

ӘОЖ 004.056:681.501.034:625.1(574)

Қолжазба құқығында

САНСЫЗБАЙ ҚАНИБЕК МҰРАТБЕКҰЛЫ

**Теміржол автоматика және телемеханика жүйелері үшін ақпарат
қауіпсіздігін қамтамасыз ету**

6D070300 – Ақпараттық жүйелер

Философия докторы (PhD)
дәрежесін алу үшін дайындалған диссертация

Ғылыми кеңесшілер:
Куандыков А.А., т.ғ.д. профессор
Sergey Vlasenko,
доктор инженер, «Siemens» AG

Қазақстан Республикасы
Алматы, 2020

МАЗМҰНЫ

	НОРМАТИВТІ СІЛТЕМЕЛЕР	4
	БЕЛГІЛЕУЛЕР МЕН ҚЫСҚАРТУЛАР	5
	КІРІСПЕ	6
1	ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МАГИСТРАЛЬДІ ТЕМІРЖОЛ ЖЕЛІСІНДЕГІ ТАТЖ ҚАЗІРГІ ЖАҒДАЙЫН ТАЛДАУ ЖӘНЕ ЖАҒҒЫРТУ ҚАЖЕТТІЛІГІН НЕГІЗДЕУ	11
1.1	Теміржол автоматика және телемеханика үшін қауіпсіздікті қамтамасыз ету жүйелерінің негіздері және даму үрдістері	11
1.2	Қазақстан Республикасы темір жолындағы автоматика және телемеханика жүйелерінің қазіргі жағдайын талдау	14
1.2.1	Электрлік орталықтандыру құрылғыларының қазіргі күйін талдау	16
1.2.2	Пойыздар қозғалысын интервалды реттеу жүйелерінің қазіргі күйін талдау	18
1.2.3	Диспетчерлік орталықтандыру құрылғыларының қазіргі күйін талдау	20
1.3	ҚР-да ТАТ әрекет етуші жүйелерін жаңғыртудың жүзеге асырылмауы жағдайындағы қауіптерді талдау	21
2	ПОЙЫЗДАР ҚОЗҒАЛЫСЫН БАСҚАРУДАҒЫ ҰЛТТЫҚ ЖҮЙЕНІҢ ҚҰРЫЛУЫ МЕН KTCS ЖҮЙЕСІНДЕ ҚОЛДАНЫЛАТЫН РАДИОКАНАЛДА АҚПАРАТТЫ ҚОРҒАУ ӘДІСТЕРІ	26
2.1	Қазақстандық пойыздар қозғалысын интервалды реттеу ұлттық жүйесінің архитектурасы мен жүйенің негізгі элементтері	26
2.2	Сандық радиоканалдар базасындағы интервалды реттеу жүйелерінің ерекшеліктері	35
2.3	Радиоканал базасында пойыздарды басқару жүйелерін құрастыру құрылымдары	37
2.4	Радиоканал қолдану арқылы пойыздар қозғалысын реттеу технологиясы	39
2.5	Сандық радиоканалда ақпарат қорғау әдістері	41
2.5.1	Сандық радиоканалда ақпарат қорғау әдістерін анықтау	41
2.5.2	TETRA стандарты жүйесінің ақпарат қауіпсіздігі	44
2.6	TETRA стандартының жүйелік хаттама моделі	48
3	KTCS ЖҮЙЕСІ МЕН БАСҚАРУ ОРТАЛЫҚТАРЫ АРАСЫНДА СЫМСЫЗ МӘЛІМЕТТЕР ЖІБЕРУДІ ҚАМТАМАСЫЗ ЕТЕТІН TETRA САНДЫҚ РАДИОКАНАЛ АРҚЫЛЫ МӘЛІМЕТТЕР ТАРАТУ КЕЗІНДЕ КІЛТТЕРДІ АУТЕНТИФИКАЦИЯЛАУ ЖӘНЕ ТҮРЛЕНДІРУ	52
3.1	KTCS жүйесінде сандық байланыстың рөлі	54
3.2	Байланыс желілерін зерттеу	56
3.3	Мәліметтер тарату хаттамаларын зерттеу	60
3.4	KTCS кілттер тарату жүйесі	61
3.5	Жер үсті транкингітік радионы аутентификациялау хаттамасының	

	қауіпсіздігін талдау (TETRA)	64
3.6	Радиобайланысты ашудың KTCS-ке әсері	73
3.7	Радиоканал арқылы мәліметтер тарату кезінде кілттерді аутентификациялау және түрлендіру	75
3.8	MAC криптографиялық талдау	80
3.9	EuroRadio кілттерін қалпына келтіру	83
4	МАГИСТРАЛЬДІ ЖЕЛІДЕ АҚПАРАТ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ ҮШІН РАДИОБЛОКТАУ ЖҮЙЕСІН ТӘЖІРИБЕДЕ ҚОЛДАНУ	86
4.1	Эксперименттік сынақ нәтижелері	86
4.2	Теміржол транкингтік байланысы үшін базалық бекетті жабу моделін құру	91
	ҚОРЫТЫНДЫ	94
	ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ	95
	ҚОСЫМША А. Енгізу актісі	103
	ҚОСЫМША Б. Енгізу анықтамасы	104

НОРМАТИВТІ СІЛТЕМЕЛЕР

Бұл диссертацияда келесі стандарттарға сәйкес сілтемелер қолданылды:
ТР ТС 003/2011 «Теміржол көлігі инфрақұрылымының қауіпсіздігі туралы»

Теміржол көлігіндегі техникалық пайдалану қағидаларын. Республикасы Инвестициялар және даму министрі 2015 жылғы 30 сәуірдегі №544 бекіткен.

ҚР СТ РК 1443-2005 Теміржол автоматикасы мен телемеханикасының қауіпсіздігі. Темір жол автоматикасы мен телемеханикасы жүйелері мен құрылғыларының қауіпсіздігін дәлелдеу әдістері

ЦШ/554-10 Сигнализация және байланыс шаруашылығындағы негізгі құрылғылар мен жабдықтар үшін жөндеу сипаттамасы, қызмет ету мерзімі және жөндеу аралық мерзімдері. Астана 2012 ж.

БЕЛГІЛЕУЛЕР МЕН ҚЫСҚАРТУЛАР

«ҚТЖ» ҰК» АҚ – «Қазақстан темір жолы» ұлттық компаниясы» акционерлік қоғамы;

ERTMS European Rail Traffic Management System – Еуропалық теміржол қозғалысын басқару жүйесі;

ETCS European Train Control System – Еуропалық пойыздар қозғалысын басқару жүйесі;

KTCS (Kazakhstan Train Control Systems) – Қазақстандық пойыздар қозғалысын басқару жүйесі;

АБ – автоматты блоктау;

АПС – автоматты переездік сигнализация;

ББОБ – белгі беру, орталықтандыру және блоктау;

ДБ – диспетчерлік бақылау;

ДО – диспетчерлік орталықтандыру;

ДСП – бекет бойынша кезекші;

ЖАБ – жартылай автоматты блоктау;

ЖДО – жиілікті диспетчерлік орталықтандыру

МПДО – микропроцессорлық диспетчерлік орталықтандыру;

МПО – микропроцессорлық орталықтандыру;

МРО – маршрутты-релелік орталықтандыру;

ОАӨЭЫ (ЦАРЭС) – Орталық Азия өңірлік экономикалық ынтымақтастық;

ПҚИРЖ-Е – пойыздар қозғалысын интервалды реттеу жүйесі, радиоарна құралдары бойынша

РБ – радиоблоктау;

ТАТЖ – теміржол автоматика және телемеханика жүйелері;

ШНЦ – ББОБ электромеханигі;

ЭО – электрлік орталықтандыру.

КІРІСПЕ

Зерттеу тақырыбының өзектілігі. Соңғы 10 жылда ақпараттық технологиялар жұмыс тиімділігін арттырып, өндірістік және басқару үрдістерін оңтайландырып, әлемдегі көптеген өнеркәсіп қызметтерінің белсенді қатысушысына айналды. Қазақстан Республикасы Президентінің 2018 жылдың 10 қаңтарындағы Жолдауы [1] Төртінші өнеркәсіптік революция элементтерін жаппай енгізу жолымен дәстүрлі базалық салаларды, соның ішінде логистиканы дамыту бойынша кешенді тапсырма қойды. Нәтижесінде, Қазақстан Республикасы үкіметіне 2025 жылға дейін «Цифрлық Қазақстан» Мемлекеттік бағдарламасының [2] (әрі қарай – Цифрлық Қазақстан) бастамасы болған базалық салаларды технологиялық қайта қаруландыру шараларының кешенін әзірлеу тапсырмасы берілді. Цифрлық Қазақстан бағдарламасына сәйкес көлік-логистикалық саланың әрі қарай өсуін қамтамасыз ету үшін көлік құралдарын басқару жолымен транзиттік әлеуеттің артуына, ақпаратты жедел өңдеу және оңтайлы және ұтымды шешімдер мен басқарушы әсерлер туғызу жолымен көліктегі қауіпсіздікті күшейтуге септігін тигізетін көлік жүйесін енгізу талап етіледі.

Сапалы көлік және логистика инфрақұрылымы аумақ байланысын арттыру және белгіленген жерге дейін тауарды жеткізуге кететін үстеме шығындарды азайту есебінен экономиканың дамуына қуатты серпін береді.

Қазіргі уақытта елде Республиканың көлік кешенін қайта құру және дамыту бойынша белсенді жұмыс жүргізілуде.

Қазақстан Республикасының кең аумағы мен түрлі саласы күшінен көптеген ірі отандық кәсіпорындар үшін теміржол көлігі логистикалық тізбекте басты рөл атқарады [3].

Қазақстанның Еуразия континентінің ортасында, Еуропа мен Оңтүстік-шығыс Азияның кеңінен және серпінді дамып келе жатқан саудаларының арасында орналасуы келешекте отандық теміржол көлігіне жоғары көлік-логистикалық әлеуетін тиімді ашуға мүмкіндік береді [4].

Осылайша, экономикалық кеңістік бірлігі, мемлекет бүтіндігі, елдегі қорғаныс және қауіпсіздік айтарлықтай дәрежеде теміржол көлігінің орнықты және сенімді жұмысына байланысты.

Жаңа темір жолдар аймақтар арасындағы ішкі байланысты қамтамасыз етті, Қазақстанның экспорттық және транзиттік әлеуетін арттырды. Халық арасында «Тәуелсіздік жолы», «Өмір және үміт жолы» деп аталған соңғы 25 жылда Қазақстанда іске асырылған ірі жобалар Ақсу – Дегелең, Хромтау – Алтынсарин, Шар – Өскемен, Өзен – Түркменстанмен мемлекеттік шекара, Жетіген – Қорғас, Жезқазған – Бейнеу, Арқалық – Шұбаркөл және Боржақты – Ерсай теміржол желілері болды [5].

Қазіргі уақытта ірі қалалардың «көлік дәліздерінде» және қала сыртындағы аумақта жүк және жолаушы тасымалы көлемінің тұрақты өсуі байқалады. Мамандардың болжауы бойынша өнімді тасымалдау қажеттілігі даму үрдісіне ие. Сол аралықта көптеген теміржол телімдерінде өткізу

кабілеттілігінің қоры нақты түрде таусылған. Сондықтан, кезекті рет, бірақ жаңа экономикалық, технологиялық және ұйымдық жағдайда, экономикалық мағынада айтқанда, Қазақстан Республикасы теміржол желісінің тасымалдау және өткізу қабілеттілігін арттырудың ұтымды әдістерін анықтау тапсырмасы өзекті болып отыр [4, б. 6].

