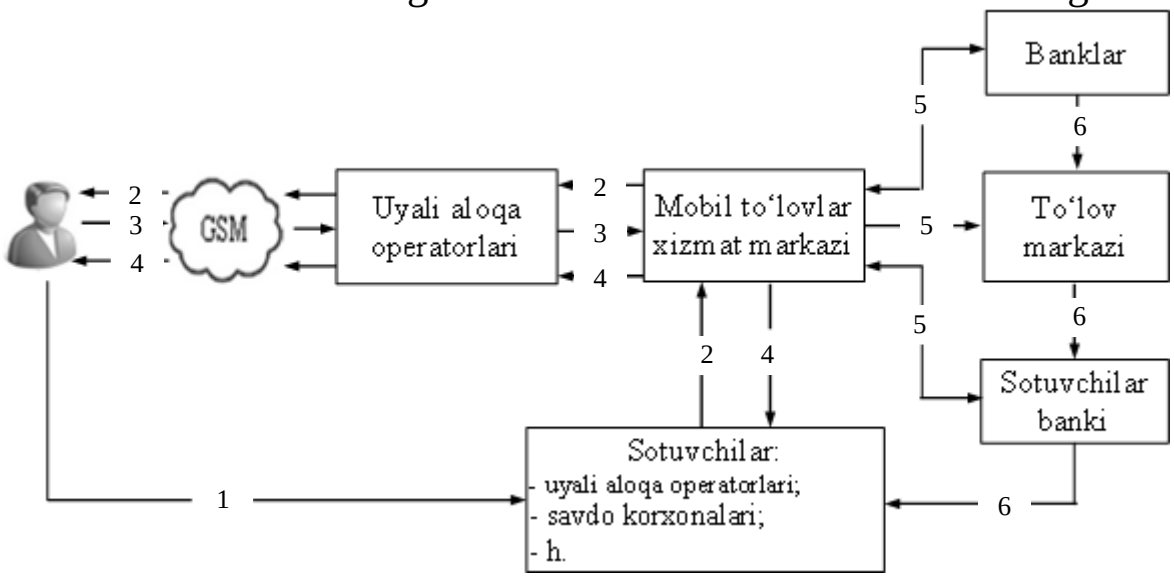
Premium-SMS asosida to’lov - qandaydir to’lov xizmatini olish uchun ishlatiluvchi SMS ning alohida tarifikatsiyalanuvchi turi.

Abonent to’lash uchun operatorning qisqa nomeriga xabar yuboradi, operator abonent hisob varag’idan sotuvchiga kerakli pul miqdorini (hisob varag’idan muomila uchun yetarli mablag’ning borligiga ishonch hosil qilganidan so’ng) o’tkazadi, so’ngra abonent xizmatni aktivatsiyalash uchun saytdan yoki koddan foydalanishga ruxsat oladi.

Jo’natiluvchi xabarga maxsus tarif bo’yicha to’lanadi (odatda, standart SMS narxidan aytarlicha qimmat). To’lovni abonentning o’zi (SMS yoki sayt orqali so’rov yuborib) yoki mablag’ni oluvchi (bunda abonentning aynan o’zi ekanligining tasdig’i kerak bo’ladi) boshlab berishi mumkin. Shaxsiy hisob varag’idan mablag’ jo’natilganidan va hisobdan chiqarilganidan so’ng, abonent xizmatdan foydalana oladi. Ba’zida, Premium-SMS mobil aloqaga bevosita tegishli bo’lmagan servislar

(masalan, Internet resurslarda to’lash uchun, turli ovoz berish va h.) uchun ishlatiladi.

SMS to’lovlarni amalga oshirish sxemasi 9.2-rasmda keltirilgan.



1 - so’ralgan tovar yoki xizmatni tanlash
2 - tovar yoki xizmat uchun to’lov scheti
3 - mijoz to’lovining tasdig’i
4 - to’langanligini bildirish
5 - moliya axboroti
6 - pulni o’tkazish

9.2-rasm. SMS to’lovlarni amalga oshirish sxemasi

Premium-SMS modelida tarifikatsiyaning quyidagi ikki turi mavjud:

- *MO-tarifikatsiya ("Mobile Originated").* Mablag’ abonent hisob varag’idan, u ma’lum qisqa nomerga SMS-xabar jo’natgan onida, hisobdan chiqariladi;

- *MT-tarifikatsiya ("Mobile Terminated").* Mablag’ abonent hisob varag’idan, SMS-xabar olingan onida, hisobdan chiqariladi. Avval foydalanuvchi qisqa nomerga SMS jo’natadi (buning uchun pul olinmaydi), so’ngra abonentning xizmatga to’lash uchun pulining yetarligi va sotuvchining ushbu xizmatni taqdim eta olishi tekshiriladi. Agar barchasi ijobiy bo’lsa, abonentga xabar jo’natiladi (buning uchun pul olinadi). To’lovning ushbu usulining afzalligi - foydalanuvchi shaxsiy ma’lumotlarini sotuvchi saytiga kiritishi shart emas, qandaydir to’lov tizimida ro’yxatga olinishi talab etilmaydi, to’satdan xarid qilinganda qulay. Xarid amalga oshirish eng kam vaqtni talab qiladi. Bu usulda operator ham foydalanadi, u 30-60% vositachilik haqiga ega bo’ladi.

Mobil kommersiya (mCommerce) - *mobil telefonni foydalanuvchining asosiy interfeysi sifatida ishlatuvchi turli kommersiya*

servislari uchun umumiy nom. Mobil kommersiyaning Premium-SMS dan farqi shundaki, mobil kommersiyada mablag' to'lovini keng doirada amalga oshirish mumkin, Premium-SMS orqali to'lovni amalga oshirish esa qisqa nomerga qat'iy bog'liq.

To'lov jarayoni cho'ntak kompyuterlari yoki smartfonlar yordamida masofaviy (Internet, GPRS va h.) bog'lanish orqali amalga oshiriladi. Mobil kommersiya Premium-SMS bilan plastik karta yordamida to'lovning aralashmasi bo'lib, ushbu aralashma masofadagi foydalanuvchilar bilan o'zaro aloqa jarayonlarini avtomatlashtirish bo'yicha dasturiy-apparat yechimda amalga oshirilgan. Ushbu texnologiya Premium-SMS dan SMS orqali ishlashni, plastik kartadan esa to'lov mablag'ini tanlashdagi erkinlikni qabul qilgan.

Mobil kommersiya mobil aloqaning ilg'or texnologiyalarini o'zida mujassamlantirgan va quyidagi yo'nalishlarga ajratiladi:

- *mobil banking* - to'lov tranzaksiyalarni amalga oshirishda bank hisob varag'idagi, mobil telefon yordamida boshqariluvchi mablag' ishlatiladi;

- *mobil to'lov* - bank hisob varag'idan foydalanmay amalga oshiriladi va bankda shaxsiy hisob varag'i bo'lmagan abonentlar foydalanadi.

Bankda *"mobil banking"* xizmati ulanganida foydalanuvchiga uning bankdagi hisob varag'idagi mablag'dan, mobil telefon yordamida, foydalanish imkoniyati beriladi. Foydalanuvchi mobil qurilmada o'zining va boshqa abonentning hisob varag'ini to'ldirishi, o'zining bankdagi hisob varag'idan boshqa foydalanuvchining bankdagi hisob varag'iga mablag'ni o'tkazishi mumkin. Mobil telefon hisob varag'ini avtomatik tarzda to'ldirish xizmati ham mavjud. Mobil bankingda nafaqat turli to'lovlarni amalga oshirish, balki u orqali turli axborot xizmatlarini olish imkoniyati ham mavjud.

Smartfonlarga talabning oshishi va tezkor Internetdan uyali telefon orqali foydalanish imkoniyatining paydo bo'lishi bilan, mobil banking navbatdagi texnologik qadam bo'ldi. Shubhasiz, u hisob varaqlaridan komfortli va muammosiz foydalanishni ta'minlaydi. Ammo axborot xavfsizligi nuqtai nazaridan ba'zi kamchiliklarga ega. Masalan, uyali telefon aloqa provayderlari serverlarining shifrlanmaganligi. Xaker-ekspert foydalanuvchilarning hisob varag'i yoki debet va kredit kartalari xususidagi axborotni osongina olishi mumkin. Bankdan olingan xabarlarning shifrlanmaganligi. Bu mobil aloqa operatori orqali uzatiluvchi axborotni osongina ushlab qolishga imkon beradi. Shu sababli,

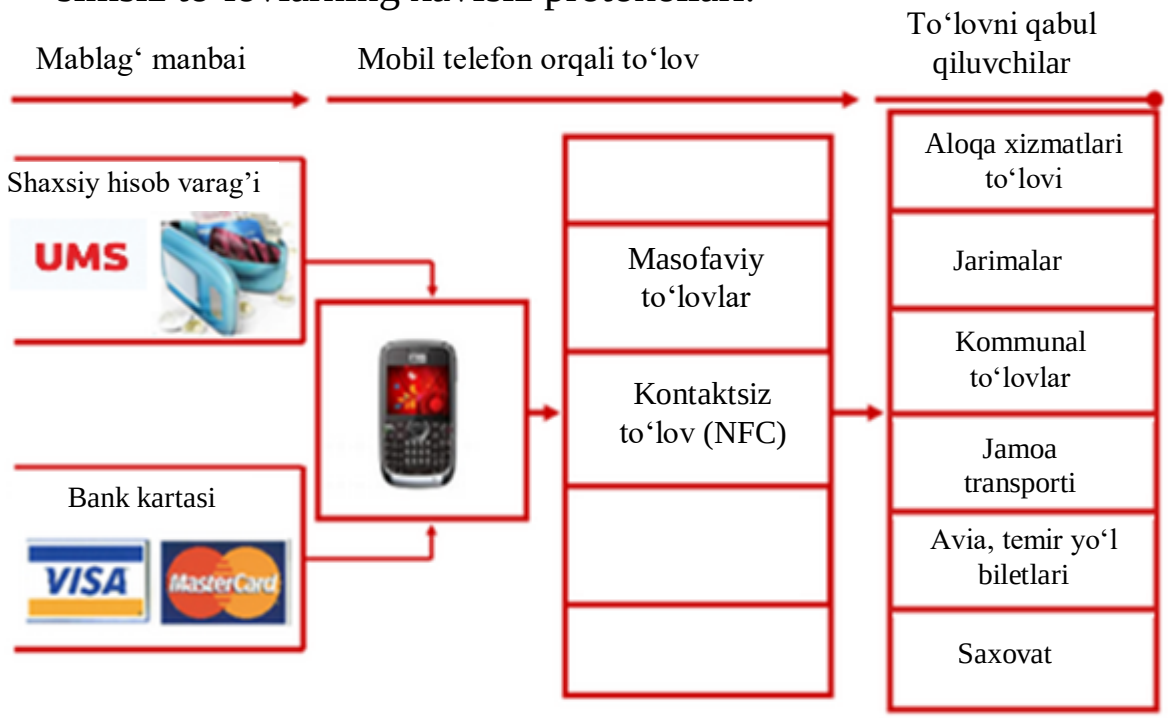
mobil bankingdan juda zarur bo’lgandagina foydalanish maqsadga muvofiq hisoblanadi.

Mobil to’lov - abonentning shaxsiy hisob varag’i hamda bank kartasi orqali uyali telefondan amalga oshiriluvchi to’lov. Ushbu to’lov xizmatlarning keng spektrini - aloqa xizmati, jarimalar, kommunal to’lovlar, kreditlar, jamoa transportidagi yo’lkira, avia, temir yo’l chiptalari, chakana savdo shoxobchalaridagi va h. to’lovlarni amalga oshirish imkoniyatini beradi. Mobil to’lov strukturasi 9.3-rasmda keltirilgan.

Amalga oshirish usuli bo’yicha mobil to’lovlar *masofaviy* va *kontaktsizliga* ajratiladi.

Masofaviy mobil to’lovlarda telefon mijozning hisob varag’idan masofadan foydalanishni tashkil etish vositasi sifatida ishlatiladi. Hisob varag’i sifatida operatorning billing tizimidagi (ko’rsatilgan xizmatlar uchun to’lovning avtomatlashtirilgan tizimidagi) mijoz hisob varag’i ishlatiladi. Internet tarmog’i infrastrukturasidan foydalanuvchi, Internet-to’lov tizimidan farqli holda, simsiz to’lov tizimlari mobil qurilmalar va ma’lum joyga bog’langan terminallar so’rovlarini ishlaydi. Ushbu tizimlar quyidagi xususiyatlarga ega:

- mobil qurilma yordamida to’lash imkoniyati;
- tranzaksiyalarni POS (Point Of Sale - to’lash nuqtasi) terminallar yordamida ishlash imkoniyati;
- simsiz to’lovlarning xavfsiz protokollari.