Қазіргі уақытта «Қазақстан темір жолы «Ұлттық компаниясы» АҚ теміржол желісінде оның үздіксіз жұмыс істеу мақсатында мәліметтер қабылдау және тарату түрлі жүйелерінің көмегімен жауапты құпия ақпараттың елеулі көлемі жіберіледі. Жауапты ақпарат ретінде бұл жерде бұрмалануы жүйені функциялау алгоритмінің қауіпті бұрмалануы орын алатын жұмысқа қабілетсіз күйге әкелетін дискертті жүйеде қолданылатын ақпарат түсіндіріледі. Жауапты ақпарат тасушы командалар тасымалдаудың функционалдық қауіпсіздігіне тікелей әсер етеді. Сонымен қатар, пойыздар қозғалыс кестесі мен орналасқан жері жөніндегі логистикалық ақпарат жоғары коммерциялық құндылыққа ие. Пойыздар қозғалысының қауіпсіздігін қамтамасыз ету негізі темір жол автоматика және телемеханика жүйелері (ТАТЖ) болып табылады [6].

ТАТЖ теміржол көлігінің стационарлық жолдық және жылжымалы объектілерімен қозғалыс қауіпсіздігінің орнатылған деңгейінде бақылау және басқаруды қамтамасыз ететін техникалық құралдар жиынтығын құрайды, онда ақпарат тарату каналдарының рөлі мен талаптары айтарлықтай жоғарылайды. Шетелдік және отандық тәжірибе негізінде ақпарат тарату жүйелерінің даму үрдісі дәстүрлі құралдардан, мысалы рельс тізбектерінен басқа, жаңа жүйелерді, мысалы – сандық радиоканалдар пайдалану қажет екендігін көрсетеді. Бұл ретте сымсыз жүйелердің ақпарат қауіпсіздігі және кедергіден қорғау аспектілері маңызды фактор болып табылады [7].

Қазіргі уақытта жаңа экономикалық жағдайда теміржол көлігі жұмысының тиімділігін арттыру жаңа автоматтандырылған басқару жүйелерін енгізу және тасымалдау үрдісін басқару және оның жүзеге асырылуын бақылау үшін қажетті жедел және мерзімдік ақпаратпен қамтамасыз ету негіздері секілді сенімді және қауіпсіз жоғары сапалы байланыссыз мүмкін емес.

Қазақстан теміржол көлігін ұзақ мерзімдік келешекте дамыту бағдарламасында [8] жаңа ақпараттық технологиялар енгізуге маңызды орындардың бірі жүктелді. Сапалы, жылдам және көлемді сипаттамаларды есепке ала отырып, заманауи инфокоммуникациялық құрылғылар теміржол байланысы, пойыздар қозғалысы, жүк және жолаушылар тасымалының дәстүрлі қызметтерін ұсыну мәселелерін шешіп қана қоймай, сонымен бірге жүк қозғалысын және қазіргі уақытта әрекет етуші байланыс құралдарының техникалық мүмкіндіктерімен шектелетін басқа да қызмет түрлерін бақылауды қамтамасыз ете отырып, тасымалдау үрдісін автоматтандыру бағдарламаларын іске асыру есебінен олардың спектрін елеулі түрде кеңейтуге мүмкіндік береді.

ТАТЖ-да ақпаратты қорғау үшін заңнамалық, ұйымдық және бағдарламалық-техникалық шараларды бірге қолдану талап етілетіндігі белгілі. ТАТЖ ақпарат қауіпсіздігін қамтамасыз етудің негізгі сатылары ақпарат

қауіпсіздігінің негізгі қауіптерін анықтау, оның саясатын, негізгі бағыттарын, қамтамасыз ету және ұйымдық-құқықтық іс-шаралар әзірлеу, ақпараттық қауіпсіздік технологияларын таңдау және бейімдеу болып табылады [9, 10].

Диссертациялық жұмыстың мақсаты. Алғаш әзірленген пойыздар қозғалысын басқарудың ұлттық KTCS (Kazakhstan Train Control Systems) жүйесіндегі ақпараттық қауіпсіздікті қамтамасыз ету болып табылады.

Диссертацияға қойылған мақсаттарға қол жеткізу үшін келесідей **тапсырмалар** шешілуі тиіс:

- «Қазақстан темір жолы» ҰҚ» АҚ инфрақұрылымындағы қолданыстағы теміржол автоматика және телемеханикасы жүйелерінің қазіргі жай-күйіне талдау жүргізу;

- пойыздар қозғалысын басқарудың ұлттық KTCS жүйесінің архитектурасын әзірлеу;

- пойыздар қозғалысын басқарудың ұлттық KTCS жүйесінің TETRA радиоарнасында ақпаратты қорғау әдістерін анықтау;

- жерүсті транкингік радионы (TETRA) аутентификациялау хаттамасының қауіпсіздігін талдау;

- теміржол транкингік байланысының базалық станциясының қамту моделін негіздеу және зерттеу;

- магистральдық желіде ақпараттық қауіпсіздікті қамтамасыз ету үшін радиоблоктау жүйесін практикалық қолдану мақсатында эксперименттік зерттеулер жүргізу.

Жұмыстың **ғылыми жаңалығы** келесі алынған нәтижелермен анықталады:

1. Теміржол автоматика және телемеханика қазіргі жүйелерінің жағдайына талдау жүргізілді.

2. KTCS пойыздар қозғалысын басқару ұлттық жүйесінің архитектурасы алғаш рет әзірленді.

3. Пойыздар қозғалысының ақпараттық қауіпсіздігін қамтамасыз ететін радиоканал арқылы өзара әрекеттесу алгоритмі әзірленді.

4. Пойыздар қозғалысын басқару және қауіпсіздігін қамтамасыз ету жүйесінің жалпылама құрылымы ұсынылды.

Диссертациялық жұмыста алынған нәтижелердің **дұрыстығы** математикалық қатандықтың заманауи деңгейіндегі таңдалған математикалық аппаратты дұрыс қолданумен, ғылыми конференцияларда, семинарларда диссертациялық зерттеулер нәтижелерін сынаумен және оларды енгізумен анықталады.

Зерттеу әдістері. Ғылыми жұмыста қойылған тапсырмаларды шешуде алгоритмдердің күрделілігі теориясының классикалық әдістері, байланыс және ақпарат тарату теориялары, ақпараттық жүйелердің сенімділік теориялары және математикалық модельдеу қолданылды.

Зерттеу объектісі ретінде осы жұмыста автоматика және телемеханика, теміржол көлігінде ақпарат тарату және тасымалдау қауіпсіздігін қамтамасыз ету құрылғылары таңдалды.

Зерттеу пәні болып ақпаратты радиоарна арқылы беру кезінде кілттердің аутентификациясы және генерациясы.

Диссертациялық жұмыс нәтижелерінің сенімділігі таңдалған математикалық аппаратты математикалық қатаңдықтың қазіргі деңгейінде дұрыс қолданумен, диссертациялық зерттеулердің нәтижелерін ғылыми конференцияларда, семинарларда сынақтан өткізумен және оларды енгізумен анықталады.

Тәжірибелік құндылық. Диссертацияда алынған нәтижелер мәлімет тарату кезінде әлемнің түрлі елдері темір жолдарында қабылданған қауіпсіздік нормаларын салыстыру, сондай-ақ «ҚТЖ» ҰК» АҚ үшін «Теміржол автоматика және телемеханика жүйелерін жаңғырту және өндіріс тұжырымдамасы» шаруашылық келісімшарты аясында орындалған тапсырмаларды қосқанда, орталықтандыру құрылғыларын одан да жаңа түрге алмастыруға дайындау үшін қажетті кеңестер ұсыну арқылы оларды талдау кезінде өзекті болып саналады.

Сенімділік дәрежесі мен апробациялау нәтижелері.

Диссертациялық жұмыстың негізгі ережелері баяндалды және талқыланды:

1. «Көліктегі инновациялық технологиялар: білім, ғылым, тәжірибе» тақырыбындағы ХLI Халықаралық ғылыми-тәжірибелік конференция (Қазақстан, Алматы, Тынышбаев атындағы ҚазККА, 2017).

2. Мұхтар Омарханұлы Әуезовтың 120 жылдығына арналған «Әуезов оқулары – 15: Қазақстанның үшінші жаңаруы – Жаңа тұжырымдамалар және заманауи шешімдер» Халықаралық ғылыми-тәжірибелік конференциясы (Қазақстан, Шымкент, М. Әуезов атындағы ОҚМУ, 2017).

3. «Интеллектуалды ақпараттық және коммуникациялық технологиялар – «Қазақстан-2030» Стратегиясы аясында үшінші индустриалдық революцияны жүзеге асыру құралы» V Халықаралық ғылыми-тәжірибелік конференция (Қазақстан, Нұр-Сұлтан, Л.Н.Гумилев атындағы ЕҰУ, 2018).

4. Hyukshin Co. компаниясында дөңгелек үстел, Ltd. (Оңтүстік Корея, Сеул қ.), 2018.

5. Халықаралық ақпараттық технологиялар университетінің 10 жылдығына арналған «Ғылым мен индустриядағы сандық технологиялар – 2019» V Халықаралық конференция (DTSI-2019). (Қазақстан, МУИТ, 2019).

6. «Теміржол көлігіндегі электротехникалық кешендер мен автоматика және телемеханика жүйелерінің тиімділігі мен қауіпсіздігі» халықаралық қатысуымен бүкілресейлік ғылыми-тәжірибелік конференциясы (Ресей, Омск мемлекеттік қатынас жолдары университеті, 2019).

7. «ҚТЖ» ҰК» АҚ филиалы – «Автоматтандыру және цифрландыру дирекциясы»-ның диссертациялық жұмыстың нәтижелерін енгізу актісі (Қосымша А).

8. Hyukshin компаниясында ғылыми әзірлемелер нәтижелерін енгізу туралы анықтама (Оңтүстік Корея, Сеул қаласы) (Қосымша Б).

Барлық баяндамалар семинарларда, түрлі деңгейдегі конференцияларда және дөңгелек үстелдерде жасалды.

Нәтижелердің жариялынымдары. Диссертация материалдары бойынша 13 мақала, 5 жұмыс ҚР ККСОН МОН тізіміне енген басылымдарда, 7 жұмыс конференция материалдарында, симпозиумдарда, семинарларда, 1 мақала Scopus базасына кіретін журналда жарияланды.

Жұмыс көлемі мен құрылымы. Диссертация кіріспеден, 4 тарау және қорытындыдан тұрады. Диссертацияның толық көлемі: 104 бет, 43 сурет, 12 кесте. Әдебиеттер тізімі 118 атаудан тұрады.

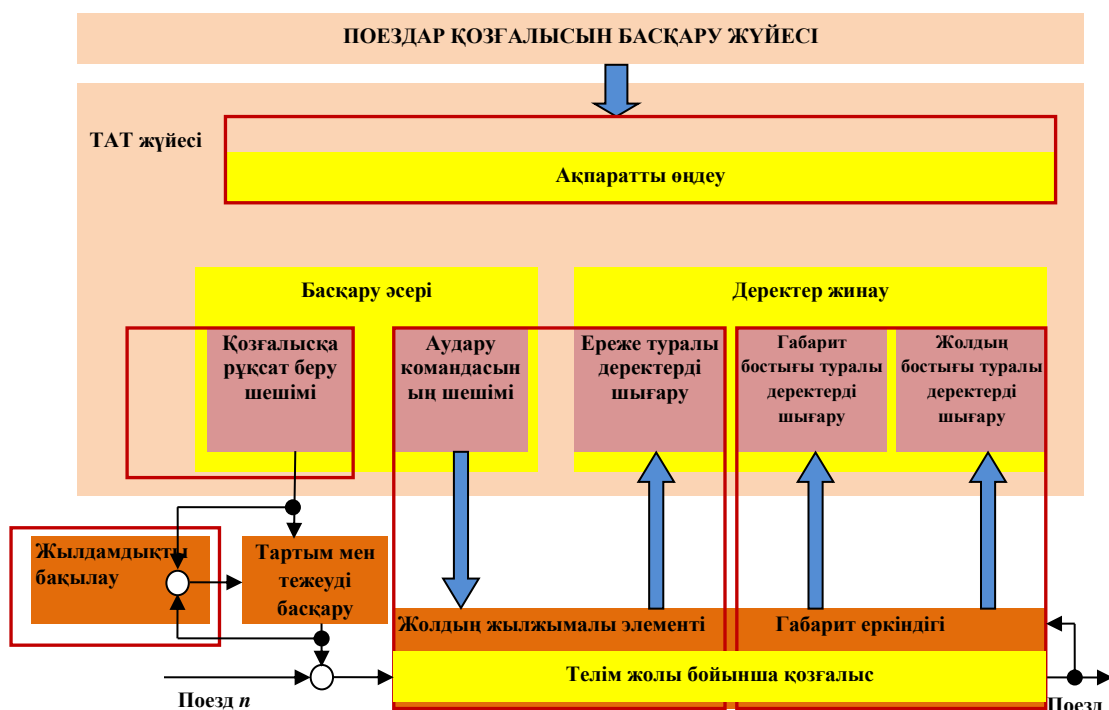
1 ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МАГИСТРАЛЬДІ ТЕМІРЖОЛ ЖЕЛІСІНДЕГІ ТАТЖ ҚАЗІРГІ ЖАҒДАЙЫН ТАЛДАУ ЖӘНЕ ЖАҢҒЫРТУ ҚАЖЕТТІЛІГІН НЕГІЗДЕУ

1.1 Теміржол автоматика және телемеханика үшін қауіпсіздікті қамтамасыз ету жүйелерінің негіздері және даму үрдістері

«Теміржол автоматика және телемеханика» түсінігі «автоматты және телемеханикалық басқару әдістерімен және құралдарымен пойыздар қозғалысын реттеу және қауіпсіздігін қамтамасыз ету тапсырмаларын орындайтын техника саласын» білдіреді [11, 12].

Бұл ретте «теміржол автоматика және телемеханика техникалық құралдарының негізгі элементтеріне белгі беру, орталықтандыру және блоктау (ББОБ) құрылымдары мен құрылғылары жатады, олардың құрамына жолдық блоктау, электр жезлдік жүйе, бұрмалар мен сигналдарды орталықтандыру, сұрыптау дөңестерінің автоматика және телемеханика құрылғылары, пойыздар қозғалысын автоматты реттеу, диспетчерлік орталықтандыру, пойыздар қозғалысын автоматты диспетчерлік бақылау және теміржол переездерінің бөгеу құрылғылары кіреді».

Темір жол автоматика (ТАТ) жүйесі ретінде түрлі объектілердің жағдайы мен жылдамдығы жөнінде ақпараттар, жолдың бостығы мен габарит туралы мәліметтер негізінде басқарушы әсерлер: аударуға бұйрық беру, қозғалысқа рұқсат ету, тартым мен тежеуді басқару және т.б. қабылданатын және жүзеге асырылатын басқару контуры түсіндіріледі (1.1 сурет) [13].



Сурет 1.1 – Темір жол автоматика және телемеханика жүйесіндегі басқару контуры [13, б. 8]

1.1 суретке байланысты, теміржол автоматика және телемеханика жүйесін одан да төмен деңгейлердің (ішкі жүйелердің) жиынтығы деп ұсынуға болады:

- жолдың бостығы мен пойыздың орналасқан жерін анықтау жүйелері (осьтер санағыштар, бақылау тетіктері және т.б.);
- темір жол мен жылжымалы құралдарда автоматты локомотивтік белгі беру (АЛС) мен жылдамдықты бақылауды қосқанда басқарушы әсерлерді (белгі беру) тарату жүйелері;
- орталықтандыру (басқарушы жүйені синхрондау және бұрыс басқару әсерлерін болдырмау) жүйесі;
- ақпарат жинау, қайта өңдеу және тарату жүйелері (коммуникациялар жүйесі);

Бұл сурет сондай-ақ темір жол автоматика және телемеханика (ТАТ) жүйелерінің пойыздар қозғалысын басқару жүйесімен өзара байланысын (негізі, ТАТ жүйелері пойыздар қозғалысын басқару жүйесі үшін ішкі жүйелер болып табылады) және осы жүйелердің мақсаттары, тапсырмалары және функциялары арасындағы өзара байланысты кескіндейді.

Жалпы теміржол автоматика және телемеханика (ТАТ) жүйелері көлік үрдістерін қауіпсіз басқаруды қамтамасыз ету қажет, яғни бастысы ақпарат жіберу мен өңдеудің қорғалған құралдары мен әдістерін пайдалану арқылы іске асырылатын қауіпсіздік аспектісі болып табылады [14].

Кеңістіктік құрылымда теміржол автоматика және телемеханика жүйесі мыналардан құралады:

- теміржол бекеттеріндегі автоматика және телемеханика жүйелері;
- аралықтардағы автоматика және телемеханика жүйелері;
- диспетчерлік орталықтандырудың автоматика және телемеханика жүйелері.

Сонымен бірге, теміржол автоматика және телемеханика жүйелерінің құрылымын темір жол көлігінде қалыптасқан функционалдық басқару құрылымы позициясынан алып қарауға болады (сурет 1.2). Бұл құрылым айтарлықтай деңгейде теміржол автоматика және телемеханика жүйелерінің ұйымдық және техникалық элементтерін және олардың арасындағы байланысты анықтайды.

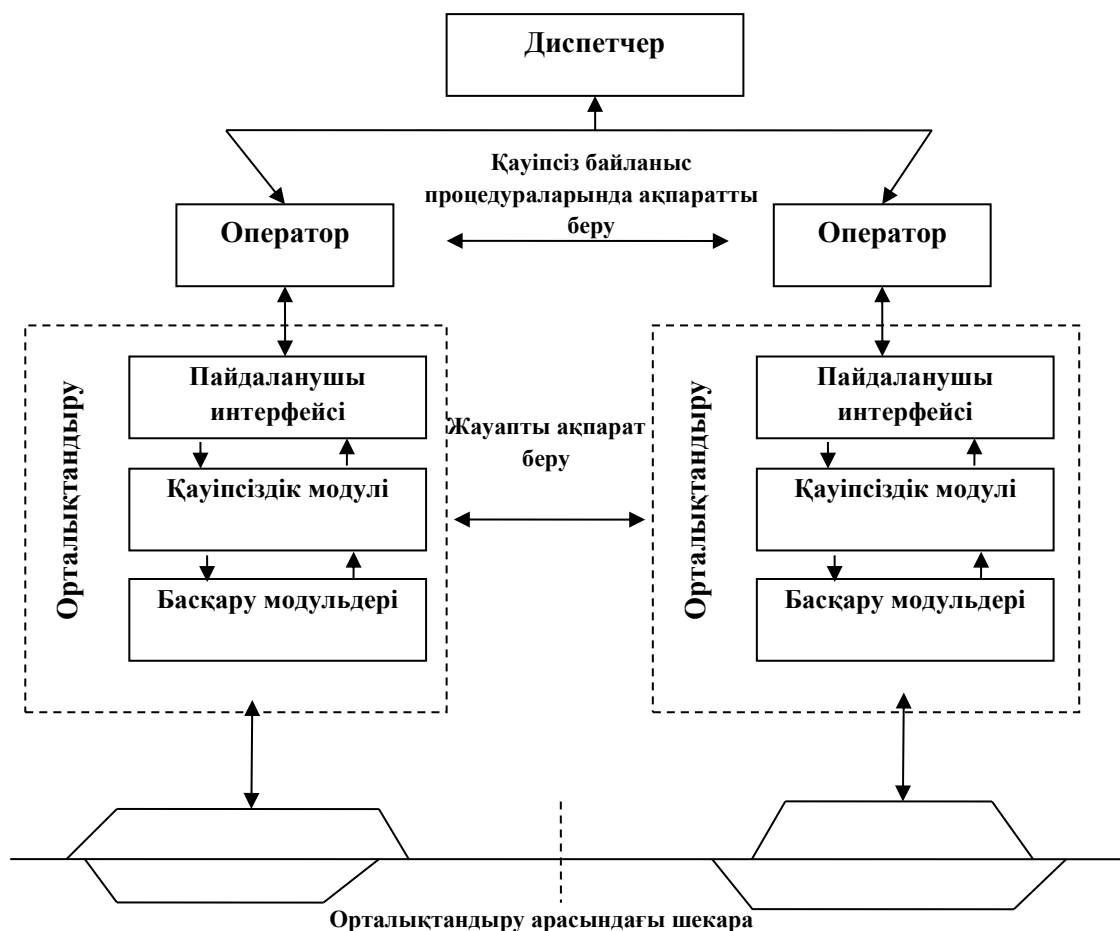
1.2 суретке сәйкес теміржол автоматика және телемеханика жүйелерінің келесі деңгейлерін атап өтуге болады:

негізгі жол құрылғылары:

- бұрмалар;
- сигналдар;
- жолдың бостығын бақылау құрылғылары;
- пойыз өткен кезде іске қосылатын құрылғылар (мысалы, пойыздың переезге жақындауын көрсететін тетіктер).

Жол құрылғылары жақын орталықтандыру посттарын басқару және бақылау тораптарымен байланысқан. Орталықтандыруды жол құрылғыларымен

үйлестіру деңгейінде ағымдағы пойыз жағдайына сәйкес жол құрылғыларын ауыстырып қосу және оларды бақылау жүргізіледі [13, б. 11].



Сурет 1.2 – Пойыздар қозғалысын басқару және қауіпсіздігін қамтамасыз ету жүйесінің функционалдық құрылымы [13, б. 11]

Бірінші деңгей – жедел басқару деңгейі («адам-машина» интерфейсі). Бұл сатыда оператор (кезекші, бұрмашы, сигналшы) рөлі жұмыс жасайды, ол пойыз қозғалысын дайындауға тікелей жұмылдырылған тұлға. Сонымен қатар, ол теміржол көлігінде пойыздар қозғалысын басқару үрдісінің талаптарына сәйкес жоспарлау алдындағы сатыда да іске қосылады. Бұл деңгейдегі оператор пойыздар қозғалыс кестесіне сай келетін құжаттарды (нұсқамаларды), сондай-ақ ағымдағы пойыз жағдайын есепке ала отырып, әрбір пойыз қозғалысы жүзеге асырылуы тиіс кестені негізге алып, міндетін атқарады. Осылайша, ол өзінің деңгейінде рұқсат етілген барлық басқару функцияларына ие болады.

Оператордың (кезекшінің) осы функцияларды орындаудағы қарапайымдылығы мен тиімділігі аса ерекшеленуі мүмкін. Басты түрде олар ақпарат жіберу және өңдеу үшін қолданылатын техникалық құрылғылардың даму деңгейіне, сондай-ақ ішінара орталықтандыру құрылғыларының пайдаланатын жүйесінің типіне байланысты.

Ағымдағы пойыз жағдайы жөнінде операторға (кезекшіге) хабарлауға қажетті ақпарат кескіндеудің пайдаланылатын стандарттары да қолданылатын жүйеге байланысты.

Екінші деңгей – орталықтандыру деңгейі. Бұл деңгей үшін Оператор қабылдаған шешімдерді келісу жолымен Оператор іс-әрекеттеріндегі/іс-әрекет реттілігіндегі қателіктерді болдырмайтын шешімдер мен құрылғылар (қауіпсіздік қамтамасыз ету модулі) негізгі болып табылады. Бұл деңгейде ТАТ жүйелерінің негізгі функциясы – пойыздар қозғалыс қауіпсіздігіне қауіп төндіру мүмкін оператордың ойдан тыс қателігін болдырмау.

Үшінші деңгей – диспетчерлік басқару деңгейі. Бұл деңгей Операторлардың (бекет кезекшілерінің) пойыздар қозғалысын басқаруды синхрондау үшін қажет. Диспетчерлік басқару деңгейі пойыздар қозғалысы барлық деңгейінің шоғырлануын қамтамасыз етеді және одан да жоғары деңгейдегі тапсырмаларды орындауға мүмкіндік береді. Осыған байланысты теміржол көлігіндегі басқару техникалық құралдары (диспетчерлік басқару орталықтары) диспетчерлік басқару деңгейінің жұмысын қолдап отырады. Егер орталықтандыру посттары диспетчерлік басқару орталықтарына қосылған жағдайда, жедел басқару деңгейінде Оператор қажет болмайды, себебі диспетчерлік басқару орталығында бір тұлға кезекшінің де, диспетчердің де жұмысын атқарады. Бұл құрылым аса тиімді болып саналады, бірақ ол басқару үрдістерін автоматтандырудың жоғары дәрежесін, техникалық құрылғылардың сәйкестігін және ақпарат қорғаудың сенімді тәсілдерін талап етеді [14, б. 12].