9.3-rasm. Mobil to’lov strukturasi

Mobil to’lovlarda bir necha tomon qatnashishi mumkin:

- xaridor-mobil qurilma egasi. Tovar va xizmatlar to’lovchisi;
- sotuvchi yoki etkazib beruvchi (jismoniy shaxs yoki tashkilot);
- tranzaksiyalar autentifikatsiyasini va avtorizatsiyasini amalga oshiruvchi ishonchli uchinchi tomon, masalan, bank, uyali aloqa operatori, kredit kartalar operatori;
- mobil to’lovlar bo’yicha xizmatlarni ta’minlash. Amallar bajarilishiga javobgar.

Kontaktsiz mobil to’lovlar NFC (Near Field Communication). - ta’sir doirasi kichik yuqori chastotali simsiz aloqa texnologiyasi. Ushbu texnologiya taxminan 10 santimetr oraliqdagi qurilmalar orasida ma’lumotlarni almashishga imkon beradi.

NFC texnologiyasi yordamida to’lov afzalliklari:

- magazinda xarid qilish, kommunal xizmatlar, pulli televidenie haqini to’lash imkoniyati;
- pulli hisobni pulsiz hisob bilan almashtirish (masalan, jamoa transportida yo’l haqini to’lash).

NFC texnologiyasi servislaridan foydalanish uchun telefonga *NFC*-stikerlar va *NFC-modullar* kabi maxsus qo’shimcha qurilmalar o’rnatish lozim.

NFC-stikerlar passivlariga va aktivlariga ajratiladi.

Passiv NFC-stikerlar mobil telefon bilan ma’lumotlarni almasha olmaydilar. Ular NFC-qurilmaga mobil operatorning aloqa kanali orqali (SMS yoki mobil Internet orqali) axborotni yozishga imkon bermaydi.

Aktiv NFC-stikerlar telefon bilan bog’lanish uchun Wi-Fi aloqa kanalidan yoki Bluetooth dan foydalanadi.

NFC-modulda mikroprosessor bo’lib, u servis ilovalarining ishonchli saqlanishini, kriptografik himoyani ta’minlaydi va quyidagi uchta aloqa kanalini madadlaydi:

- kontaktsiz tranzaksiyalar uchun NFC-kanal;
- TSM dan (Trusted Service Manager) mobil operator tarmog’i orqali axborot oqimi;
- telefonning mobil ilovasi orqali foydalanuvchi bilan ma’lumotlar almashish.

NFC-modulda servis ilovalari - dasturiy modullar (to’lov, transport va h.) yozilgan. Servis ilovalari ruxsatsiz foydalanishdan kalitlar yordamida himoyalangan xavfsizlik tizimiga ega.

NFC-modulli telefon to’lov terminali bilan bog’lanishni o’rnatadi, natijada abonent hisob varag’idan xizmat narxi undiriladi.

NFC-texnologiyasini qo’llashning uchta asosiy sohasi mavjud:

- *kartalar emulyasiyasi:* NFC qurilmasi o’zini mavjud simsiz karta sifatida tutadi;
- *o’qish rejimi:* NFC qurilma aktiv hisoblanadi va passiv RFID metkani, masalan interaktiv reklama uchun, o’qiydi;
- *P2P rejim* - ikkita NFC qurilma o’zaro bog’lanishib, axborot almashishadi.

NFC-modul ishlatilishining boshqa usullari ham bo’lishi mumkin:

- chiptalarni (avia chiptalar, konsert chiptasi va h.) elektron xarid qilish;
- jamoa transportida chiptalarni mobil xarid qilish;
- mobil to’lovlar - qurilma to’lov kartasi sifatida;
- elektron taxta - mobil telefon ko’chadagi e’lonlar taxtasidan RFID metkalarni o’qishda ishlatiladi.

9.2. Mobil to’lov zaifliklari va ulardan himoyalanish usullari

Mobil to’lov amalga oshirilganidagi barcha zaifliklarni, ular amalga oshirilishi sathiga mos holda, quyidagilarga ajratish mumkin:

- ma’lumotlarni uzatish protokollarining zaifliklari;
- uzatish texnologiyalari (RFID) zaifliklari;
- mobil operatsion tizim zaifliklari.

Ma’lumotlarni uzatish protokollarining zaifliklari

Uyali telefon yoki "mobil terminal" operator tarmog’iga bazaviy stansiyalar orqali ulanadi. Bitta bazaviy stansiya bir vaqtning o’zida bir necha mobil terminallarga xizmat ko’rsatadi va o’ziga xos "shlyuz" hisoblanadi. Ushbu "shlyuz" orqali so’zlashuvlar, Internet ma’lumotlari va muayyan abonent bilan bog’liq axborot o’tadi.

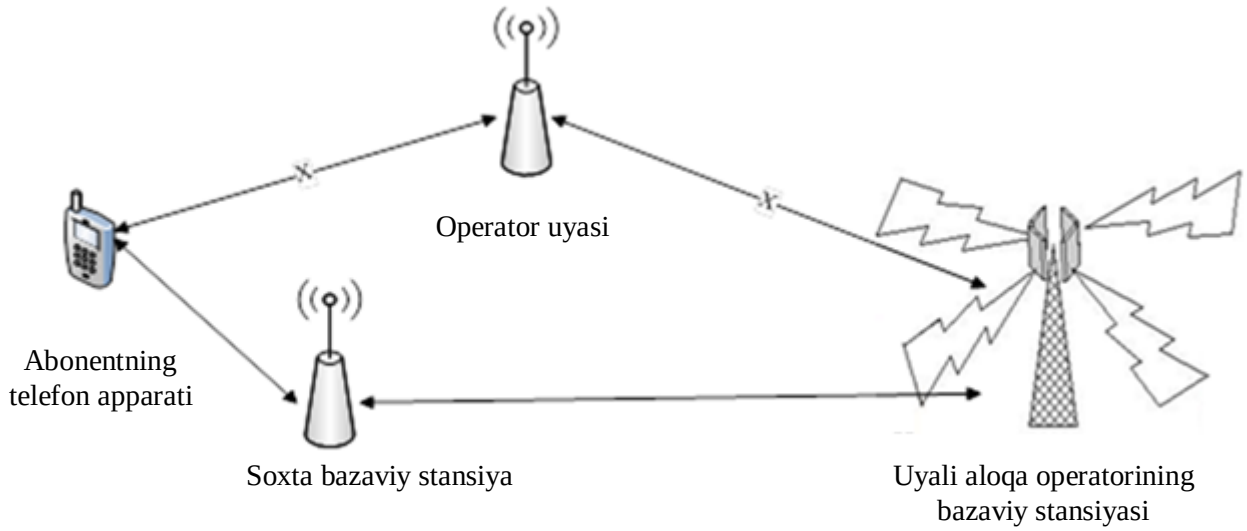
Ochiq radioefirda mobil terminal va bazaviy stansiya ixtisoslashtirilgan A5 algoritm turkumi yordamida shifrlanadi. A5 algoritm turlari quyidagilar:

- A5/0 (shifrlashsiz);
- A5/1 (eng ommaviy, 64-bitli kalit);
- A5/2 (sust shifrlash);
- A5/3 (eng barqaror usul, 128-bitli kalit).

A5/1 va A5/2 shifrlash sxemalari buzilgan, demak, ma’lum maxsus dastur ta’minotiga va unchalik qimmat bo’lmagan texnikaga ega niyati buzuq radioefir orqali foydalanuvchilarning SMS larini ushlab olishi mumkin.

A5/3 algoritmi ishonchli hisoblanadi. Uning buzilganligi xususidagi tasdiqlangan axborot mavjud emas.

Tarmoqda ro’yxatga olingan apparatning ushbu tarmoqqa mansubligi tekshiriladi, telefonning aynanligini esa tarmoq tekshira olmaydi. Bu holdan niyati buzuqlar muvaffaqiyatli foydalanishadi. Ular abonentga yaqin joyga uyali tarmoqning standart bazaviy stansiyasiga o’xshab niqoblangan quvvatli signal manbaini o’rnatadi. Telefon stansiyani "ko’radi" va, bunday stansiya signali quvvatliroq bo’lgani sababli, unga ulanadi (9.4-rasm).



9.4-rasm. Abonent apparatidan qo’ng’iroqlarni
va xabarlarni ushlab olish sxemasi

Ulanishdan so’ng, stansiya telefonga A5/0 algoritmiga o’tishni, ya’ni shifrlashni uzishni "buyuradi". Bunda telefon bo’ysinishga majbur. Endi barcha so’zlashuvlar va SMS lar ochiq holda niyati buzuq tizimi orqali o’tadi. Hech nimani buzish kerak emas: telefon soxta bazaviy stansiya buyruqlarini ko’r-ko’rona bajaradi va shifrlashni uzadi.

Ushbu usulda apparat haqiqiy stansiyaga ulanmasligi uchun niyati buzuq abonentga yaqin joyda bo’lishi lozim. Soxta bazaviy stansiya kiruvchi qo’ng’iroqlarni va SMS larni qabul qila olmaydi, chunki yo’nalish o’zgarganda noto’g’ri nomer ko’rsatiladi.

Hozirgi vaqtda aksariyat uyali operatorlar abonentlarga shifrlash uzilganligi xususida maxsus piktogramma yoki matn orqali xabar beradilar.

Zamonaviy 3G- va LTE-tarmoqlar tutib olinishdan juda yaxshi himoyalanganlar. Himoyalanish muammolari yangi texnologiyalarni (A5/3 shifrlash algoritmini, himoyalangan autentifikatsiya algoritmlarini, A5/1 algoritmini kuchaytirish) joriy etish orqali echiladi.

Uzatish texnologiyalari (RFID) zaifliklari

RFID - radiosignallar yordamida ob'ektlarni avtomatik tarzda identifikatsiyalash usuli bo'lib, ularda RFID-metkada saqlanuvchi ma'lumotlar o'qiladi va (yoki) yoziladi. Har qanday RFID-tizimi o'quvchi qurilmadan va RFID-metkadan tashkil topgan. RFID-metka ikki qismdan iborat:

- axborotni saqlashga va ishlashga, radiochastota signalini modulyatsiyalashga va demodulyatsiyalashga mo'ljallangan integral sxema (mikrochip);
- signalni qabul qiluvchi va uzatuvchi antenna.

Ishlatiluvchi xotira xili bo'yicha quyidagi RFID-metkalar farqlanadi:

- *RW (Read and Write)* - bunday metkada identifikator va axborotni o'qish/yozish uchun xotira bloki mavjud. Ularda ma'lumotlar ko'p marta qayta yozilishi mumkin;
- *WORM (Write Once Read Many)* – bunday metkada noyob identifikatordan boshqa, keyinchalik ko'p marta o'qilishi mumkin bo'lgan, bir marta yoziluvchi xotira mavjud;
- *RO (Read Only)* – yasalishida faqat bir marta ma'lumotlar yoziladi. Bunday metkalar faqat identifikatsiya uchun yaroqli. Unga hech qanday yangi axborotni yozish mumkin emas va ularni qalbakilashtirishning iloji yo'q.

Hozirda energiya manbai o'rnatilmagan *passiv RFID-metkalar* keng tarqalgan. Bunday chip-metkaning ishlashi va javob signalining uzatilishi antennada induksiyalanuvchi elektrotok hisobiga ta'minlanadi. Passiv RFID-metkalar odatda stikerga (magazindagi tovar etiketkasi) o'rnatiladi yoki teri ostiga kiritiladi. O'qishning maksimal distansiyasi, tanlangan chastota va antenna o'lchamiga bog'liq holda, 10 sm dan to bir necha metrgacha bo'ladi.

Aktiv RFID-metkalar shaxsiy ta'minot manbaiga ega. Shunga binoan, signal katta masofadan o'qiladi, chiplarning o'zi esa katta o'lchamga ega va qo'shimcha elektronika bilan jixozlanishi mumkin.

Aktiv metkalarda shaxsiy ta’minot manbai hisobiga, chiqish signalining sathi passiv metkalarga nisbatan yuqori. Bu aktiv metkalarni suvda, inson va hayvonlar tanasida, metallarda (kema konteynerlari, avtomobillar), havoda katta masofada qo’llashga imkon beradi. Aktiv metkalarni ishlab chiqarish katta mablag’ni talab etadi va ularning o’lchami katta.