Теміржол автоматика және телемеханика жүйелері бірдей элементтерді құрайтындығына қарамастан, олардың құрылымы айтарлықтай дәрежеде бір-бірінен ерекшеленетін болады, бұл экономикалық, саяси және климатты-географиялық секілді макро орта факторларына байланысты темір жол қозғалыс ұйымдарының елеулі айырмашылықтарымен негізделеді.

Осылайша, теміржол автоматика және телемеханика жүйесінің негізгі және басты функциясы (мақсаты) қозғалыс толассыздығын, үздіксіздігін және қауіпсіздігін қамтамасыз ету, адам өмірі мен денсаулығын, жүк және теміржол инфрақұрылымын сақтау болып табылады. Бұл ретте заманауи даму сатысында пойыздар қозғалысын басқару жүйесімен аса терең бірігуі себепті теміржол автоматика жүйелерінің талап етілетін функцияларын кеңейту жүргізіледі.

1.2 Қазақстан Республикасы темір жолындағы автоматика және телемеханика жүйелерінің қазіргі жағдайын талдау

Магистральді желі телімдерінде жүк және жолаушы тасымалдаудың технологиялық үрдісінде көптеген мамандандырылған техникалық құралдар іске қосылған, бірақ әсіресе теміржол автоматика, телемеханика және телекоммуникация құралдары тасымалдау қауіпсіздігін қамтамасыз етеді және заманауи теміржол көлігіндегі инфрақұрылымның міндетті құрамдас бөліктерінің бірі болып табылады.

Қазақстан Республикасы теміржол саласының қазіргі күйі тұтынушылардың қызмет ассортиментіне, икемділігіне, сапасына,

жылдамдығына, сенімділігіне қоятын өсуші талаптары мен қызмет сипаттамаларына бәсекеге қабілетсіз рухани және физикалық көнерген технологиялар арасындағы тепе-теңсіздікпен сипатталады.

Қазақстан теміржол көлігінде кешенді техникалық алғаш қаруландыру 1975-1985 жылдары бұрынғы КСРО қатынас жолдары министрлігі басшылығымен жүргізілді. Қазіргі уақытта бұл теміржол көлігінің техникалық құралдары физикалық және рухани ескірген [15].

Қазақстан темір жолдарында ТАТ жүйелерінің дамуы 30-шы жылдардың соңында басталып, жүк қауырттылығының ұлғаюына орай XX ғасырдың 80-ші жылдарының соңына дейін өсті. Бұл сол кезде қажетті максималды өткізу қабілеттілігін, техникалық жылдамдықты және пойыздар қозғалыс қауіпсіздігін қамтамасыз етуге мүмкіндік берді.

Пойыздар қозғалысын басқарудың әрекет етуші жүйелерінің көпшілігі, атап айтқанда электрлік орталықтандыру, автоматты блоктау, диспетчерлік орталықтандыру XX ғасырдың 60-70-80-ші жылдары қолданысқа енгізілді. Бұл жүйелердің негізі релелік аппаратура болып табылады, ол осы аппаратураны ағымдық қамту және жөндеумен айналысатын жұмысшылардың елеулі штатын жинақтауға және қамтамасыздандыруға кететін эксплуатациялық шығындардың артуына әкелетін тұрақты жоспарлы-ескерту қызмет көрсетуін талап етеді [15, б.10].

«Қазақстан темір жолы» ұлттық компаниясы» акционерлік қоғамының» магистральді желісінде темір жол автоматика, телемеханика құрылғыларына 35 белгі беру және байланыс дистанциясы қызмет көрсетеді. Бұл ретте пойыздар қозғалысын, қозғалыс қауіпсіздігін басқаруды және бақылауды қамтамасыз ететін теміржол автоматика және телемеханика қызмет көрсетілетін жүйелерінің тізімі мынадай [16]:

- бұрмалар мен сигналдарды басқаруды электрлік орталықтандыру жүйелері (ЭО);
- пойыздар қозғалысын интервалды реттеу жүйелері (автоматты блоктау (АБ), жартылай автоматты блоктау (ЖАБ) және радиоблоктау (РБ));
- переездік белгі беруді автоматты басқару жүйелері (АПС);
- диспетчерлік орталықтандыру (ДО) және диспетчерлік бақылау (ДБ) жүйелері.

Әрі қарай 1.1 кестеде Қазақстан Республикасындағы ТАТ жүйесі құраушыларының негізгі сипаттамалары келтірілген [17].

Ұсынылған мәліметтер негізінде, Қазақстан темір жолы теміржол желісінің жалпы ұзындығы 15,8 мың км құрай отырып, мыналармен жабдықталған: пойыздар қозғалысын интервалды реттеу жүйелерімен – автоматты блоктаумен АБ – 11346 км (71,8 %), заманауи радиоблоктау жүйелерімен (ПҚИРЖ-Е) – 1629 км (11,5 %), жартылай автоматты блоктаумен ЖАБ – 2825 км (16,6 %). Диспетчерлік орталықтандырумен ДО 12057 км (76,3 %) жабдықталған. Бекеттерде электрлік орталықтандыруға 15817 бұрма (92 %) қосылған.

Кесте 1.1 – Қолданыстағы ТАТ жүйесінің қазіргі жағдайы

№	Техникалық құралдар атауы	Өлш. бірл.	Техникалық құралдардың жалпы қуаты	Пайдалануға берілген қуаттар (2000 ж. -дан кейін)	Пайдалануға берілген қуаттар (1980- 2000 ж.) мерзімі	37 жылдан астам пайдаланылатын қуаттар (1980 ж. -ға дейіг)
1	Автоматты блоктау	км.	11346	2681,5	5163,92	3501,5
2	Радиоблоктау	км	1629	1629	-	-
3	Жартылай автоматты блоктау (ЖАБ)	км.	2825	1327,47	832,62	664,9
4	Электрлік орталықтандыру ЭО (соның ішінде МПО, РПО)	бұрма	15817 (1216)	2076 (1216)	7888	5853
5	Негізгі байланыс	бұрма	412	25	146	241
6	Диспетчерлік орталықтандыру (соның ішінде МПДО)	км.	12057 (7702)	7702 МПДЦ	2435	1920
7	Дөңестік орталықтандыру	бұрма	361	43	208	110

Өзінің сапа деңгейі бойынша әрекет етуші ББОБ жүйелері Қазақстан Республикасы темір жолында тасымалдау үрдісін кешенді автоматтандырудың заманауи талаптарын қанағаттандырмайды, ақпараттық технологияларды жаппай енгізуді тежейді, оларға қызмет көрсету бойынша адамсыз технологиялар енгізуді қамтамасыз етпейді, орташа және жоғары деңгейдегі жүйелермен үйлесімділікті әрқашан қамтамасыз ете бермейді, сондай-ақ оларға қызмет көрсету және жөндеуге кететін эксплуатациялық шығындардың оңтайлы деңгейін қамтамасыз етпейді [18].

1.2.1 Электрлік орталықтандыру құрылғыларының қазіргі күйін талдау

Бұрмалар мен сигналдарды электрлік орталықтандыру (ЭО) – бұрмалар мен сигналдарды бекетте бір пунктен бекет кезекшісімен басқаруды қамтамасыз ететін автоматика және телемеханика құрылғыларының кешені [19].

Қазіргі уақытта ҚР теміржол желісінде әр жылда құрылған және шағын, орташа және ірі бекеттерді басқаруға арналған ЭО жүйелері пайдаланылады. Заманауи микропроцессорлық жүйемен (МПО) негізінен жаңа темір жол телімдерін салу кезіндегі бекеттер, кірме жолдардың жанасу бекеттері және ТЖ салдарынан қайта құрылған телімдердегі бекеттер жабдықталды.

Бүгінгі күні Қазақстан Республикасының магистральді теміржол желісі бойынша ЭО құрылғылары пайдаланылады, олар қондырылған [18, б. 18]:

- 1950-1970 жж. қазіргі кезде көнерген құрылғыны пайдаланумен (негізгі байланысы бар бекеттер бұрмалық орталықтандырғыштармен, аккумуляторлардан жергілікті қоректенетін және штепсельді емес типті реле базасында орындалған бекеттер қылталарында орналасқан құрылғысы бар бекеттер). Мұндай бекеттердің ЭО құрылғылары өндірістен шығарылған, немесе ауыстыру қорымен қамтамасыз ету мүмкіндігі жоқ;

- 1970-1980 жж. құрылғы мәліметтері бойынша қазіргі уақытта өзіндік диагностика жүйесін және қашықтан мониторингтеуді қосумен ішінара жаңғырту мүмкіндігі бар (қоректендіру панельдерін заманауи түріне, пульт

таблоларды ДСП, ШНЦ автоматтандырылған жұмыс орындарына, теру тобының релелік сұлбаларын микропроцессорлық түрге алмастыру);

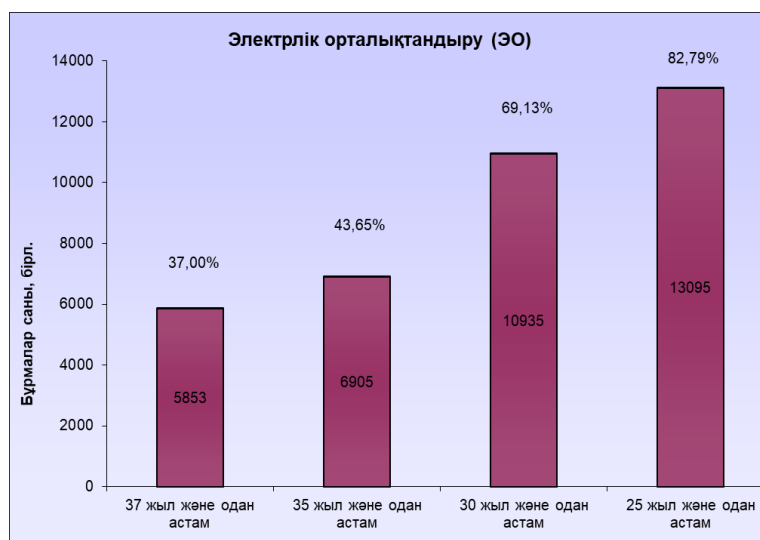
- 1980 ж. кейін бұл құрылғыларды олардың сұлбалық орындалуының ерекшеліктеріне байланысты толықтай жаңарту көзделеді (мысалы, Р80 «Alstom» электржетектері бар төрт сымдық бұрманы басқару сұлбасы бойынша сұлбалық шешімдер қарастырылмаған) [16, б. 5].

1.2 кесте мен 1.3 сурет мәліметтеріне сәйкес пайдалану мерзімі 25 жылдан астам бекеттерде орталықтандырылған бұрмалар үлесі 82,7% (немесе 13095) құрайды, шамамен 70% (10935) орталықтандырылған бұрмалар 30 жылдан астам пайдалану мерзіміне ие, 43,65% (6905) орталықтандырылған бұрмалар 35 жылдан астам пайдалану мерзіміне ие, шамамен 37% (5853) орталықтандырылған бұрмалар 37-40 жылдан астам пайдалану мерзіміне ие. Бұл ретте кейбір бекеттердің құрылғысы 50 жылдан астам уақыт пайдаланылады (өткен ғасырдың 50-60-шы жылдары қолданысқа енгізілген).

Кесте 1.2 – Магистральді теміржол желілеріндегі электрлік орталықтандыру жүйелерінің пайдалану мерзімдері

Электрлік орталықтандыру (ЭО) құрылғылары				
Енгізу жылы	1950-1980	1981-1982	1983-1987	1988-1992
ЭО бұрмасы	5853	1052	4030	2160

Пайдалану мерзімі	37 жыл және одан астам	35 жыл және одан астам	30 жыл және одан астам	25 жыл және одан астам
ЭО бұрмалары	5853	6905	10935	13095
% жалпы бұрма санынан.	37,0%	43,65%	69,13%	82,79%



Сурет 1.3 – Электрлік орталықтандыру жүйелерінің пайдалану мерзімдері бойынша диаграмма

Бекеттердің жалпы санынан 390 бекет пен разъездерде ЭО жүйелері 1980 жылға дейін, 250 бөлім пунктерінде – 1981-1990 жж. мерзімінде пайдалануға

берілген. Сол уақытта, микропроцессорлық жүйелер МПО үлесі айтарлықтай емес және 7,6 %-ды (1216 бұрма) құрайды.

Қазіргі уақытта 25 жылдан астам уақыт бұрын әзірленген, ЭО жүйелерінің дамуына орай бір уақытта енгізумен түрлі нұсқадағы электрлік орталықтандырудың (ЭО) релелік жүйелері қолданыста. Темір жол желісінде пайдаланылатын ЭО құрылғыларының ең кеңінен таралған типтері шағын бекеттерді релелік орталықтандыру құрылғылары және маршрутты-релелік орталықтандыру (МРО) болып табылады, олардың негізінде сенімділігі I класс релелері қолданылады. Оларды бірте-бірте жаңғырту теру тобын енгізу, құрылымды типтендіру, бұрмалар мен сигналдарды басқару жүйесін өзгерту, шағын өлшемді релелерді қолдану және т.б. жолдармен жүзеге асырылды [18, б. 20].

Жалпы ЭО жүйелерінің құрылғылары ҚР теміржолы желісінде келесі ерекшеліктермен сипатталады:

- «классикалық»-релелік жүйелердің жаппай басымдылығы;
- ЭО негізгі және ең кең таралған типтері шағын бекеттерді релелік орталықтандыру құрылғылары және ірі және орташа бекеттерді маршрутты-релелік орталықтандыру (МРО) болып табылады;
- релелік орталықтандыру құрылғылары сенімділігі I класс релелерін пайдалануға негізделген;
- ЭО жүйелері барлық бекеттерде жасалатын жобалардың ерекшелігімен, жолдық, жергілікті және пайдалану шарттарымен сипатталады [15].

1.2.2 Пойыздар қозғалысын интервалды реттеу жүйелерінің қазіргі күйін талдау

Пойыздар қозғалысын интервалды реттеу жүйесі (ПҚИРЖ) аралықтарда пойыздар қозғалысын бақылау және басқару үшін арналған, автоматты блоктау (АБ), жартылай автоматты блоктау (ЖАБ), радиоблоктау (РБ) жүйелерін құрайды.

ПҚИРЖ жабдықталған желі ұзындығы мынаны құрайды: автоматты блоктау АБ жүйесімен – 11346 км немесе 71,8%, заманауи радиоблоктау жүйелерімен (ПҚИРЖ-Е) – 1824 км немесе 11,5%, жартылай автоматты блоктау жүйесімен ЖАБ – 2630 км немесе 16,6% [18, б. 21].

Телімдерді АБ және ЖАБ жүйелерімен жабдықтау темір жол жаңа телімдерін құру немесе әрекет етуші телімдерін қайта құру кезінде 1960 жылдан 2000 жыл аралығында іске асырылды [16, б. 5].

Радиоблоктау жүйесімен негізінен 2011-ден 2017-жыл аралығында пайдалануға енгізілген темір жолдың жаңа телімдері (1824 км) жабдықталған.

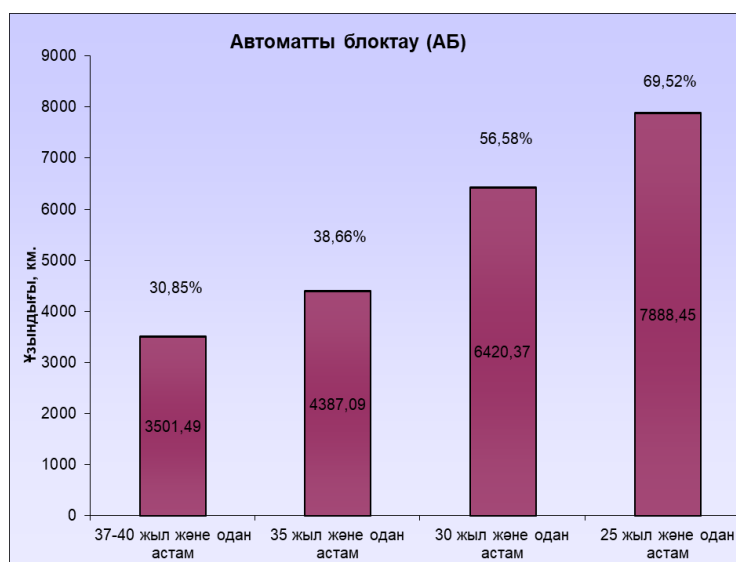
1.3 кесте мен 1.4 суретте келтірілген мәліметтерге сәйкес пайдалану мерзімі 25 жылдан астам автоматты блоктау АБ жүйелерімен 7888,4 км немесе 69,5% жабдықталған. Соның ішінде, 6420 км немесе 56,58% пайдалану мерзімі 30 жылдан астам АБ жүйелерімен, 35 жыл аса сыни деңгейдегі пайдалану мерзімі бар жүйе – 4 387 км или 38,6% жабдықталған. Пайдалану мерзімі 40 жылдан астам АБ жүйелеріне ұзындығы 3501 км немесе 30,85% телім тиесілі.

Бұл ретте кейбір телімдерде АБ жүйелері 50 жылдан астам уақыт пайдаланылады (өткен ғасырдың 60-шы жылдарында пайдалануға берілген).

Кесте 1.3 – Магистральді теміржол желілеріндегі пойыздар қозғалын интервалды реттеу жүйелерінің пайдалану мерзімдері

Автоматты блоктау құрылғылары (АБ)				
Енгізу жылы	1950-1980	1981-1982	1983-1987	1988-1992
км АБ	3501,492	885,6	2033,28	1468,08

Пайдалану мерзімі	37-40 жыл және одан астам	35 жыл және одан астам	30 жыл және одан астам	25 жыл және одан астам
Ұзындығы (км)	3501,492	4387,092	6420,372	7888,452
% АБ жалпы ұзындығының (11346 км)	30,85%	38,66%	56,58%	69,52%



Сурет 1.4 – Пойыздар қозғалын интервалды реттеу жүйелерінің пайдалану мерзімдері диаграммасы

Жалпы пойыздар қозғалысын интервалды реттеу жүйелерінің құрылғылары ҚР темір жолы желісінде келесі ерекшеліктермен сипатталады:

- АБ жүйесімен жабдықталған телімдердің шамамен 40%-ы сыни тозуға ие және ауыстыруды қажет етеді;
- ЖАБ жүйесімен жабдықталған телімдер (келешекті даму көзделмеген аз әрекетті телімдерді санамағанда) таңдаулы жаңғыртуды талап етеді;
- радиоблоктау жүйесімен жабдықталған телімдердің шағын бөлігі тасымалдау үрдісін кешенді автоматтандыруды енгізу кезінде тежеуші фактор болып табылады.

1.2.3 Диспетчерлік орталықтандыру құрылғыларының қазіргі күйін талдау

Диспетчерлік орталықтандыру пойыз диспетчерінің ДНЦ

автоматтандырылған жұмыс орнында кескіндеу арқылы бекеттегі бұрмалар мен сигналдарды басқару және бақылауды, аралықтардың, бекет жолдарының және оған жанасқан блок-телімдердің бос еместігін және бастығын бақылауды қамтамасыз етеді. Диспетчерлік орталықтандыру кезінде пойыздарды қабылдау, жөнелту, маневрлер жүргізу бойынша бекеттерде бұрмалар мен сигналдарды қосымша басқару мүмкіндігі бар [20].

Диспетчерлік орталықтандыру жолды жаңартуға қосымша шығынсыз телімдік жылдамдықтың артуының арқасында өткізу қабілеттілігін жоғарылатуға және пойыздар қозғалысын жылдамдатуға мүмкіндік береді.

Қазіргі уақытта диспетчерлік орталықтандырумен жабдықталған желінің ұзындығы ҚР темір жолы жалпы пайдаланылатын ұзындығының 11 233,447 км немесе 76,3%-ын құрайды.

ДО ең алғашқы жүйелерінің (ДО – ДВКЗ) бірі 1950 жылы Шиелі – Қазалы телімінде қолданысқа енгізілді. 1955 ж. бастап ДВК жүйесінің орнына теміржол желісінде полярлық-жиілікті және жиілікті диспетчерлік орталықтандыруды (ПЖДО, ЖДО) қолдана бастады, онда ТБ сигналдары полярлық, ал ТС сигналдары – жиіліктік импульстермен таратылды. Бұл жүйе қазіргі уақытта Қазақстан Республикасының темір жол желісінде, соның ішінде Алматы – Ақтоғай, Мақат – Қандыағаш, Шорнақ – Қазалы телімінде (1275,5 км) пайдаланылады [18, б. 24].

1967 ж. бастап объектілер күйін циклдік бақылайтын «Нева» типті жүйе енгізілді. Мұндай типті жүйемен 2759,5 км темір жол жабдықталған. Бұл жүйеде шамамен 1300 объектіні бақылау циклінің ұзақтығы 5 с құрайды, ол бекетті желілік қосу кезінде де, радиалды сұлба кезінде де дуплекстік режимде жұмыс жасайды. Бұл ретте бір және екі жақты басқару мүмкін болады, ол ДО жұмысының сенімділігін айтарлықтай арттырады.

«Нева» жүйесінің негізінде «Луч» жүйесі құрылды және алғаш 1977-1978 ж.ж. Белоруссия жолының телімдерінің бірінде қолданылды. Ол аралық бекеттерде тек пойыздық емес, сонымен бірге маневрлік жұмысты басқаруға, жауапты бұйрықтар жіберуге, атап айтқанда бір жолдық аралықта қозғалыс бағытын өзгертуге мүмкіндік берді. Бұл жүйе сондай-ақ Қазақстан темір жолында ұзындығы 320 км телімдерде пайдаланылады.

XX ғасырда құрылған барлық диспетчерлік орталықтандыру жүйелері жақсы сипаттамаға ие болды, алайда жоғары технологиялар мен адам өмірінің барлық саласын жаһандық компьютерлеудің келуімен бұл жүйелер рухани, техникалық және физикалық көнерді.

2000-шы жылдардан кейін ҚР 7702 км темір жолына микропроцессорлық диспетчерлік орталықтандыруды (МПДО «НЕМАН», «Диалог», «АСДО», «Ebilock») енгізу микроэлектрониканың және есептеуіш техниканың заманауи құралдарын қолдану есебінен, пойыздар қозғалысын басқару тиімділігін арттыруды қамтамасыз етуге мүмкіндік берді, сондай-ақ диспетчерлік посттарды ірі автоматтандырылған диспетчерлік басқару орталықтарына біріктіруге, сонымен бірге Астана қаласында бірыңғай диспетчерлік басқару орталығын құру мүмкіндігін берді [15, б. 17].

1.4 кесте мен 1.5 сурет мәліметтері бойынша МПДО заманауи жүйелердің үлесі ДО жалпы пайдаланылатын көлемінің 63,8%-ын (7702 км), ЖДО, ПЖДО, ДВК – 1275,5 км (10,5%), ДО НЕВА, Луч – 3079,5 км (25,5%) құрайды [16, б. 6].

Алайда кейбір жол телімдерінде, соның ішінде халықаралық көлік дәліздерінің құраушыларында диспетчерлік орталықтандыру жоқ. Бұл ұзындығы 76 км Шымкент – Арыс және 436 км Атбасар – Есіл – Тобыл телімдері. Сонымен қатар, Ақтоғай – Шар – Семей телімдерінде желілік пунктер «НЕВА» жүйесімен, ал орталық пост МП «Диалог» микропроцессорлық жүйесімен жабдықталған.