Uzatish texnologiyalari RFID ning afzalliklari:

- *qayta yozish imkoniyati.* RFID-chiplarda saqlanuvchi ma’lumotlar ko’p marta qayta yozilishi va to’ldirilishi mumkin;

- *saqlanuvchi ma’lumotlarning katta hajmi.* RFID-metka, shtrix-kodga nisbatan, axborotni katta hajmini saqlashi mumkin. 1 sm^2 yuzali chipda axborotning 10000 bayti, shtrix-kodda esa bayt birliklari saqlanishi mumkin;

- *oshkora ko’rinishiga ehtiyojning yo’qligi.* Shtrix-koddan farqli holda, metka bilan o’qish vositasining o’zaro orientatsiyasining ahamiyati yo’q. Metkaning ro’yxatga olish zonasiga qisqa muddatga kirishi va, xususan, katta tezlikda siljishi yetarli. Metka o’rov orqali o’qilishi mumkin. Bu ularni yashirin tarzda joylashga imkon beradi;

- *katta masofadan o’qilishi.* RFID-metka, shtrix-koddan farqli holda, aytarlicha katta masofadan o’qilishi mumkin. O’qilish radiusi bir necha yuz metrni tashkil etishi mumkin;

- *tashqi omillar ta’siriga barqarorlik.* Maxsus RFID-metkalar ishchi muhitning qat’iy sharoitlarida yetarlicha puxtalikka va chidamlikka ega. Bitta ob’ekt ko’p marta ishlatiluvchi sohalarda radiochastotali metka identifikatsiyaning, iqtisod nuqtai nazaridan, eng foydali vositasi hisoblanadi. Passiv RFID-metkalarning ekspluatatsiya muddati esa chegaralanmagan;

- *intellektuallik.* RFID-metka nafaqat ma’lumotlarni eltishi, balki boshqa masalalarni ham echishi mumkin. Metkadagi ma’lumotlar shifrlanishi mumkin. Bitta metkada bir vaqtda ochiq va yashirin ma’lumotlarni saqlash mumkin.

Uzatish texnologiyalari RFID ning kamchiliklari.

- tizim narxining nisbatan yuqoriligi;

- elektromagnit xalallar ta’siriga zaifligi;

- RFID ning insonlar xususidagi axborotning noqonuniy ishlatish imkoniyati.

Mobil to'lovlardagi zaifliklar va ulardan himoyalanish bo'yicha tavsiyalar

Zamonaviy smartfonlar qator zaifliklarga ega. Masalan, yaqinda Exynos 4210 va 4412 prosessorlar bazasidagi Android-smartfonlarning jiddiy zaifligi aniqlangan. Qurilmaning fizik xotirasi bilan ishlovchi tizimli biblioteka naborining xavfsizlik tizimida raxna borligi aniqlandi. Ushbu raxnadan foydalangan niyati buzuq yoki zararli ilova smartfonning barcha fizik xotirasidan root foydalanish huquqiga ega bo'lishi mumkin.

Xaker yoki virus root foydalanish huquqiga ega bo'lib, mobil qurilmaning fizik xotirasiga xohlaganicha tus berishi mumkin. So'z nafaqat smartfonda saqlanuvchi barcha ma'lumotlarni o'g'irlash mumkinligi, balki qurilma xotirasini to'la formatlash xususida so'z boradi.

Root foydalanishni ishlatuvchi ustomon va mohir usullar mavjud. Masalan, niyati buzuq telefonni ma'lum nomerni terishga va tarifikatsiyasi yuqori qisqa nomerga xabarlarni jo'natishga majburlab, mablag'ni o'g'irlashi mumkin. Niyati buzuq o'zining nomerini terib sizning telefoningiz atrofidagi sodir bo'luvchi barcha hodisani, dasturiy shlyuzni o'rnatib esa sizning qo'ng'iroqlaringizni eshitish imkoniyatiga ega bo'ladi. Bu holda mobil telefon tinglash va ta'qib qiluvchi qo'ng'izchaga ("juchok"ga) aylanadi.

NFS modulli Android-smartfonlar ham xavfsizlikning ba'zi muammolariga ega. Ushbu raxnalar niyati buzuqlarga NFS dan foydalanib foydalanuvchilar telefonlariga fon rejimida zararli dasturlarni yuklash imkoniyatini beradi.

Android-smartfonlarda aniqlangan oxirgi zaifliklardan biri Internetdan foydalanish ruxsatiga ega ixtiyoriy ilovaga foydalanuvchining shaxsiy ma'lumotlarini, xususan SMS ma'lumotlarini (telefon nomerlarini va xabarlarning shifrlangan matnini) yig'ish va uzatish imkonini beradi.

Shunday ilova mavjudki, nafaqat yuqorida tilga olingan axborotdan foydalana oladi, balki har qanday avtorizatsiyalanmagan foydalanuvchiga ushbu axborotni lokal porti so'rovi bo'yicha taqdim etish qobiliyatiga ega. Bunda Internetdan foydalanish ruxsatidan boshqa maxsus ruxsatlar talab etilmaydi. Ushbu ruxsat olingan ma'lumotlarni xohlagan joyga va kimsaga uzatishga imkon beradi.

Mobil telefonlardan tovarlar va xizmatlarni to'lov vositasi sifatida foydalanilganda quyidagi qoidalarga rioya qilish tavsiya etiladi:

- Internet sahifaga havola yoki qisqa nomerga xabar jo’natish iltimosi mavjud xabar olinganida, agar siz tovarga yoki xizmatga buyurtma bermagan bo’lsangiz, hech qanday harakatni bajarmaslik;

- qisqa nomerga xabar jo’natmasdan oldin operatordan xabar jo’natish narxini aniqlash lozim;

- tovarga yoki xizmatga buyurtma berishdan oldin ularni taqdim etish shartlarini hamda "*" simvol bilan joylashtirilgan axborotni sinchiklab o’qish;

- begona abonent hisob varag’iga pulni o’tkazishdan oldin moddiy yordam beriluvchi shaxsni aniqlash lozim;

- notanish SMS-konkurslarda va SMS-o’yinlarda ishtirok etmaslik;

- shubhali saytlarga telefon nomerini kiritmaslik;

- "mobil o’tkazma" xizmati ishlatilganida telefon nomerini terishda hushyorlik zarur;

- uchinchi shaxsga telefon bermaslik;

- ishlatilish zarurati bo’lmaganida Bluetooth va Wi-Fi ni o’chirib qo’yish.

Mobil telefondan ma’lumotlarni uzatishda protokollardan, texnologiyalardan, operatsion tizimlardan va dasturiy ta’minotdan foydalanishdagi tavsiyalar:

- ma’lumotlarni uzatishning kriptografik himoyasi o’chirilgan bo’lsa, aksariyat operatorlar u xususida o’z abonentlarini telefon ekranidagi mos ikonka mavjudligi orqali xabardor qiladi. Bunday ikonka mavjudligida telefondan qo’ng’iroq qilish, xabarlarni uzatish va Internetga chiqish tavsiya etilmaydi;

- ma’lumotlarni uzatishning RFID texnologiyasi ishlatilganida shubhali o’quvchi vositalari orqali axborotni uzatishda telefondan foydalanmaslik lozim. NFC modullarini faqat ixtisoslashtirilgan ishonchli ishlab chiqaruvchilardan xarid qilish kerak;

- mobil telefon operatsion tizimi himoyasini ta’minlash uchun avvalo virusga qarshi dasturiy ta’minotni o’rnatish zarur. Virusga qarshi dasturiy ta’minotni shubhali serverlardan emas, balki mobil operatsion tizimlarni ishlab chiqaruvchilarining har birida mavjud Internet resursdagi ishonchli dasturiy ta’minotni olish mumkin. Bunda, hatto shaxsiy ma’lumotlar o’g’irlangan holda etkazilgan moddiy zarar sud orqali qoplanishi mumkin;

- mobil to’lovlarning asosiy "muammosi" - niyati buzuq qo’lida o’g’irlangan uyali telefonning mavjudligi. Telefon o’g’irlangandagi harakatlarni blokirovka qilish uchun zudlik bilan SIM-kartani blokirovka

qilish lozim. Undan tashqari, o’g’irlangan uyali telefonda mobil bank bilan amallar uchun ilovalar o’rnatilgan bo’lsa, mobil bankdan foydalanish parolini almashtirish tavsiya etiladi;

- unutmaslik lozimki, agar telefon o’g’irlangan bo’lsa nomerni almashtirish yetarli bo’lmaydi, chunki SIM-karta nomeri telefonning IMEI identifikatoriga bog’langan. Qanday nomer ishlatilganidan qat’iy nazar, niyati buzuq IMEI ni bilib olib qurilmani aniqlashi mumkin.

10 BOB. BULUTLI HISOBLASHLARDA AXBOROTNI HIMOYALASH USULLARI

10.1. Mobil ilovalar va bulutli hisoblash tizimlarining o’zaro ta’sir arxitekturasi

Bulutli hisoblashlar - Internet ("bulut") orqali serverlar, axborot saqlagichlari, ma’lumotlar bazasi, tarmoqlar, dasturiy ta’minot va h. xizmatlarini taqdim etish. Bulutli hisoblashlarni soddalashtirilgan holda masofadagi serverda joylashgan brauzer asosidagi ilova sifatida tasavvur etish mumkin. Boshqacha aytganda, "bulutli hisoblashlar" - provayder tomonidan iste’molchi so’rovi bo’yicha masofadagi hisoblash resurslarini taqdim etish. Bu oddiy foydalanuvchi uchun, uning bulutli hisoblashlar xususida bilishiga yetarli. Ammo, aslida, bulutli hisoblashlarning imkoniyatlari g’oyat katta.

Bulutli hisoblashlarning eng katta afzalliklaridan biri axborot saqlagichidir. Misol tariqasida Internetdagi elektron pochta xizmatlarini ko’rsatish mumkin. Pochta xizmatlari ko’pincha bulutdagi bo’lishi mumkin bo’lgan makondan foydalanib foydalanuvchilarga xotiraning katta hajmini taqdim etadi, chunki ular uchun bu arzon. Natijada ma’lumotlar yo’qolishini bartaraf etish imkoniyati yaratiladi. Oxirgi yillarda ko’pgina yirik banklarda mijoz xususidagi muhim axborotning yo’qolishi haqida gaplar ko’paygan edi. Agar ushbu axborot bulutli muhitda saqlanganida, ma’lumotlarning yo’qolishi ehtimolligi aytarlicha kamaygan bo’lar edi.

Mobil qo’rilmalardan foydalanuvchi bulutli texnologiyaning rivojida muhim omil hisoblanadi. Bulutli texnologiyadan foydalanuvchi apparat vositalariga va dasturiy ta’minotga kapital xarajatisiz axborot va ilovarni almashishlari mumkin. Barcha hisoblash amallari bulut ichida amalga oshirilishi sababli, yuqori texnologiyali apparat vositalariga ehtiyoj qolmaydi. Natijada foydalanuvchilar uchun mobil qurilmalar narxi pasayadi.

10.1-rasmda OpenMobster (Open Source Mobile Cloud Platform) ochiq platforma misolida mobil ilovalar va bulutli hisoblash tizimlarining o’zaro ta’sir arxitekturasi keltirilgan.

Mobil qurilmalar tarafidan zaruriy namunaviy xizmatlar

Sinxronizatsiya xizmati - ushbu xizmat mobil qurilmada qilingan barcha o’zgarishlarni bulutli serverga qaytarib yuboradi.

OfflintAPp xizmati - ushbu xizmat Sync va Push kabi pastki sath xizmatlari ishidagi muvofiqlikni yaratishga imkon beradi; dasturchini sinxronlashni bajarish kodini yozishdan ozod qiladi, chunki muayyan vaziyat uchun sinxronlashning qaysi mexanizmi yaxshiroq mos kelishini ushbu xizmat hal qiladi.

InterApp Bus xizmati - ushbu xizmat qurilmada o'rnatilgan ilovalar orasidagi pastki sath ta'sirini ta'minlaydi.

Tarmoqli o'zaro ta'sir xizmati - ushbu xizmat serverdan push-xabarni olish uchun kerakli uzatish kanalini o'rnatadi; qurilma va server orasida aloqani avtomatik tarzda o'rnatishga imkon beradi. Bu pastki sath xizmati.

Push xizmati - bulutli servis tarqatgan tuzatishlarni boshqaradi; foydalanuvchi ishini yaxshilaydi, chunki foydalanuvchining yangi axborot mavjudligini mustaqil tekshirishi kerak emas.

Ma'lumotlar bazasi xizmati - mobil ilovalar uchun ma'lumotlarni lokal saqlagichidan iborat: platformaga bog'liq holda saqlash uchun mos imkoniyatlar ishlatiladi. Ushbu xizmatning asosiy vazifasi - ma'lumotlarni saqlash va ulardan xavfsiz foydalanishni ta'minlash. Network kabi pastki sath xizmati hisoblanadi.