Кесте 1.4 – Магистральді теміржол желілеріндегі диспетчерлік орталықтандыру жүйелерінің пайдалану мерзімдері

Пайдалану мерзімі	МПДО	ДО «НЕВА», «Луч»	ЖДО, ПЖДО, ДВК
Енгізу жылы	2000 жылдардан	1970 – 1985	1950 – 1970
Ұзындығы (км)	7702 км	3079,5	1275,5
% ДО жалпы ұзындығының (12057км)	63,8%	25,5%	10,5%



Сурет 1.5 – Диспетчерлік орталықтандыру жүйелерінің пайдалану мерзімдері диаграммасы

Жалпы диспетчерлік орталықтандыру жүйелерінің құрылғылары ҚР темір жолы желісінде келесі ерекшеліктермен сипатталады:

- телімдердің шамамен 64%-ы заманауи микропроцессорлық диспетчерлік орталықтандыру жүйесімен жабдықталған;
- ұзындығы 512 км телімдерде диспетчерлік орталықтандыру жүйесі жоқ;
- үлесі шамамен 36%-ды құрайтын телімдерде техникалық және рухани ескірген диспетчерлік орталықтандыру құрылғылары пайдаланылады.

1.3 ҚР-да ТАТ әрекет етуші жүйелерін жаңғыртудың жүзеге асырылмауы жағдайындағы қауіптерді талдау

Талдау 1990 ж. дейін енгізілген ББОБ пайдаланылатын құралдары ұзақ қызмет ету мерзіміне, жоғары тозу деңгейіне ие екендігін, өзінің сапалық

деңгейі бойынша тасымалдау үрдісін кешенді автоматтандырудың заманауи талаптарын қанағаттандырмайтындығын, сондай-ақ ақпараттық технологияларды, соның ішінде аз қызмет көрсетілетін технологияларды жаппай енгізуді тежейтіндігін көрсетті.

Теміржол көлігі елдегі барлық көлік инфрақұрылымының негізі болып табылады. Оның тиімді жұмыс атқаруы жаңғырту, жаңа инновациялық даму жолына көшу және ұлттық экономиканың орнықты өсуі үшін жағдай жасауда айырықша рөл ойнайды, сондай-ақ өзгеруші әлемдік экономикалық жүйеде көшбасшылықты қамтамасыз етуге жағдай жасауға ықпал етеді [21]. Теміржол көлігінің күйі мен жұмыс сапасына оның әрі қарай қоғамдық-экономикалық дамуының келешегі ғана емес, сонымен бірге мемлекеттің келесі маңызды функцияларды тиімді орындау мүмкіншіліктері байланысты:

- ұлттық егемендікті және ел қауіпсіздігін қорғау;
- экономикалық кеңістік бірлігін нығайту;
- азаматтардың тасымалдау қажеттілігіне ие болуын қамтамасыз ету;
- аймақтардың қоғамдық-экономикалық дамуын туралау үшін жағдай жасау;
- ресурстық тәуелсіздікті және жаһандық бәсекеге қабілеттілікті арттыру.

ТАТ құрылғыларының жаңғыртылуының жүзеге асырылмауы жағдайында техникалық, экономикалық және саяси деп бөлінетін қауіптерді атап өтуге болады.

Техникалық қауіптер. ТАТ әрекет етуші жүйелерін жаңғыртудың жүзеге асырылмауы жағдайында олардың созылмалы көнеруінде, ТАТ инфрақұрылым объектілерінің «шекті жағдайға» жетуінде байқалады. Бұнымен қатар әрекет етуші құрылғыларда (НР, НШ және т.б. топ релелері) қолданылатын ескірген жабдықты өндірістен шығару қосалқы бөлшектерді ауыстыруға мүмкіндік бермейді. Қауіпсіздікті қамтамасыз ететін құрылғыны өзара жалғауды жүзеге асыратын сымдар мен кабельдердің жиі істен шығуы (жарылу және окшаулаудың бұзылуы). Окшаулаудың жоғалуы сымдар мен кабельдердің өртенуіне, және артынша, бастапқыда газ өрту сөндіру қарастырылмаған ЭО постында өртке әкеліп соғуы мүмкін. «Белгіленген қызмет ету мерзімін (кеден Одағының техникалық регламенті) – өнімді пайдаланудың күнтізбелік ұзақтығын орындамау, ол мерзімге жеткен кезде техникалық күйіне қарамастан өнімді пайдалану тоқтатылу қажет». Техникалық қауіптер дәрежесінің өсуі эксплуатациялық шығындардың артуына, пойыздар қозғалыс қауіпсіздігінің төмендеуіне және жиі кідіруіне әкеп соғады. Сонымен қатар, жылдан жылға автоматика объектілерінің көбі ішінара жаңғырту мүмкін болмайтын «шекті жағдайға» жетіп жатыр [18, б. 49].

Техникалық қауіптерге сонымен бірге ТАТ құрылғыларын толық «цифрландыру» және диагностикалау қамтамасыз етілмеуін жатқызуға болады.

Экономикалық қауіптер. Қазақстан ежелгі Жібек жолы маршрутының ортасында орналасқан. Сауда ОААЭЫ (ЦАРЭС) халқы аз және ірі ресурстарға ие елдері үшін өмірлік маңызды. Ішкі аймақтық секілді аймақаралық сауда да егер шағын жерлер, тасымалдау мен жеткізу тізбектерінің мәселесі шешілсе,

жоғары даму әлеуетіне ие болады. Ежелгі Ұлы Жібек жолы уақытынан бері ішкі аймақтық және аймақаралық сауда аймақтағы елдер экономикасына қомақты үлес әкеледі, бұл ретте халықаралық сауданың елеулі бөлігі теміржол көлігі жүйелерінің ынтымақтастығы мен аса тығыз бірігуін талап ете отырып, көптеген көрші елдердің аумағы арқылы жер тасымалдарына байланысты болады. Қазіргі уақытта Қазақстан Республикасы мен ҚХР-да бірнеше жылдар бойы ынтымақтастық пен бірігуді кеңейту жұмыстары жүргізілуде. Мұның нәтижесі жылдам контейнерлік пойыздардың арқасында ҚР арқылы транзитпен ҚХР-нан жүк тасымалының еселеп артуы болды. Жүк тасымалының бұл түрі үлестік құны жоғары сауда ағындары үшін теңіз және әуе көлігімен салыстырғанда аса бәсеке қабілетті болып келеді [4, б. 7].

ТАТ әрекет етуші жүйелерін жаңарту жүзеге асырылмаған жағдайда транзиттік дәліздерге кіретін теміржол телімдерінің өткізу және тасымалдау қабілеттілігі қамтамасыз етілмеу мәселесі туындайды. Бұл жоғары талаптар қойылатын тасымалдау үрдісінің сапасына кері әсерін тигізеді, және соның салдарынан Қазақстан Республикасының теміржол дәліздері арқылы транзиттік ағындарға шектеу қойылады. Сонымен қатар, ТАТ жүйелерін жаңартусыз жиі істен шығу әсерінен жыл сайын теміржол инфрақұрылымы жүк жеткізудің талап етілетін мерзімін қамтамасыз ете алмайды және артынша теміржол көлігінің бәсекеге қабілеттілігі төмендейді.

Саяси қауіптер жаңғырту жүзеге асырылмаған жағдайда телімдердің өткізу қабілеттілігінің көрсеткіштері Үкіметтің бірқатар қаулысын және Қазақстан Республикасы Президентінің қойған тапсырмаларын іске асыруға мүмкіндік бермейді.

Қазақстан Республикасының ұзақ мерзімде дамуының стратегиялық бағыттарында өнімділікті арттыру, жаңа даму саясатын қалыптастыру, инновациялық жүйе құру, инфрақұрылымды жаңғырту және энергия тиімділігін жоғарылату арқылы ғылымды қажет ететін экономика құруды қолдайтын жеделдетілген инфрақұрылым қалыптастыруға нұсқау берілген. Сандық технологияны пайдалану есебінен Қазақстан Республикасы экономикасының даму қарқынын жылдамдату және халықтың өмір сүру сапасын жақсарту, сондай-ақ Қазақстан экономикасының болашақта сандық экономика құруды қамтамасыз ететін принципіалды жаңа даму траекториясына көшу үшін жағдай жасау орташа мерзімді келешектің жоспарында. Ұзақ мерзімді келешекте жоғарыда айтылғандарды іске асыру үшін 12.12.2017 жылы № 827 ҚР Үкіметі қаулысымен бекітілген «Цифрлық Қазақстан» Мемлекеттік бағдарламасы әзірленді. Бұл ретте ТАТ құрылғыларын жаңғырту болмаған жағдайда темір жол ірі инфрақұрылымын ескере отырып, «Цифрлық Қазақстан» бағдарламасын іске асыру мүмкін емес.

Сонымен қатар Қазақстан темір жолында ТАТ құрылғыларын елеулі жаңартусыз «2050 жылға қарай Қазақстанның әлемнің 30 ең бәсекеге қабілетті елдері қатарына кіру бойынша «Қазақстан-2050» стратегиясы» да жүзеге асырыла алмайды, себебі ескірген жүйелер басқа дамыған елдерде қолданылатын ТАТ сандық микропроцессорлық жүйелеріне бәсекелестік жасай

алмайды [22].

«ҚТЖ» ҰҚ» АҚ мәліметтеріне сәйкес ТАТ инфрақұрылымы басқаларымен (жол, түйіспелі торап, локомотив шаруашылығы және т.б.) салыстырғанда ұзақ қызмет ету мерзіміне ие және іс жүзінде жаңартылмады. ТАТ жаңа және заманауи құрылғыларының үлесі елеусіз, олар жоспарлы жаңғырту есебінен емес, жаңа желілер құрылысы кезінде пайдалануға берілді.

Осы тарауда жүргізілген талдау негізінде ТАТ құралдарының жалпы жағдайы қауіпті күйге жақын деп қорытындылауға болады. Пойыздар қозғалысының қауіпсіздігін және басқаруды тікелей қамтамасыз ететін ТАТ негізгі құрылғыларының 70%-дан астамы ұзақ қызмет ету мерзімімен қолданылады. Егер жақын арада ББОБ қазіргі жүйелерімен жабдықталған теміржол телімдерін қайта құру және жаңғырту шаралары жасалмаса, онда 2025 жылға таман бұл цифр 80%-дан асып кетуі әбден ықтимал.

ББОБ құрылғыларының тозу және қызмет ету мерзімдері мәселелерін талдай отырып, объективті түрде республикада ішкі және сыртқы тасымалды оңтайландырушы жаңа теміржол желілерін құру жөнінде кең көлемді жұмыс атқарылғандығын атап өтпеуге болмайды. Бұл ретте, қазіргі темір жол ТАТ құрылғыларын ауыстыру және жаңғырту сұрағы тиісті түрде қарастырылмады, яғни ТАТ жүйелерінің инфрақұрылымы негізінен кеңестік кезеңде құрылған әлеуетпен жұмыс істейді.

Қызмет ету мерзімі ұзақ құрылғылардың үлкен көлемі, ескі релелік аппаратураны жаңа түрге ауыстырудағы жоғары қажеттілік, диагностика құралдарының жоқтығы оларды күтіп ұстауға кететін эксплуатациялық шығындардың өсуіне әкеледі. Олардың істен шығу қаупі жылдан жылға жоғарылайды. Релелік жүйелерді пайдалану тасымалдау үрдісін автоматтандырудың заманауи деңгейін, автоматтандырылған жүйелердің жұмысын диагностикалау және мониторингтеуді қамтамасыз етуге мүмкіндік бермейді. Өндірістен шығарылған бірқатар релелік элементтік базаның нормативті апаттық-қалпына келтіру қорының жоқтығы және оны қалпына келтіру мүмкін еместігі теміржол көлігі қызметінің толық тоқтау қаупінің елеулі факторы болып табылады.

ТАТ техникалық құралдарының қазіргі құрылымы мен жағдайы теміржол көлігін дамыту бойынша тапсырмалар орындау кезінде тежеуші фактор болып саналады. Сондықтан соңғы жылдары сервистік орталықтар құрумен бірге көпдеңгейлі қауіпсіздік жүйесі мен бірыңғай автоматтандырылған басқару жүйесін қалыптастыру негіздері секілді біріккен жүйе құру, ТАТ техникалық құралдарын қашықтан мониторингтеуді ұйымдастыру және тұрақты әкімшілеу тапсырмаларына толыққанды жауап беретін ТАТ заманауи микропроцессорлық жүйелерін енгізу қажеттілігі туындады.