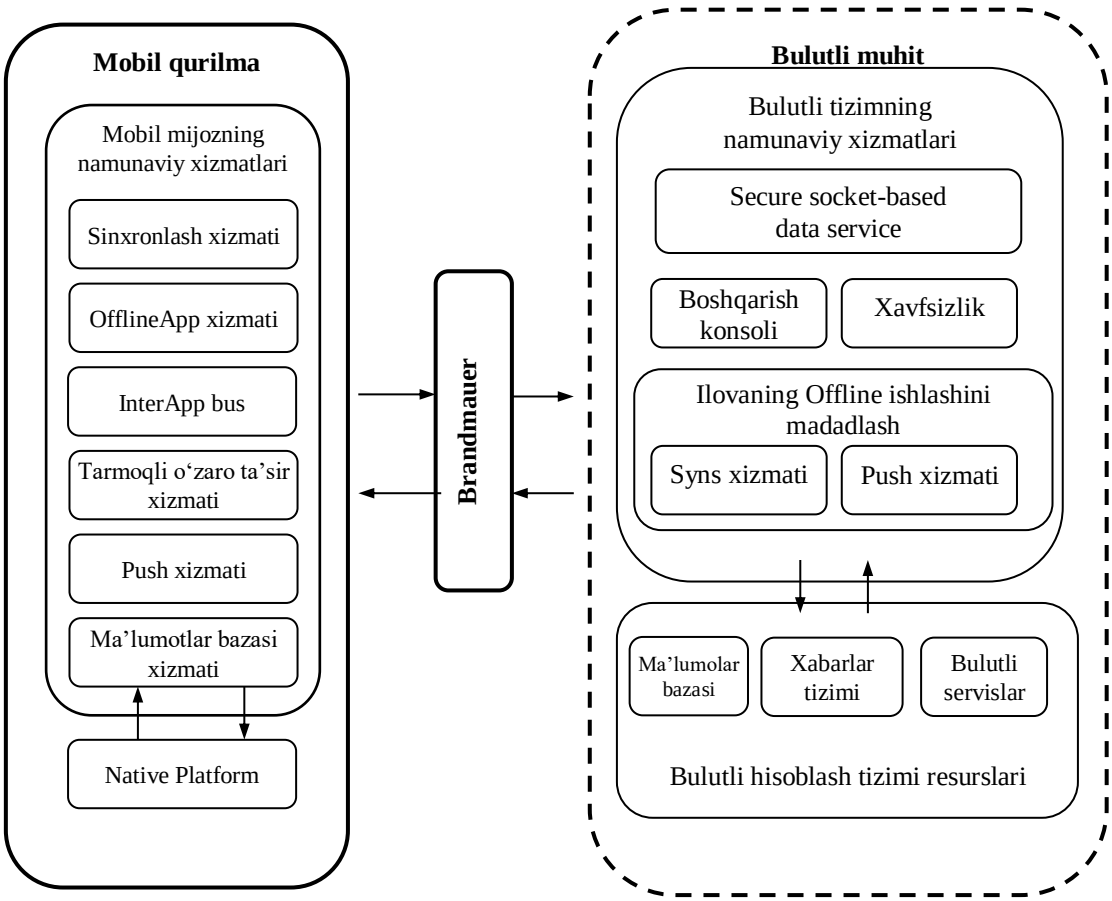
Bulutli muhit tarafidan zaruriy namunaviy xizmatlar

Sync xizmati (Cloud Syncronization) - bulutli saqlagichda joylangan ma'lumotlarni foydalanuvchining mobil qurilmasidagi ma'lumotlar bilan avtomatik tarzda sinxronlash texnologiyasi.

Push xizmati - server Push xizmati yangilashlar uchun ma'lumotlarni uzatish kanallarini kuzatadi. Yangilashlar aniqlangani onida qurilmaga mos xabar jo'natiladi. Qandaydir sababga ko'ra qurilma tarmoqdan uzilgan bo'lsa, xizmat kutadi va so'ngra, qurilma yangitdan ulanishi bilanoq, xabar etkaziladi.

Secure Socket-Based Data Service xizmati - ushbu xizmat ilova talab qiluvchi xavfsizlik darajasiga bog'liq holda plain socket yoki SSL socket serverlarni yoki ikkalasini ta'minlaydi.

Xavfsizlik - ushbu komponent autentifikatsiyani va avtorizatsiyani ta'minlaydi. Natijada, bulutli serverga ulangan mobil qurilmalarning haqiqatan undan foydalanishlariga ishonch hosil qilinadi. Har bir qurilma oldindan ro'yxatdan o'tishi lozim. So'ngra, qurilma autentifikatsiya/avtorizatsiya muolajasidan o'tadi va undan keyingina serverdan foydalanishga ruhsat oladi.



10.1-rasm. OpenMobster platforma arxitekturasi

Boshqarish konsoli - har bir bulutli server foydalanuvchiga tizimni boshqarish va ma’murlash (masalan, ma’lumotlarni masofadan yo’q qilish, masofaviy blokirovkalash va h.) imkonini beruvchi maxsus ilovaga ega bo’lishi lozim.

10.2. Mobil texnologiyalarda bulutli hisoblashlardagi muammolar va ularning yechimi

Bulutli hisoblashlar nafaqat foydali tomonlarga ega, balki bulutli xizmatlarni taqdim etish uchun quyidagi zarur talablar qondirilishi lozim.

- ilova funksiyalarini bulut va qurilma tarafidan ajratish imkoniyati;
- tezkor javob uchun tarmoqning past latentligi;
- bulut va qurilma orasida ma’lumotlarni tezlik bilan uzatish uchun tarmoqning yuqori o’tkazish qobiliyati;

- xarajatlarni optimallashtirish maqsadida tarmoq holatini adaptiv monitoringlash;

- kanalni nazoratlash uchun doimiy tarmoq ulanishi;

- so’rov bo’yicha ulanishni madadlash imkoniyati;

- energiya samaradorligini va kam chiqimlikni hisobga olgan holda tarmoqni tanlash imkoniyatiga egaligi.

Ushbu talablar bulutli resurslarni ishlatishga qator cheklashlar qo’yadi va echilishi lozim bo’lgan qator muammolarni kelib chiqaradi:

Barcha e’tirof etgan ochiq standartlarning mavjud emasligi. Bulutli xizmat provayderlari orasidagi mobillik va o’zaro ta’sir mumkin emas. Bu bulutli texnologiyalarning tezkor rivojlanishini va keng ishlatilishini qiyinlashtiradi. Foydalanuvchilar o’zlarining joriy ma’lumot manbalarini bulutli platformalarga istar-istamas o’tkazadilar, chunki bulutli platformalarda qator echilmagan texnik muammolar mavjud.

Masshtablanishning cheklanganligi. Bulutli xizmatlarni ta’minotchilarining aksariyati cheksiz masshtablanishni taqdim etishlari xususida gapiradilar. Aslida, bulutli hisoblashlarning keng tarqalishi va foydalanuvchilar sonining oshishi bilan, bulutli xizmatlarni taqdim etuvchilarning hech qaysisi barcha foydalanuvchilar so’rovlarini qondirish imkoniyatiga ega emas.

Xizmatdan foydalanishdagi ishonchsizlik. Ko’pgina bulutli tizimlarda (xususan Amazon, Google, Microsoft) vaqtincha nosozliklar bo’lib turadi. Bitta ta’minotchi xizmatiga bog’liqlik nosozlik vaqtida tanglik holatiga sabab bo’ladi, chunki ilova bulutli xizmatlarning boshqa ta’minotchisiga o’ta olmaydi. Natijada xizmat ko’rsatish to’xtatiladi.

Xizmat provayderi tomonidan blokirovkalash. Mobillikning mavjud emasligi ilova va ma’lumotlarning bulutli xizmatlarning bir ta’minotchisidan ikkinchisiga o’tishiga imkon bermaydi.

Turli bulutli tizim xizmatlaridan foydalanishning mumkin emasligi. Hozirda bulutli xizmatlarning turli ta’minotchilari orasida o’zaro qo’shilishning yo’qligi ilovalarning turli bulutli hisoblash tizimlari imkoniyatlaridan foydalana olmasliklariga sabab bo’ladi.

Ushbu muammolarni mobil agentlar texnologiyasidan foydalanib echish mumkin.

Mobil agent (MA) texnologiyasi - mobil telefonlar uchun Mail.ru Agent dasturining maxsus versiyasi. MA yordamida abonentlar bilan aloqa, ular manziliga bog’liq bo’lmagan holda, ta’minlanishi mumkin. Hozirda ushbu dastur aksariyat kompyuterlarda butun dunyo bo’yicha on-

line rejimida muloqot vositasi sifatida ishlatiladi. Dastur ovozli, videoli aloqani hamda matnli xabarlarni tarqatishni ta’minlash imkoniga ega. Undan tashqari dastur mobil operatorning imkoniyatidan foydalanib trafikni nazoratlashga imkon beradi. Dasturning o’zi tekin, mablag’ esa faqat foydalanuvchining tarif rejasiga muvofiq uning hisob varag’idan olinadi (internet-GPRS trafigi to’lovi). MA orqali xohlagan telefon nomeriga SMS ni tekin jo’natish mumkin. MA telefon nomerlari yozilgan yon daftarchaning "zaxirali nusxasini" serverda saqlashga imkon beradi (apparat yo’qolishi holi uchun).

Shunday qilib, MA - geterogen kompyuter tarmog’idagi kompyuterlar orasida avtonom tarzda ko’chib yuruvchi va foydalanuvchi tomonidan qo’yilgan masalani echish uchun har bir mashinadagi servislar bilan o’zaro aloqa qiluvchi dasturiy modul. MA foydalanuvchilar va texnik qurilmalar orasida vositachilik sifatida ishlatilishi mumkin. Masalan, agar foydalanuvchi qurilmani boshqarishni xohlasa, ammo mos dasturiy ta’minotga ega bo’lmasa, ma’lumotlar almashish protokoliga ega MA ga murojaat etishi mumkin.

Odatda, foydalanish so’rovlari bulutdan to’g’ridan-to’g’ri Internetga jo’natiladi. Bu tarmoq trafigi tezligining oshishiga va reaksiya vaqtining kamayishiga olib keladi.

Mobil agentlar yordamida bulutli hisoblashlarni ifodalovchi tizimning bazaviy arxitekturasida Task manager ga asoslangan markazlashtirilgan yondashish ishlatiladi. Har bir ma’muriy domen bulutli xizmatlar ta’minlovchisida o’zining virtual mashinasiga va mobil agent joyiga (Mobile Agent Place, MARga) ega. Virtual mashinalaridan biri ko’pgina funksiyalarni (resurslarni indeksatsiyalash, autentifikatsiya, xavfsizlik, billing, avariyali tiklash, buzilishga bardoshlik) bajaruvchi Task manager sifatida tanlanadi.

MA dagi ma’lumotlar strukturasi sifatida ifodalangan foydalanuvchining masalasi bulutga jo’natiladi. MAR mobil agent tomonidan jo’natilgan barcha ma’lumotlarni qabul qiladi. MAR mobil agentdan ma’lumotlar olinganmi yoki olinmaganligidan qat’iy nazar, Task manager ni ogohlantiradi. MAR va Task manager orasida ma’lumotlar almashuvi doimiy.

10.2-rasmda ushbu mobil-agentli yondashishdan foydalanib, bulutli muhitda mobil agentlarni hisoblash tizimining modifikatsiyalangan arxitekturasi keltirilgan.

Ushbu arxitektura mobil texnologiyalarning bulutli hisoblash tizimlari bilan birgalikda ishlatilishidagi ba’zi jiddiy muammolarni echish imkoniyatiga ega va qator afzalliklarni beradi:

Portativlik. Ilova kodini yoki foydalanuvchi masalalarini uzatuvchi mobil agent bir MAR dan boshqa MAR ga, bulutli tizimning o’ziga xos xususiyatiga bog’liq bo’lmagan holda, ko’chishi mumkin, ya’ni portativlik amalga oshiriladi.

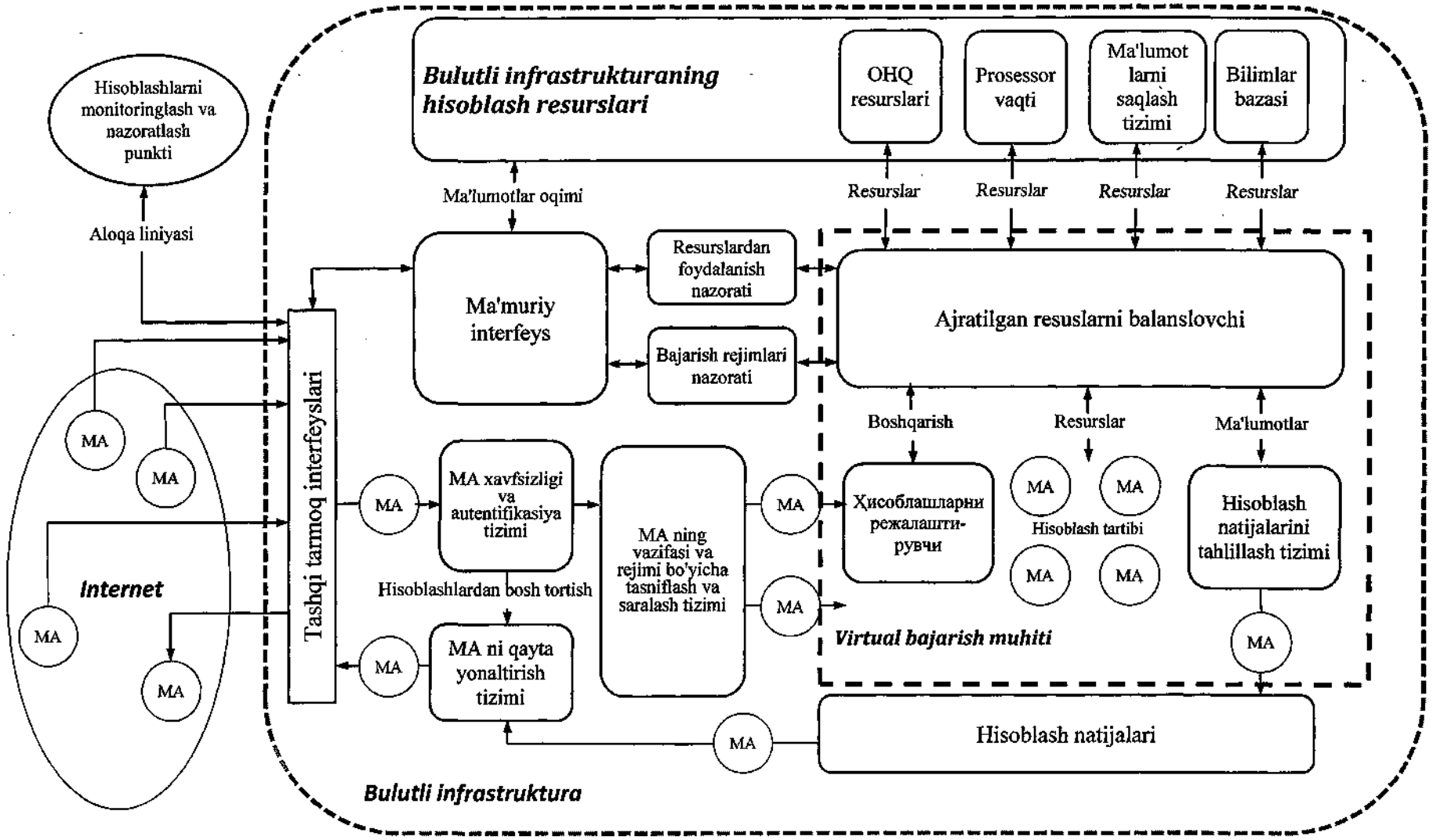
Tarmoq o’zaro ta’sirini standartlashtirish. Turli mijozlar va hisoblash tizimlari uchun o’zaro ta’sirni unifikatsiyalash quyidagilarga imkon beradi:

- tarmoq kanalining beqarorligida tizim ishini barqarorlashtirish;
- yuqori tarmoq yashirinligida tizim ishini normallashtirish;
- elastik mobil ilovalarining (Elastic Mobile Applications) rivoji uchun texnologik asosni yaratish.

Elastik (moslanuvchan) mobil ilovalar mobil qurilma imkoniyatlari bilan cheklanmagan. Qo’shimcha hisoblash quvvati yoki saqlash uchun joy talab qilinganida, ularni bulutdan olish mumkin. Tarmoq o’zaro ta’sir standarti tarmoq protokollari HTTP(S), ma’lumotlar formati va API larni ishlatishga asoslangan. Bu qurilmaga katta moslanuvchanlikni taqdim etadi.

Elastik mobil ilovalar mobil qurilmada yoki bulutda ishga tushirilishi va ular orasida, vaziyatga yoki foydalanuvchi maquligi bog’liq holda, ko’chishi mumkin. Elastik ilovalar arxitekturasi quyidagi komponentlarga ega (10.3-rasm):

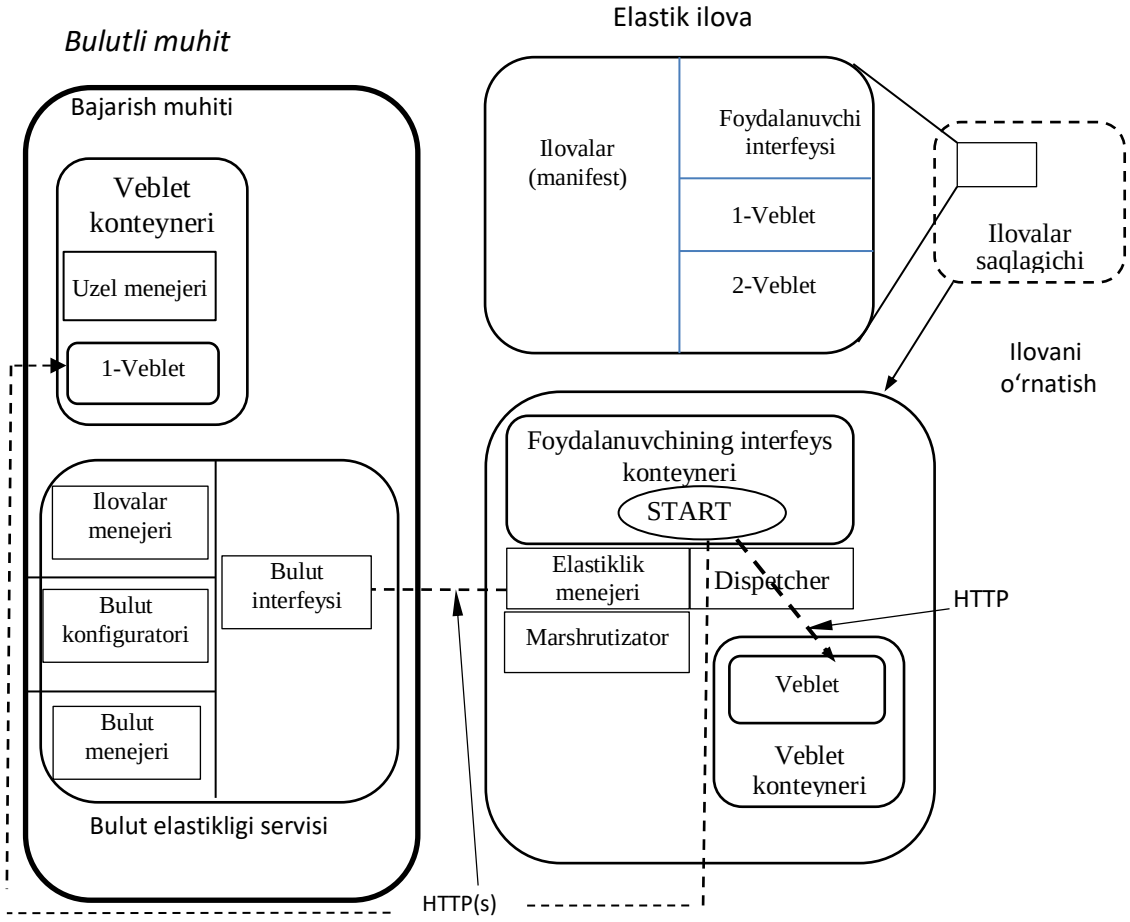
- *elastik ilova* - foydalanuvchi tomonidan tanlanadi va ixtiyoriy platformada, qurilma cheklashlariga muvofiq, ishga tushiriladi;
- *elastiklik menejeri* - qurilmada ishga tushiriladi, weblet (WIDL tilidagi dasturiy modul - "veblet" deb ataluvchi funksional mustaqil va o’zaro ta’sir etuvchi birliklar naboridan tashkil topgan) uchun zaruriy resurslarni nazoratlaydi va boshqaradi;
- *dispetcher* - jarayon kechayotgan joy (mobil qurilmada yoki bulutda) xususida weblet uchun kerakli energiyani aniqlash uchun optimizatorni ishga tushiradi va optimal variantni tanlaydi;
- *bulutning elastiklik servisi* - vebletlarga resurslarni taqsimlaydi. Bulut menejeridan, bulut konfiguratoridan va ilovalar menejeridan tashkil topgan:



10.2-rasm. Bulutli muhitda mobil agentlarni hisoblash tizimning modifikasiyalangan arxitekturasi

- *bulut menejeri* - bulutda ishga tushiriluvchi ilovalarning turli qismlaridan foydalanganligi xususidagi axborotni saqlaydi;

- *ilovalar menejeri* - mobil qurilmada ilovalarni o’rnatish va ishga tushirish imkoniyatini ta’minlaydi;



10.3-rasm. Elastik ilovalarning arxitekturasi

- *bulut konfiguratori* - bulutdagi operativ ma’lumotlarni yig’ishni amalga oshiradi;

- *uzel manejeri* - bulutning har bir uzelida ishlaydi, ilovalar menejeri va bulut menejeri bilan bevosita o’zaro ta’sirda bo’ladi.

Shunday qilib, bulutli hisoblash konsepsiyasi mobil ilovalar rivoji uchun yangi imkoniyatlarni taqdim etadi, chunki hisoblash va ishlash jarayonlarini virtual muhitga ko’chiradi.

10.3. Bulutli hisoblashlarga tahdidlar va ulardan himoyalanish usullari

Bulutli hisoblashlar xavfsizligiga qo’yiladigan talablar ma’lumotlarni ishlash markazlariga qo’yiladigan talablardan farqlanmaydi. Ammo, ma’lumotlarni ishlash markazining virtuallanishi va bulutli muhitga o’tish yangi tahdidlarning paydo bo’lishiga olib keladi.

Quyida bulutli hisoblashlarga asosiy tahdidlar keltirilgan:

- *oddiy serverlarning bulutli hisoblashga ko’chishidagi qiyinchiliklar*. Aksariyat an’anaviy ma’lumotlarni ishlash markazlarida injenerlarning serverlardan foydalanishi fizik sathda nazoratlanadi, bulutli muhitda ular Internet orqali ishlaydilar;

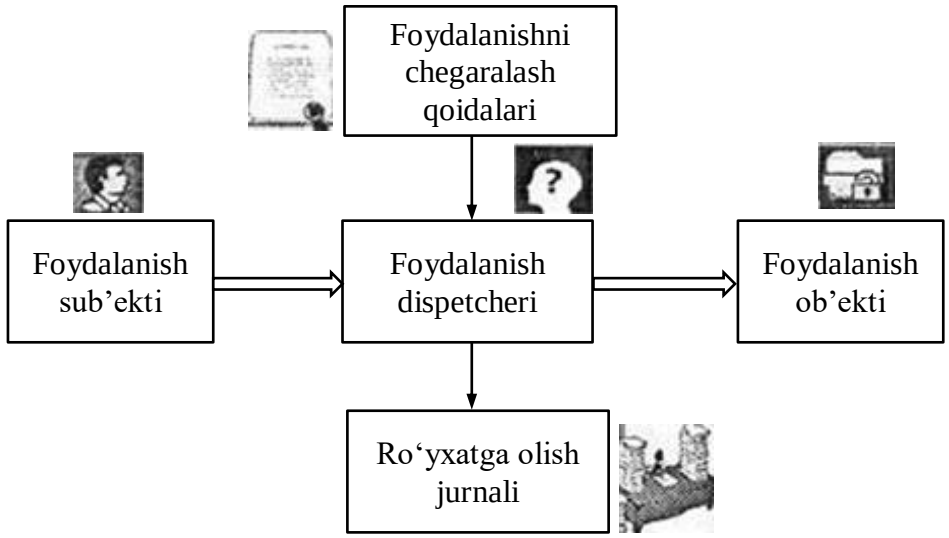
- *virtual mashinalarning dinamikligi*. Yangi mashinani yaratish, uning ishlashini to’xtatish, qaytadan ishga tushirish qisqa vaqt mobaynida amalga oshirilishi mumkin. Ular klonlashtiriladi va fizik serverlar orasida ko’chirilishi mumkin. Bunday o’zgaruvchanlik xavfsizlik tizimining yaxlitligiga ta’sir qiladi. Ammo, virtual muhitda operatsion tizim yoki ilovalarning zaifligi nazoratsiz tarqaladi va ko’pincha vaqtning ixtiyoriy oralig’idan so’ng (masalan, rezerv nusxadan tiklashda) namoyon bo’ladi. Bulutli hisoblashlar muhitida tizim himoyasi uning holatiga va o’rnashgan joyiga bog’liq bo’lmasligi lozim;

- *virtual muhit ichidagi zaifliklar*. Bulutli hisoblash serverlari va lokal serverlar bir xil operatsion tizimlardan va ilovalardan foydalanadi. Bulutli tizimlar uchun masofaviy yorib kirish yoki zararli dasturiy ta’minot bilan zararlanish tahdidi yuqori. Virtual tizimlar uchun risk ham yuqori. Parallel virtual mashinalar "hujumlanuvchi yuzani" kattalashtiradi. Yorib kirishlarni aniqlash va bartaraf etish tizimi virtual mashinalar sathida, ularning bulutli muhitdagi o’rniga bog’liq bo’lmagan holda, zararli aktivlikni aniqlashga qodir bo’lishi shart;

- *ishlamayotgan virtual mashinalar himoyasi*. Virtual mashina o’chirilganida zararlanish xavfiga duchor bo’ladi. Virtual mashinalar obrazlarini saqlagichidan tarmoq orqali foydalanish yetarli bo’ladi. O’chirilgan virtual mashinada himoyalovchi dasturiy ta’minotni ishga tushirish mutlaqo mumkin emas. Bu holda himoya nafaqat har bir virtual mashina ichida, balki gipervizor sathida amalga oshirilishi lozim;

- *tarmoq perimetri himoyasi va tarmoqni chegaralash.* Bulutli hisoblashlardan foydalanilganda tarmoq perimetri yo’qoladi. Natijada tarmoqning kamroq himoyalangan qismi himoyalanishning umumiy

darajasini belgilashi mumkin. Bulutdagi turli ishonch darajasiga ega foydalanishlarni chegaralash uchun virtual mashinalar, tarmoq perimetrini virtual mashinaning o'ziga ko'chirish orqali, o'zlariga himoyani ta'minlashlari lozim (10.4-rasm). Korporativ brandmauer bulutli muhitlarda joylashgan serverlarga ta'sir etishga qodir emas.