Заманауи жүйелердің сипаттамасы өзіндік диагностикалау, аппаратураны қазіргі бөлмелерде орналастыруға мүмкіндік беретін кез-келген аппараттық-бағдарламалық кешендермен біріктіру функцияларының болуы болып табылады. Бұл ретте бір уақытта жоғары кернеу көздерінен қорғау сұрақтарын шешу арқылы талшықты-оптикалық кабель пайдалану жолымен құрылғыны

орталықсыздандырылған орналастыру кезінде материалдарды үнемдеу байқалады. Сонымен қатар бұрмалар мен сигналдарды түйіспесіз басқару, аз қызмет көрсетілетін технологияларды максималды пайдалану сұрақтарын орындау эксплуатациялық шығындарды айтарлықтай қысқартуға және теміржол көлігінің бәсекеге қабілеттілігін арттыруға мүмкіндік береді.

ТАТ құрылғыларын жаңғырту, жалпы теміржол көлігі секілді келесі тапсырмаларды орындауға көзделген:

- жүк және жолаушыларды максималды жұмылдыру, көлік қамтамасыз ету тиімділігін арттыру есебінен қосымша тасымалдау көлемін тарттыру;
- тасымалдау үрдісін тиімді басқару үшін ақпараттық қамтамасыз етуді дамыту;
- ресурс үнемдеу технологияларын енгізу;
- эксплуатациялық жұмыстардың қауіпсіздігін, сенімділігін, тазалығын және үздіксіздігін арттыру.

Халықаралық және ел ішіндегі көлік дәліздерінің қауіпсіздігі мен сенімділігі орнықты экономикалық дамуды және қоғамның жолаушы тасымалдау, тауар айналу қажеттілігін, елдегі көлік жүйесінің бәсекеге қабілеттілігін арттыруды қамтамасыз етуге мүмкіндік береді.

Сонымен қатар, ТАТЖ жаңғырту вагондар, локомотивтер айналымын қысқартуға, бекетте маневрлік локомотивтердің жұмыс істеуін азайтуға әсер етеді. Жолаушы қозғалысында пойыздардың жүру жылдамдығын тура телімдерде 200 км/сағатқа дейін арттыруға мүмкіндік береді, бұл ұлттық масштабта шеткі нүктелер арасында 12 сағаттан аспайтын жолда жүру уақытын қамтамасыз ету есебінен Қазақстан Республикасы халқының орнықтылығын жоғарылатуға мүмкіндік береді.

Алайда бұл ретте Қазақстан Республикасының темір жолында ТАТ жүйелерін жаңғырту кезінде тежеуші факторлар болып табылатын мәселелер бар:

- Қазақстан Республикасының аумағында теміржол көлігі саласында жүйелерді өңдеп шығару, оларды сертификаттау бойынша мамандандырылған ұйымдар жоқ;
- жүйелер мен құрылғыны дайындаушы отандық зауыттардың жоқтығы, бұл шетелдік өндірушілерге (соның ішінде валюта бағамына) тәуелді болуға әкеледі;
- енгізілетін микропроцессорлық жүйелер сервистік қызмет көрсетуді талап етеді. Өздігінен сервистік қызмет көрсету орындауға қабілетті штаттың жоқтығынан, басқа ұйымдарды жұмылдыру қажет болады.

2 ПОЙЫЗДАР ҚОЗҒАЛЫСЫН БАСҚАРУДАҒЫ ҰЛТТЫҚ ЖҮЙЕНІҢ ҚҰРЫЛУЫ МЕН KTCS ЖҮЙЕСІНДЕ ҚОЛДАНЫЛАТЫН РАДИОКАНАЛДА АҚПАРАТТЫ ҚОРҒАУ ӘДІСТЕРІ

2.1 Қазақстандық пойыздар қозғалысын интервалды реттеу ұлттық жүйесінің архитектурасы мен жүйенің негізгі элементтері

Теміржол – бұл үлкен және күрделі жүйе. Ол бірнеше жылдар бойы бірте-бірте құрастырылады, кеңейтіледі және жаңартылады. Жаңа технологиялар жаңа және жаңғыртылған темір жол желілеріне енгізілген уақытта, ескі түрлері басқа телімдерде қолданылуын жалғастырады. Сондықтан теміржол технологияларының қызмет ету мерзімі әдетте онжылдықпен есептеледі. Темір жолдың мұндай технологиялық алуын түрлілігі сол мемлекеттің ерекше стандарттарына сәйкес артады. Дәстүрлі түрде әр ел белгілі бір дәрежеде көрші темір жолмен салыстырғанда басқаша болып келген өздерінің жеке ұлттық жүйелерін жасап шығарды. Осы себепті Қазақстан темір жолының технологиялық ландшафты әдетте көптеген үйлесімсіз жүйелер мен стандарттардан тұрады. Бұл электрлендіру, платформа жолтабанына, биіктігіне және басқа да көптеген заттарға қатысты. Бірақ бұл әр түрлілік автоматика, телемеханика және байланыс темір жол технологияларында ерекше байқалады.

Бұл технологиялық әр түрлілік пойыздардың трансшекаралық трафигі үшін негізгі кедергі болып табылады. Әсіресе бұл мәселе пойыздарды басқарудың 20-дан астам жүйесі пайдаланылатын [23, 24, 25] көлік дәлізінің телімдерінде байқалады, бұл ретте жүйелер жиі өте ұқсас белгілер мен функционалдылыққа ие болады. Алайда, олар үйлесімсіз болғандықтан, трансшекаралық пойыздарды пайдалану негізсіз күрделі және экономикалық тиімсіз. Локомотивтер топтық басқару мен байланыстың бірнеше жүйелерімен жарақтандырылуы тиіс, бұл экономикалық және эксплуатациялық шығындарға әкеледі. Мысалы, бұл қосымша басқару жүйелері локомотивте орнату үшін қосымша орынды қажет етеді, ал онда барлық орын шектеулі. Сонымен бірге олар локомотив бағасын айтарлықтай жоғарылатады (басқару жүйелері локомотив бағасының 25%-ын құрауы мүмкін), сондай-ақ жүйенің түрлі типтерін басқаратын локомотив бригадалары үшін қосымша біліктілік қажет болады [26].

Халықаралық тасымалдау көлемінің артуына байланысты біздің елде де координаталық басқару принципіне негізделген жүйелер құру қажеттілігі туындайды. Дәл сол себепті «ҚТЖ» ҰҚ» АҚ-ның автоматтандыру және цифрландыру дирекциясының мамандарымен бірге Қазақстандық пойыздар қозғалысын басқарудың KTCS (Kazakhstan Train Control Systems) ұлттық жүйесін алғаш әзірледік [25, б. 15].

Барлық әлемде интервалды реттеу жүйелерін дамытудың негізгі үрдісі аралықты блок-телімге бөлуге негізделген (fixed blocks signalling systems) дәстүрлі автоматика жүйелерінен (traditional signalling systems) координаталық интервалды реттеу принципіне негізделген жүйелерге көшу әрекеттері болып табылады [27, 28]. Дәстүрлі автоматика жүйелерінде пойыз алдыңғы пойыз

блок-телімнен шықпайынша, оған кіре алмайды. Шетел ғалымдарының ойынша, мұндай жүйеге икемділік жетіспейді [29, 30], себебі жылдамдыққа қарамастан барлық пойыз үшін блок-телімнің өлшемі бірдей. Осылайша, жүрдек пойыздар үшін қажетті блок-телімнің ұзындығы жылдамдығы төмен пойыздар үшін де қолданылады, бұл телімнің өткізу қабілеттілігін әлбетте төмендетеді [31].

Өткізу қабілеттілігін арттыру және қозғалыс қауіпсіздігін қамтамасыз ету тапсырмаларын орындау үшін ағылшын тілі әдебиетінде moving block signalling system (сөзбе-сөз «жылжымалы» блоктары бар жүйе деп аударуға болады, сонымен бірге Communications Based Train Control (ақпарат таратуға негізделген пойызды бақылау) атауы жиі пайдаланылады) деп аталатын координаталық интервалды реттеу принципіне негізделген жүйелер әзірленді.

Қазақстандық пойыздар қозғалысын басқару жүйесі (KTCS) [25, б. 15] Еуропалық теміржол қозғалысын басқару жүйесінің (ERTMS) аналогы болып табылады – бұл Еуропалық пойыздар қозғалысын басқару жүйесі (ETCS) [32] мен GSM-R құралған келесі кезеңді пойыздар қозғалысын басқару және белгі беру еуропалық стандарты [33].

Еуропалық теміржол қозғалысын басқару жүйесі (ERTMS) жерде пойыздарды басқару және пойыздар арасындағы байланыс үшін алғашқы халықаралық стандарт болып табылады. 1980-ші жылдардың соңында еуропалық елдер теміржол нарығын сегменттеу теміржол көлігін болашақта дамыту үшін елеулі мәселеге айналып бара жатқандығын ұғынды [23, б. 31]. Үйлесімділіктің болмауы трансшекаралық орын ауыстырусыз артықшылығы толықтай іске асырыла алмайтын жоғары жылдамдықты темір жолдар үшін ерекше мәселе туындатты. Осыған байланысты еуропалық теміржол өнеркәсібі үшін бірыңғай стандарт енгізілді.

ERTMS бастапқыда ЕС-де еуропа континентінде теміржол жүйелерін жалғау үшін әзірленді. ЕС Еуропалық кеңес нұсқаулары [34] мен Еуропалық комиссия шешімдері [35] арқылы еуропалық темір жолдарға ERTMS құруды міндеттеді [23, б. 31]. Алайда бұл жүйенің артықшылығы оны басқа елдерде енгізу үшін көрнекті етті. Еуропадан тыс ERTMS мына елдерде пайдаланылады немесе пайдалануға жоспарланған: Алжир, Аргентина, Аустралия, Бразилия, Қытай, Египет, Үндістан, Индонезия, Қазақстан, Ливия, Малайзия, Мексика, Марокко, Жаңа Зеландия, Ресей, Сауд Арабиясы, Оңтүстік Корея, Тайван, Түркия және Біріккен Араб Әмірлігі [36]. Осылайша, ERTMS бірте-бірте барлық әлем елдерінің кең қолдауымен еуропалық стандарттан жаһандық стандартқа айналып барады [37].

Технология жасау кезінде кешенді тәсіл қолданылды, онда техникалық шешімді таңдаумен қатар әлем стандарттарына сай болу, бірнеше мәрте сынақтан өткізу және отандық жағдайларға бейімдеу толығымен пысықталды.

«KTCS» жүйесін әзірлеу кезінде негізін қалаушы құжаттар EN 50126 [38], EN 50128 [39], EN 50129 [40], IEC 61508 [41] халықаралық қауіпсіздік қамтамасыз ету стандарттары болып табылады. SIL4 жүйесінің мәлімделген

қауіпсіздік деңгейі аталған стандарттардың ең жоғарғы талабы болып саналады, ол 10^{-9} істен шығу ықтималдылығына сәйкес келеді [42].

Жылжымалы құрамға орнатылатын барлық компоненттер EN 50155 [43] сәйкес сертификатталған.

Жұмыс тобымен Австрия, Германия, Бельгия, Түркия, Ресей темір жолдары, зертханалары және өндірістік қуаттары арқылы сапарлар жүргізілді. Бұл сапарлар нәтижелері бойынша осындай шешімдерді қарастыруда құнды тәжірибе алынды және «KTCS» жүйесін әрі қарай дамыту жоспары құрылды.

«KTCS» жүйесінің прототипін жасау кезінде Өзен – Болашақ және Қорғас – Жетіген телімдерінде пилоттық сынақтар өткізілді, онда сандық радиожүйелерді қолданумен нағыз уақыт режимінде пойыздар қозғалысын интервалды реттеу үрдісін автоматтандыру үшін көпфункционалды жүйе енгізілді. Алынған әсер келесі бойынша сипатталады:

- бастапқы капиталдық салымдардың айтарлықтай азаюы. Алғашқы пилоттық жобаны енгізудің толық құны бейімделуді, тестілеуді және СОБ және байланыс бойынша құрылыс-монтаж жұмыстарына кететін шығындарды қосқанда дәстүрлі АБ құру құнынан 3,8%-ға төмен.