10.4-rasm. Foydalanishni chegaralash mexanizmining ishlashi sxemasi

Hozirda bulutli hisoblashlarda axborotni himoyalashning quyidagi to'rtta usuli keng tarqalgan:

- shifrlash;
- uzatishda ma'lumotlarni himoyalash;
- autentifikatsiya;
- foydalanuvchilarni izolyasiyalash.

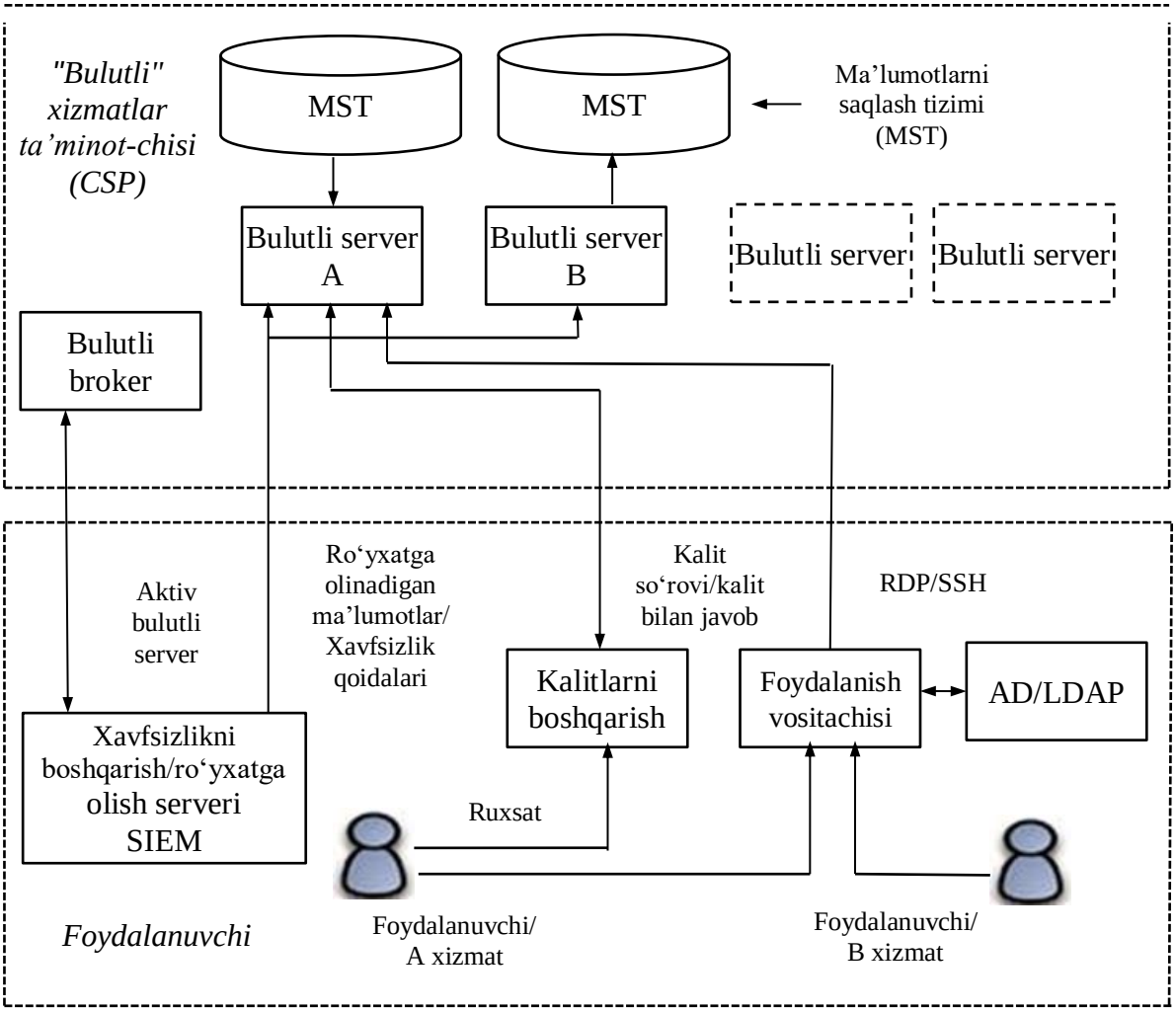
Shifrlash - ma'lumotlarni himoyalashning eng samarali usullaridan biri. Ma'lumotlardan foydalanishni taqdim etuvchi provayder mijozning ma'lumotlarni ishlash markazida saqlanuvchi axborotini shifrlashi hamda zaruriyat bo'lmasa qaytmaydigan qilib yo'q qilishi lozim.

Ma'lumotlarni shifrlashda doimo kalitlar xususida masala paydo bo'ladi. Ularni bulutli serverda saqlash maqsadga muvofiq hisoblanmaydi, chunki bulutli serverlardan yoki shablonlardan foydalanish huquqiga ega sub'ekt kalitdan, demak deshifrlangan ma'lumotlardan foydalanishi mumkin. Kalitni fizik kiritish so'rov bilan almashtiriladi. So'rovni bulutli server tashqi manbaga - kalitlarni boshqarish serveriga (Key Management Server, KMS) jo'natadi.

Bunday yechimning xavfsizligini ta’minlashda hal qiluvchi omil sifatida bulutli serverning va boshqarish serverining, agar ikkalasi bulutli serverlarning bitta provayderida saqlangan bo’lsa, alohida ekspluatatsiyasini ko’rsatish mumkin (10.5-rasm).

Uzatishda ma’lumotlarni himoyalash. Ma’lumotlarni xavfsiz ishlashda ularni shifrlangan holda uzatish majburiy shart hisoblanadi. Ommaviy bulutda ma’lumotlarni himoyalash maqsadida virtual xususiy tarmoq (VPN) tunneli ishlatiladi. Ommaviy bulutli xizmatlarni olish uchun tunnel mijoz bilan serverni ulaydi. VPN-tunnel xavfsiz ulanishni ta’minlaydi va turli bulutli resurslardan foydalanish uchun yagona ism va parolni ishlatishga imkon beradi. Ommaviy bulutlarda VPN-ulanishlar ma’lumotlarni uzatish vositasi sifatida Internet kabi umumfoydalanuvchi resurslarni ishlatadi. Jarayon Secure Sockets Laer (SSL) protokoli bazasida ikkita kalit yordamida shifrlashli foydalanish rejimiga asoslangan. SSL va VPN protokollarining aksariyati opsiyalar sifatida autentifikatsiya uchun raqamli sertifikatlarni ishlatishni madadlaydi. Raqamli sertifikatlar yordamida ma’lumotlarni uzatmasdan oldin, ikkinchi tomonning identifikatsiya axboroti tekshiriladi. Bunday raqamli sertifikatlar shifrlangan ko’rinishda virtual qat’iy disklarda saqlanishi mumkin va ular faqat kalitlarni boshqaruvchi server identifikatsiya axboroti va tizim yaxlitligini tekshirganidan so’ng, ishlatiladi. Demak, bunday o’zaro bog’liqlik zanjiri ma’lumotlarni faqat dastlabki ko’rikdan o’tgan bulutli serverlarga uzatishga imkon beradi. Uzatishda shifrlangan ma’lumotlardan faqat autentifikatsiyadan so’ng foydalanish mumkin.

Autentifikatsiya. Yuqori ishonchlikni ta’minlash uchun ko’pincha tokenlardan va sertifikatlardan foydalaniladi. Bir martali parollar texnologiyasi (One Time password, OTP) autentifikatsiyaning eng sodda va yetarlicha ishonchli usuli hisoblanadi. Bunday parollar, SMS orqali foydalanuvchiga jo’natish bilan, maxsus dasturlar yoki qo’shimcha qurilmalar yoki servislar yordamida generatsiyalanishi mumkin. Bulutli infrastrukturaning masshtablanishining kattaligi va geografik taqsimlanishining kengligi bir martali parollarni olishda birinchi o’ringa, hozirda har kimda mavjud, gadjetlardan foydalanishning paydo bo’lishiga sabab bo’ldi. Avtorizatsiyada provayderning identifikatsiya tizimi bilan o’zaro ta’sirning shaffofligi uchun LDAP (Lightweight Directory Access Protocol) protokolidan va SAML (Security Assertion Markup Language) dasturlash tilidan foydalanish tavsiya etiladi.



10.5-rasm. Foydalanuvchining, kalitlarni boshqarish serverining va bulutli serverning o'zaro ta'sir sxemasi. (RDP/SSh - server bilan Remote Desktop Protocol (RDP) protokoli va SSh shlyuzi orqali ulanish; LDAP (Lightweight Directory Access Protocol) - kataloglardan foydalanishning "yengillashtirilgan" protokoli.

Foydalanuvchilarni izolyasiyalash. Ba'zi provayderlar barcha mijozlarning ma'lumotlarini yagona dasturiy muhitga joylashtiradilar va undagi kodni o'zgartirish hisobiga buyurtmachilarning ma'lumotlarini bir-biridan ajratishga urinadilar. Bunday yondashish bemulohaza va ishonchsiz. Birinchidan, niyati buzuq nostandart koddagi raxnani topishi mumkin. Ushbu raxna niyati buzuqqa u ko'rishi mumkin bo'lmagan ma'lumotlardan foydalanishiga imkon beradi. Ikkinchidan, koddagi xatolik natijasida bir mijoz ikkinchi mijozning ma'lumotlarini tasodifan "ko'rishi" mumkin. Shu sababli, foydalanuvchilar ma'lumotlarini chegaralashda turli

virtual mashinalarni va virtual tarmoqlarni ishlatish eng mulohazali qadam hisoblanadi.

Xulosa sifatida aytish lozimki, xavfsizlik har doim ham faqat himoya yordamida ta’minlanmaydi. Xavfsizlikka ob’ektlarning ishlashi va o’zaro xarakatiga mos qoidalari, xodimlarning yuqori kasbiy tayyorligi, texnikaning buzilmasdan ishlashi, axborot xavfsizligi ob’ektlari ishlashini ta’minlashning turli hillarining ishonchligi orqali erishish mumkin.

11 BOB. SIMSIZ TARMOQ XAVFSIZLIGINING AUDITI VA MONITORINGI

11.1. Simsiz tarmoq xavfsizligining auditi

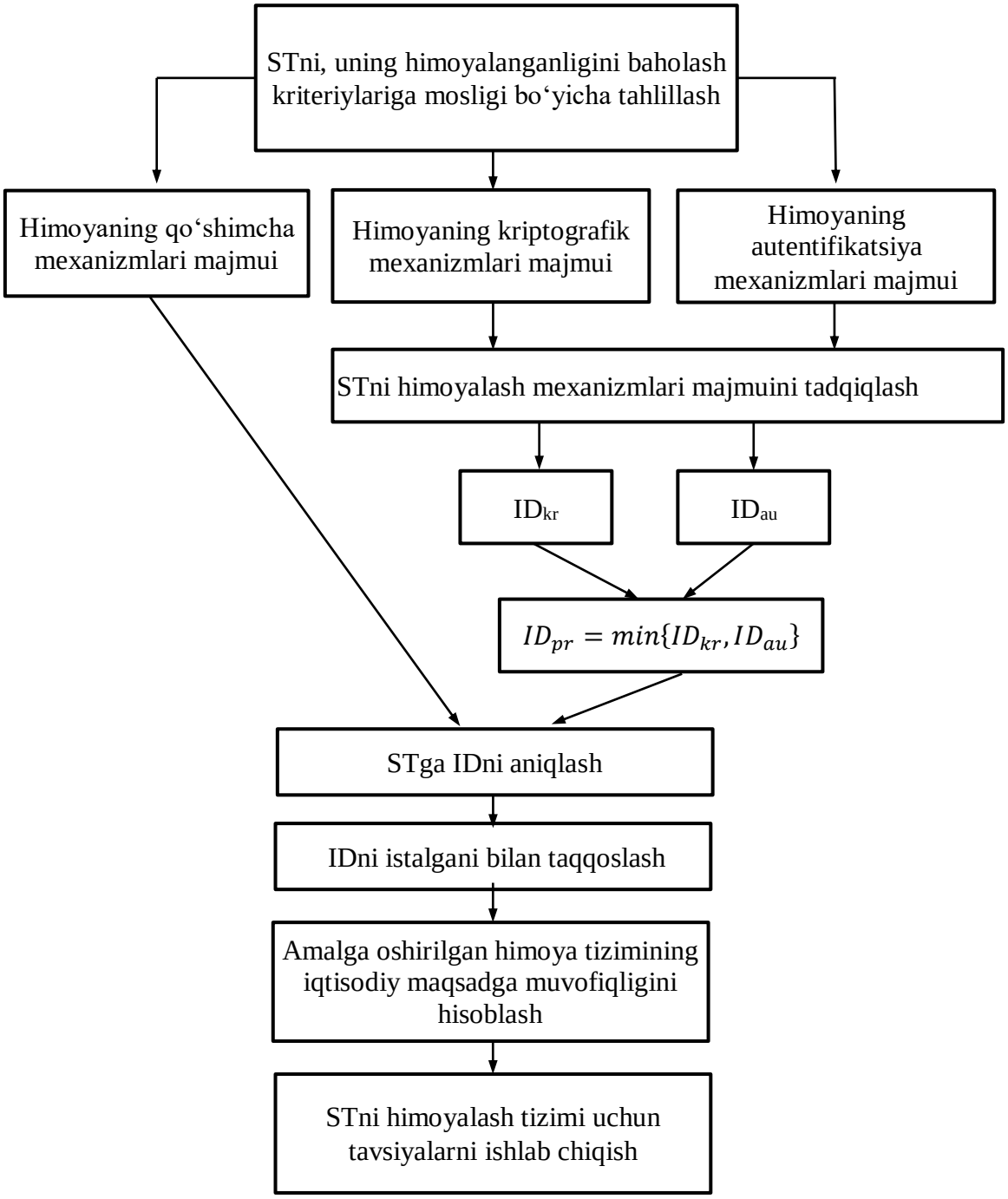
Simsiz tarmoq xavfsizligining auditi - simsiz tarmoqning joriy holatini aniqlashga va olingan ma’lumotlar asosida uni optimallashtirish bo’yicha tavsiyalar paketini shakllantirishga mo’ljallangan muolaja.

Simsiz tarmoq (ST) xavfsizligi - zamonaviy AT-industriyasining eng muhim masalalaridan hisoblanadi. Shu sababli, simsiz tarmoq xavfsizligining muntazam auditi vaziyatni nazoratda ushlab turishning yagona usulidir.

Maqsadga bog’liq holda simsiz tarmoq xavfsizligining auditini masshtablari bo’yicha farqlash mumkin. Juz’iy muammolar kompaniya xodimlari tarafidan hal etilsa, tarmoqning muntazam beqaror ishlashida, kompleks auditni bajarish uchun tashqaridan mutaxassislarni taklif etishga to’g’ri keladi.

Simsiz tarmoq xavfsizligining auditi jarayonini bir necha bosqichga ajratish mumkin (11.1-rasm):

- simsiz tarmoqni, uning himoyalanganligini baholash kriteriylariga mosligi bo’yicha tahlillash;
- axborotni himoyalashning qo’shimcha mexanizmlarini aniqlash maqsadida simsiz tarmoqni tahlillash;
- alohida kriptografik funksiyalar va autentifikatsiya funksiyalari bo’yicha ishlab chiqilgan ishonch darajasi (ID) asosida simsiz tarmoqqa ishonch darajasini belgilash maqsadida, asosiy himoya mexanizmlarining tadqiqi;
- simsiz tarmoqqa ishonchning oraliq darajasini belgilash;
- simsiz tarmoqda amalga oshirilgan himoyaning qo’shimcha mexanizmlarini hisobga olgan holda unga haqiqiy ishonch darajasini aniqlash;
- simsiz tarmoqda amalga oshirilgan axborotni himoyalash tizimining iqtisodiy maqsadga muvofiqligini hisoblash;
- simsiz tarmoqning himoyalanganligini baholash maqsadida va buyurtmachi talabiga muvofiq simsiz tarmoqni himoyalash tizimini o’zgartirish uchun tavsiyalarni ishlab chiqish zaruriyati tug’ilganda, olingan natijalarning haqiqiyligi bevosita ularning malakasiga bog’liq.



11.1-rasm. Simsiz tarmoq xavfsizligining auditi jarayoni

Birinchi bosqichda tarmoq himoyalanganligining passiv auditini o’tkazish lozim. Bunda simsiz tarmoq tadqiqlanadi va mavjud uskuna imkoniyatlariga hamda qo’yilgan maqsad va masalalarga tayangan holda, unda amalga oshirilgan axborotni himoyalash mexanizmlari aniqlanadi. Barcha muolajalarni himoyalanganlikni baholash kriteriylari bo’yicha o’tkazish maqsadga muvofiq hisoblanadi, chunki keyinchalik bu tarmoqqa

ishonch darajasini belgilash va u uchun himoya profilini qurish jarayonini aytarlicha soddalashtiradi va tezlashtiradi.

Ikkinchi bosqich, mohiyatan, birinchi bosqichning davomi va uning qismi hisoblanadi. Farqi shundaki, bu bosqichda asosiy e’tibor tahdid va hujumlarning ma’lum turlariga qarshi choralar sifatida simsiz tarmoqda joriy etilgan axborotni himoyalashning ko’shimcha mexanizmlariga qaratiladi.

Keyingi bosqichda tarmoqqa ishonch darajasini belgilash maqsadida olingan himoyalash mexanizmlari majmuini qiyosiy tahlillash lozim. Avval himoyalash mexanizmlarining har bir guruhi bo’yicha ishonch darajasi aniqlanadi, so’ngra olingan ma’lumotlar asosida umumiy oraliq ishonch darajasi shakllantiriladi.

Undan keyin olingan himoyalashning qo’shimcha mexanizmlari majmuini XFT (xavfsizlikning funksional talablari) bilan solishtirish lozim. Keyinchalik, hatto, simsiz tarmoqni sertifikatsiyalash yoki attestatsiyalash ko’zda tutilmasadi, ushbu jarayon tegishlicha e’tiborga loyiq. Chunki, ushbu jarayon natijalarining to’g’riligi keyingi bosqichda simsiz tarmoqqa haqiqiy ishonch darajasini belgilashga va, umuman, simsiz tarmoq himoyalanganligi darajasi xususida mulohaza yuritishga imkon beradi.

Simsiz tarmoqqa haqiqiy ishonch darajasi aniqlanganidan so’ng, uni buyurtmachi fikri bo’yicha simsiz tarmoqda amalga oshirilishi lozim bo’lgan ishonch darajasi bilan taqqoslash kerak. Quyidagi uchta natija olinishi mumkin:

$$ID > ID_{\text{buyurtma}};$$
$$ID = ID_{\text{buyurtma}};$$
$$ID < ID_{\text{buyurtma}};$$

Bu yerda ID_{buyurtma} - buyurtmachi fikri bo’yicha simsiz tarmoqqa talab qilingan yoki taxmin qilingan ishonch darajasi.

Aniqlangan ishonch darajasi buyurtmachi fikri bo’yicha simsiz tarmoq himoyalanganligiga mos kelgan vaziyat ideal hisoblanadi. Ammo, afsuski, uning ehtimolligi juz’iy. Ko’pincha simsiz tarmoqqa real ishonch darajasi taxmin qilinganligiga teng bo’lmaydi. Bu holda amalga oshirilgan himoya tizimining iqtisodiy maqsadga muvofiqligini hisoblash lozim.

Olingan natijalar asosida va buyurtmachi talabiga muvofiq simsiz tarmoqning istalgan himoyalangan darajasini ta’minlash maqsadida unda ishlatiluvchi himoyalash mexanizmlarini o’zgartirish bo’yicha tavsiyalar berish mumkin.

Himoya tizimini kuchaytirish yoki zaiflashtirish zaruriyati tug’ilganda e’tiborni himoyalash mexanizmlarining turli guruhlari uchun belgilangan ishonch darajasiga qaratish lozim. Shunday vaziyat sodir bo’lishi mumkinki, o’zgartirishga himoya tizimi to’liqligicha duchor bo’lmay, faqat uning uzatiluvchi ma’lumotlarni shifrlashga yoki tarmoqdan foydalanishni nazoratlashga javob beruvchi qismigina o’zgartirilishi mumkin.

11.2. Simsiz tarmoq xavfsizligining monitoringi

Simsiz tarmoq xavfsizligining monitoringi, uning vazifasi bilan bog’liq barcha biznes jarayonlarning maksimal samarali ishlashini madadlash uchun zarur. Tarmoqni tekshirish davriy yoki bir martali bo’lishi mumkin. Tarmoqni davriy tekshirish, odatda, muammolarning paydo bo’lishini oldini olishga yo’naltirilgan, bir martali tekshirish esa mavjud buzilishni lokalizatsiyalash zarurati tug’ilganida yoki berilgan vaqt onida simsiz tarmoq holati xususida xulosa qilish uchun bajariladi.

Shu sababli tekshirish "teranligi" farqlanadi. Davriy tekshirish ko’pincha yuzakiroq, bir martali tekshirish esa simsiz tarmoq holatining maksimal batafsil auditiga yo’naltirilgan.

Simsiz tarmoq rivojining turli bosqichlarida monitoring zarurati tug’ilishi mumkin. Loyihalash bosqichida radioefir monitoringi tarmoq qurilishining o’ziga xos xususiyatiga yoki bo’lishi mumkin bo’lgan xalallarga bog’liq holda foydalanish nuqtasini to’g’ri joylashtirishga yordam beradi. Bunday tekshirish tarmoq rivoji (simsiz tarmoqni kengaytirish) bosqichida ham kerak bo’lishi mumkin. Simsiz tarmoqning joriy holatini baholash foydalanishning yangi nuqtasini kirgizish masalasini engillashtiradi.

Simsiz tarmoqning radiomonitoringi korxona yoki tashkilotning simsiz tarmog’i xavfsizligining yuqori darajasini ta’minlash bo’yicha masalalarni bajarishda kerak bo’ladi.

Quyida, misol tariqasida, simsiz tarmoqlar bo’yicha axborot sirqib chiqish kanalini avtomatlashtirilgan nazoratlovchi ixtisoslashtirilgan vosita sifatida ishlab chiqilgan ZODIAK dasturiy-apparat kompleksi xususida so’z boradi.

ZODIAK dasturiy-apparat kompleksining imkoniyatlari:

- simsiz tarmoqlarni aktiv va passiv rejimlardagi monitoringi;

- vaqtning real rejimida qurilmalar parametrlarining va ulanishlarning nazorati;

- qurilmalar parametrlarining "xavfli" birikmalarini avtomatlashtirilgan kuzatuvi;

- soni cheklanmagan qurilmalar va tarmoqlarning bir vaqtdagi monitoringi;

- tarmoq trafigini monitoringlash dasturiga ko'rinmaydigan yashirin mijozlarni va foydalanish nuqtalarini aniqlashi;

- ko'p zonali tarmoq konfiguratsiyasini madadlashi;

- aniqlangan qurilmalar o'rnashgan joyini belgilashi.

Simsiz tarmoqlarni aktiv va passiv rejimdagi monitoringi. Passiv rejimdagi monitoringda kompleks paketlarni faqat oladi va tahlillaydi. Aktiv rejimdagi monitoringda kompleks maxsus shakldagi paketlarni jo'natib, "yashirin" mijozlarning va foydalanish nuqtalarining aktivlashishini yuzaga keltirishga urinadi. Ushbu rejimda kompleks passiv rejimda ko'rinmaydigan qurilmalarni aniqlashi mumkin.

Vaqtning real rejimida qurilmalar parametrlarining va ulanishlarning nazorati. Kompleks vaqtning real rejimida qurilmalarning quyidagi parametrlarini nazoratlaydi:

- tarmoq adapterining apparat adresi;

- foydalanish nuqtasi uchun tarmoq nomi;

- aniqlanish vaqti;

- aktivlik darajasi;

- aktiv ulanishlar soni;

- qurilma ishlashi rejimi;

- qurilmadan keladigan signal sathi.

Kompleks ulanishlarning quyidagi parametrlarini nazoratlashga imkon beradi:

- qabul qiluvchining tarmoq adapterining apparat adresi (MAS-adresi);

- shlyuzning tarmoq adapterining apparat adresi (MAS-adresi);

- birinchi aniqlangan seans vaqti;

- joriy seans aniqlangan vaqt;

- joriy seans davomligi;

- uzatiluvchi trafik hajmi;

- aktivlik darajasi;

- ulanish protokoli;

- port;

- jo’natuvchining IP adresi;
- qabul qiluvchining IP adresi.

Qurilmalar parametrlarining "xavfli" birikmalarini avtomatlashtirilgan kuzatuvchi. Kompleksda qurilmalar parametrlarining "xavfli" birikmalarini aniqlash uchun qoidalar vositasi amalga oshirilgan. Ular yordamida operator kompleks tomonidan avtomatik rejimda kuzatiluvchi, qurilma parametrlarining "xavfli" birikmalarini beradi. Bunday parametrlar aniqlanganida kompleks xavfni qaydlaydi va oldindan belgilangan harakatlarni bajaradi.

Qoidalar parametrlarning ma’lum nabori bo’yicha qurilmalar va ulanishlar ro’yxatlarini filtrlashni sozlash uchun ishlatilishi mumkin. Bu, masalan, nodolzarb qurilmalar yoki bog’lanishlarni bekitish uchun qurilmalarning "aktiv bo'lmaganida" yoki "yuqori tarmoq aktivligida" axborotni ifodalashni optimallashtirishga imkon beradi.

Soni cheklanmagan qurilmalar va tarmoqlarning bir vaqtdagi monitoringi. Kompleksda ko’p rejimli foydalanish amalga oshirilgan, ya’ni bir necha foydalanishli, xususan yashirin tarmoqlarga (parol, mavjudligi shartida), mijoz sifatida ushbu paketlarni tahlillash bilan, ulanish imkoniyati mavjud.

Tarmoq trafigini monitoringlash dasturiga ko’rinmaydigan yashirin mijozlarni va foydalanish nuqtalarini aniqlash. Kompleks radio ilg’aydigan zonadagi simsiz tarmoqning barcha qurilmalaridan keluvchi ma’lumotlar paketini qabul qiladi va tahlillaydi. Olingan axborot asosida kompleks aktiv qurilmalar va ular parametrlarning ro’yxatini tuzadi. Olingan paketlarning tahlili tarmoq mijozlarini va foydalanish nuqtalarini nafaqat kompleksning radio ilg’aydigan zonasida, balki uning chegarasidan tashqarida aniqlashga imkon beradi.

Ko’p zonali tarmoq konfiguratsiyasini madadlash. Tarmoq strukturasi xususidagi axborot o’zaro bog’langan qurilmalar daraxti va ularning bog’lanishlari ko’rinishida ifodalangan. Bu yangi qurilmalar yoki bog’lanishlarning paydo bo’lishini vaqtning real rejimida kuzatishga imkon beradi.

Aniqlangan qurilmalar o’rnashgan joyini belgilash. Simsiz tarmoq mijozlarini maydoni yoki qavatlar soni katta ob’ektlarda 10 m aniqlikda lokalizatsiyalash uchun kompleksning ko’p zonali konfiguratsiyasi tashkil etilishi lozim.

ZODIAK zakladka qurilmalarini aniqlashga mo’ljallab ishlab chiqilgan. Shu sababli, u "xavfli" qurilmalarni, xususan efirning qonuniy

qurilmalar signallari bilan yuqori yuklanishi sharoitida, samarali aniqlashga imkon beradi.

Demak, ZODIAK binolarni maxsus tekshirish amalga oshirilganida mobil vosita sifatida va taqsimlangan infrastrukturali simsiz tarmoqlarning radiomonitoringida statsionar kompleks sifatida ishlatilishi mumkin.

FOYDALANILGAN ADABIYOTLAR

1. Зубков К. Н., Диасамидзе С. В. Проблемы защиты информации в приложениях для мобильных систем. Ж. Интеллектуальные технологии на транспорте. 2017. № 2.
2. А. С. А. Мутханна, А. А. Атея, М. И. Филимонова. Исследование облачных вычислений в сотовых сетях. Информационные технологии и телекоммуникации. 2017. Т. 5. № 3. Санкт-Петербург.
3. Скабцов Н. "Аудит безопасности информационных систем". Издательский дом "Питер", 2017 г.
4. С.К. Ганиев, М.М.Каримов, З.Т.Худайкулов, М.М.Кадыров. Толковый словарь терминов и понятий по безопасности информации на русском, узбекском и английском языках-Т.: "Iqtisod-moliya" - 2017. 480 с.
5. Сафин Л. К. Исследование информационной защищенности мобильных приложений. Ж. Вопросы кибербезопасности №4(12) - 2015.
6. Безопасность мобильных технологий в корпоративном секторе общие рекомендации. Ассоциация руководителей служб информационной безопасности. Москва, 2015.
7. Лукашов Р. В. «Анализ опыта развития мобильных платежей в мире» ЗАО "Интервэйл", Российская Федерация, 2014 г.
8. Престон Кокс (Preston Cox). Мобильные облачные вычисления: Устройства, тенденции, проблемы и технологии. IBM. Developer Woks. 2014/
9. Мобильные платежи. [Электронный ресурс]. Дата обновления: 03.12.2012. – URL: http://ru.wikipedia.org/Мобильные_платежи (дата обращения: 10.03.2013).
10. Мобильные платежи в контексте СТО БР ИББС и требований по ИБ в НПС. [Электронный ресурс]. Дата обновления: 23.04.2012. – URL: http://slideshare.net/lukatsky/ss-12660626 (дата обращения: 10.03.2013).
11. SMS-платежи: как это работает. [Электронный ресурс]. Дата обновления: 11.02.2013. – URL: http://habrahabr.ru/post/168987/ (дата обращения: 15.03.2013).

12. Мобильная коммерция. [Электронный ресурс]. Дата обновления: 5.05.2011. – URL: http://habrahabr.ru/sandbox/28612/ (дата обращения: 15.03.2013).

13. Бесконтактные платежи. [Электронный ресурс]. Дата обновления: 30.04.2012. – URL: http://habrahabr.ru/company/blog/128564/ (дата обращения: 18.03.2013).

14. Платежи с использованием мобильного телефона. [Электронный ресурс]. Дата обновления: 12.06.2012. – URL: http://mgovservice.ru/technologies/payment/ (дата обращения: 25.03.2013).

15. Мобильный банкинг. [Электронный ресурс]. Дата обновления: 31.08.2011. – URL: http://bankir.ru/publikacii/s/mobilnyi-banking-10000394/ (дата обращения: 16.03.2013).

16. Near Field Communication. [Электронный ресурс]. Дата обновления: 18.04.2012. – URL: http://nfctime.ru/topic/chto-takoe-nfc/ (дата обращения: 18.03.2013).

17. Технология NFC и ее применение. [Электронный ресурс]. Дата обновления: 12.08.2012. – URL: http://rfidsolutions.ru/94.html (дата обращения: 28.03.2013).

18. Взлом сотовых сетей GSM. [Электронный ресурс]. Дата обновления: 9.08.2010. – URL: http://news.tut.by/it/193253.html (дата обращения: 1.04.2013).

19. Радиочастотная идентификация (RFID). [Электронный ресурс]. Дата обновления: 10.04.2013. – URL: http://ru.wikipedia.org/wiki/RFID (дата обращения: 2.04.2013).

20. Уязвимости смартфонов на базе Exynos. [Электронный ресурс]. Дата обновления: 16.11.2012. – URL: http://www.jammer.su/214.html (дата обращения: 9.04.2013).

21. Миноженко А. Евдокимов Д. Анализ безопасности банковских приложений. Ж. Digital Security. 2012.

22. Ю.Р. Акинин, В.Н. Черников, В.Ф. Барабанов. Использование ресурсов облачных вычислительных систем и мобильных агентов при решении задач мобильных технологий. Вестник Воронежского государственного технического университета. 2012. Т.8. № 12. С. 66-68.

23. Степаненко В. Мобильные технологии // Мобильные платежи. – М.: КАРТ БЛАНШ, №5, 2010. – С.4-5

24. Иващук И. Ю. Модель и метод построения семейства профилей защиты для беспроводной сети. Автореферат дисс. канд. Санкт-Петербург. 2010.

25. Багров Е.В. Мониторинг и аудит информационной безопасности на предприятии. Вестник ВолГУ. Серия 10. Вып. 5. 2011.

26. Тужилкин О.В., Чувыкин Б.В. Системы мониторинга на основе беспроводных сетей. Известия ЮФУ. Технические науки. Труды научно-исследовательского института физических измерений. Г. Пенза.

27. С.К. Ғаниев, М.М.Каримов, К.А. Ташев. Ахборот хавфсизлиги. Ўқув қўлланма Т., "Aloqachi", 2008, 382 бет.

28. "Ахборот технологиялари. Ахборот хавфсизлиги. Атамалар ва таърифлар". Узбекистан Давлат стандарта. O'z DSt ISO/IEC 2382-8:2007.

29. В.Г. Олифер. Защита информации при работе в Интернет// Connect. -2002. -№ 11.

30. Н.А. Олифер. Дифференцированная защита трафика средствами IPSec //LAN.-2001.":7R)4; http://www.osp.ru/lan/ 2001/04/ 024.htm.

31. Н.А. Олифер. Протоколы IPSec. //LAN.-2001.-M03; http://www.osp.ru/lan/2001/03/024.htm.

32. Гейер, Джим. Беспроводные сети. Первый шаг: Пер. с англ. - М. : Издательский дом "Вильяме", 2005. –192 с.: ил. – Парал. тит. англ.

33. Спутниковые системы навигации. Учебное пособие. Киев. 2008 г.

34. Максим М. Безопасность беспроводных сетей / Мерритт Максим, Дэвид Поллино ; Пер. с англ. Семенова А. В. - М. : Компания АйТи ; ДМК Пресс, 2004. - 288 с.: ил. - (Информационные технологии для инженеров).

35. Столлингс В. Беспроводные линии связи и сети.: Пер. с англ. – М.: Издательский дом "Вильямс", 2003. – 640 с.

36. Вишневский В., Ляхов А., Портной С., Шахнович И. Широкополосные беспроводные сети передачи информации. - М.:Эко-Трендз, 2005. – 592 с.

37. Григорьев В.А., Лагутенко О.И., Распаев Ю.А. Сети и системы радиодоступа. – М.:Эко-Трендз, 2005. – 384 с.

38. Рошан Педжман, Лиэри Джонатан. Основы построения беспроводных локальных сетей стандарта 802.11.: Пер. с англ. - М.: Издательский дом "Вильямс", 2004. – 304 с.

39. Доступ к беспроводным сетям и безопасность сетей стандарта 802.1X: мифы и факты. Техническое описание. www.flukenetworks.com

40. Расширяемый протокол идентификации (EAP) (Extensible Authentication Protocol (EAP). Энциклопедия сетевых протоколов. www.protocols.ru

41. Н.А. Беляев. Организация безопасных вычислений на распределенных мобильных устройствах. Новосибирский государственный технический университет, Новосибирск.

42. Ле-Бодик Г. Мобильные сообщения: службы и технологии SMS, EMS и MMS / Пер. с англ. – М.: КУДИЦ-ОБРАЗ, 2005. – 448 с.

Internet manbalari

1. http://www.tayle.com – сайт компании ТАЙЛЕ.

2. http://www.airdata.ru – сайт компании Air Data Communications.

3. http://www.dlink.ru – сайт компании D-LINK.

4. http://wifi-wiki.ru

5. http://www.wireless.bape3.org

6. http://www.alpha-teleport.info – сайт компании alpha-teleport.info.

7. http://www.ixbt.com – информационный портал.

8. http://www.wireless.ru – специализированный портал, посвященный беспроводным технологиям.

9. http://www.umd.ru – сайт компании УМД проект.

10. http://www.ferra.ru – информационный портал.

11. http://ru.wikipedia.org – википедия, русский проект свободной многоязычной энциклопедии.

12. http://pcweek.ru – сайт журнала PCWeek Russian Edition.

13. http://www.thg.ru – Русский Tom's Hardware Guide, информационный портал.