- құрылыс мерзімдерінің айтарлықтай қысқаруы (20%-дан астам).

- эксплуатациялық шығындардың айтарлықтай азаюы (дәстүрлі АБ құру Жобасымен анықталған саннан 27%-ға пайдаланушы тұлға санының қысқаруы, автокөлік құралдары жалпы санының шамамен 2 есеге қысқаруы, ЦШ-720 нұсқаулығына сәйкес СОБ құрылғыларын тексеру көлемінің шамамен 3 есеге азаюы).

- жүйенің жоғары сенімділігі және дайындығы – негізгі басқару құралдары істен шыққан жағдайда жүйе пойыз аралыққа кіруін және босатуын қауіпсіз бақылаумен қорғаныс күйіне көшкен жағдайда жүйенің негізгі элементтерін «ыстық резервтеу»

Осылайша темір жолда ең заманауи топтық басқару және белгі беру жүйесі болып табылатын KTCS пойыз қозғалысын басқаратын және бақылайтын коммуникациялық жүйені құрайды.

KTCS теміржол қабатымен байланысқан инерциялық координаталық жүйені пайдаланады. Нөлдік есеп нүктесіне жөнелту бекетінің ортаңғы жолағы қабылданады. Жүрілген қашықтық жүріп өту жолының бойымен метр арқылы өлшенеді. Жүрілген қашықтықты өлшеу және құрамның ағымдағы күйін анықтау үшін екі тәуелсіз тетік пайдаланылады: осьтік тетік және радарлық тетік. Осьтік тетікті калибрлеу үшін бір-бірінен қатаң белгіленген қашықтықта орнатылған жолдық реперлік белгілер қолданылады. Әр реперлік белгі бірегей нөмірге ие [44].

Ағымдағы координаталарды анықтау үшін инерциялық жүйені пайдалану KTCS жүйесі жұмысының сыртқы әсерлерге орнықтылығын арттырады, бұл оған автономды жұмыс істеуге мүмкіндік береді.

Бекеттерде локомотивті позициялау, құрам қозғалысының бағытын анықтау және локомотивті құрамға қатысты бағдарлау үшін спутниктік навигация жүйе мәліметтері пайдаланылады. Жаһандық навигациялық жүйе

жоғары дәлдікпен локомотивтердің сағат жүрісі мен диспетчерлік қозғалысты басқару құралдарын синхрондауға мүмкіндік береді, ол өз кезегінде, борттық басқарушы бақылағышқа уақытылы шешім қабылдап, құрамды жүргізу бойынша уақытылы ұсыныстар жіберуге мүмкіндік береді.

Борт құрылғысы өзінің құрамында локомотив тартымын және пневматикалық тежегішті басқару құралдарын қамтиды. Апаттық тежеуді машинист те, диспетчерлік басқару да орындауы мүмкін, соңғы жағдайда апаттық тежеу бұйрығы бойынша бастапқыда тартым қозғалтқыштары ажыратылады да, кейін пневматикалық тежеу қосылады. Тежеу жолы мен тежеу уақытын есептеу тежегіш қалыптарының экипаждарында пайдаланылатын жол профилін, әр экипаж салмағын ескере отырып есептеледі [45].

«KTCS» жүйесінің негізгі жұмыс принциптері қысқаша түрде келесі элементтермен ұсынылған:

1. Борттық бақылағыш және машинист терминалы.

Бақылағыш тежеу жолының ағымдық мәнін есептейді, инерциялық координаталар жүйесіне калибрлеу жүргізеді, пойыздар арасындағы қауіпсіз арақашықтықты, қабылданған координаталар жүйесінде құрамның ағымдық күйін есептейді, машинист мониторында қозғалыстың ағымдық параметрлерін, диспетчер АЖО-мен байланыс күйін, алда жүріп келе жатқан құрам соңына дейінгі арақашықтықты, виртуалды бағдаршам көрсеткіштерін, тежеу жолының ұзындығын кескіндейді. Борттық бақылағыш ретінде арнайы «KTCS» жобасы үшін әзірленген бақылағышты пайдалану ұсынылады.

2. Координаталық жүйе құралдары.

Ось тетігі одометриялық жүрілген жолды өлшеу жүйесінде пайдаланылады. Әр локомотивте орнатылады:

- құрам қозғалысының желілік жылдамдығын, жылдам жеделдетілуін және жүрілген жолды есептеу үшін осьтік жылдамдық тетігі;
- доплерлік радарлық құрам жылдамдығының тетігі. Координаталық навигациялық жүйенің қосымша каналы – жылдамдықты, жеделдетілуді және жүрілген жолды түйіспесіз өлшейтін доплерлік радар.

Екі қозғалыс параметрлері тетігінен мәліметтерді пайдалану инерциялық координаталар жүйесінде құрамды позициялау қателігін азайтады да, навигациялық координаталық жүйенің сенімділігін арттырады.

Құрамның бүтіндігі тежегіш магистралінде қысымды бақылайтын, соңғы вагон координаталарын анықтайтын және машинист кабинасына радиоканал арқылы мәліметтер жіберетін құралмен анықталады.

Басқару орталығының негізгі компоненті істен шығуға орнықты хост-компьютерлер жүйесі болып табылады (1oo2D). Қауіпсіз интервалды қамтамасыз етуші бақылағыш блоктауды басқару ядросынан және қауіпсіздікті қамтамасыз ету ядросынан тұрады, аралықта барлық қауіпсіздік функцияларын атқарады. Хост-компьютерлер аппараттық және бағдарламалық қамтамасыз етуді бірге бақылау үшін бір-бірімен желі көмегімен жалғанған [46].

3. Объекталық бақылағыш.

Объекталық бақылағыш бекеттерде «KTCS» жүйесінің құрамында функция атқарады және бағдаршамдарды, бұрмалы электр жетектерін, переездік белгі беруді басқару, пойыз жағдайын шолу үшін қызмет етеді.

Объекталық бақылағыш аумақтық таратылған компоненттерді бақылау және басқару үшін және күрделі климат жағдайында және қатаң сыртқы ортада пайдалану үшін арналған.

4. Қозғалыс қауіпсіздігін қамтамасыз етуші жол құрылғысы:

1. Осьтер санау жүйелері.

Осьтер санау жүйесі құрамның бекет жолдары арқылы өтуін бақылау, құрамның рұқсат етілмеген қозғалысын бақылау, жол телімдерінің, бағыттама бұрмаларының бостығын анықтау үшін пайдаланылады.

Рельс тетіктері жылжымалы құрам дөңгелектерінің өтуін тіркейді, соның негізінде осьтер санау бақылағышы телімге кірген және одан шыққан осьтер санын анықтайды. Телімде орналасқан санағыштар көрсеткіші бойынша әр санау пунктінде телімнің бос емес немесе бостығы жөнінде ақпарат қалыптасады [47].

2. Реперлік тетіктер.

Бекеттен шыға берісте рельс табанында орнатылған қабылдап-таратушылар локомотив бортына олардың қондырылған координаталарын жібереді. Реперлік тетіктерді қолдану инерциялық локомотивтік координаталар жүйесін калибрлеуге мүмкіндік береді. Ешқандай қосылуды талап етпейтін пассивті реперлік тетіктерді пайдалану ұсынылады. Бұл тетіктер өздеріне жазылған ақпаратты, дәлірек айтқанда өздерінің орналасқан жері жөнінде ақпаратты таратады [48].

3. Мәліметтер тарату жүйесі.

«ҚТЖ «ҰК» АҚ-да ғылыми техникалық кеңес шешіміне сәйкес бұл жүйе ІР-хаттама қолданумен бірегейлендірілген тәсіл арқылы жүзеге асырылған. Байланыс инфрақұрылымы, ғылыми техникалық кеңес шешіміне сәйкес, «TETRA» стандартының транкингітік байланыс жүйесіне құрылған, ол мынаны қосады:

- басқару және коммутациялау инфрақұрылымын;
- абоненттік терминалдарды.

«TETRA» инфрақұрылымына «TETRA» желісінің радиохабарын және қажетті функциялау режимдерін қамтамасыз ететін құрылғы жатады; коммутациялау/маршруттау орталығы; базалық бекеттер; диспетчер пульттері; жүйені басқару орталығы; басқа желі шлюздері; қосымша серверлері және т.б.

Қауіпсіз мәліметтер тарату хаттамасы FSFB2 пайдаланылады.

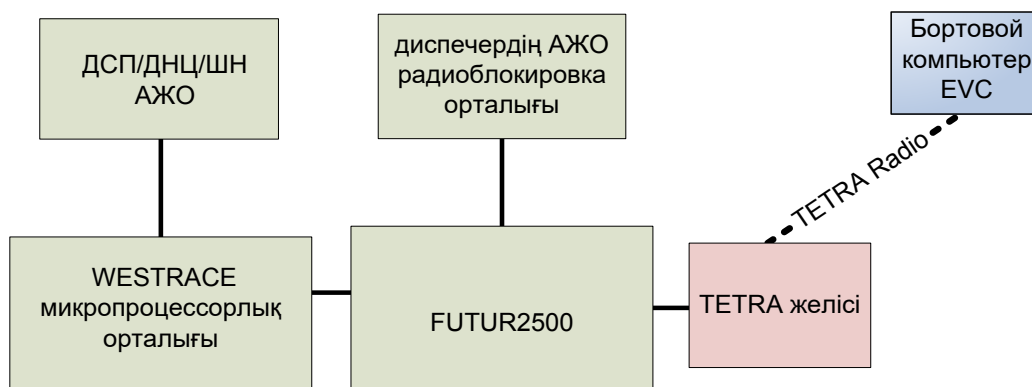
Жүйе қозғалыс қауіпсіздігінің халықаралық стандарттарына да, қазақстандық ұлттық стандарттарына да сай келеді. Ұзындығы құрамның қозғалыс жылдамдығына, жол профиліне, құрам типіне, құрамдағы экипаждардың тежегіш сипаттамаларына байланысты болатын жылжымалы блок-телімдер тұжырымдамасы негіз болып табылады. Диспетчерлік басқару жүйесі пойыздар қозғалыс кестесінің орындалуын үздіксіз бақылайды, пойыз қозғалысында ақау туындаған жағдайда жету және кестені қалпына келтіру

функциясын іске асырады. Пойыз диспетчері үшін көрнекті жүйе интерфейсі көмекші диалог режимінде де, автоматты режимде де пойыздар қозғалысын басқаруға мүмкіндік береді. Сонымен қатар, жүйе пойыз жағдайы мәліметтерінің бірыңғай базасына ие, бұл маневрлік жұмысты басқаруды аралықтағы қозғалыспен тыныш үйлестіруге мүмкіндік береді. Жүйе құрамына «ДСП» АЖО-дары, «ПТО» АЖО, «ШН» АЖО кіреді [49].

KTCS жүйесі аралықта және бекетте пойыздар қозғалысының қауіпсіздігін және басқаруды қамтамасыз ететін жүйелердің бірыңғай кешенін құрайды:

- микропроцессорлық орталықтандыру жүйесі (аралықта пойыздар қозғалысын басқару жүйелерін, сондай-ақ тасымалдауды басқару орталығының құрылғысын және ДСП, ДНЦ және ШН АЖО-дарын қосқанда);
- радиоблоктау орталықтары (жылдамдық шектеуді енгізу үшін диспетчер орталығы АЖО, сондай-ақ пойыздың орналасқан жерін нақтылау үшін жол құрылғысын қосқанда);
- пойыз қозғалысын бақылау және басқарушы борт компьютері және оған жататын перифериялық құрылғылар;
- жол құрылғыларының ішкі жүйелері Ethernet желісі арқылы жалғанады. Борт компьютері мен радиоблоктау орталығы арасындағы жалғану TETRA радиоканалы арқылы жүзеге асырылады [50].

KTCS жүйесінің негізгі компоненттерінің арасындағы байланыстың құрылымдық сұлбасы 2.1 суретте ұсынылған.



Сурет 2.1 – KTCS ұлттық жүйесінің негізгі компоненттері

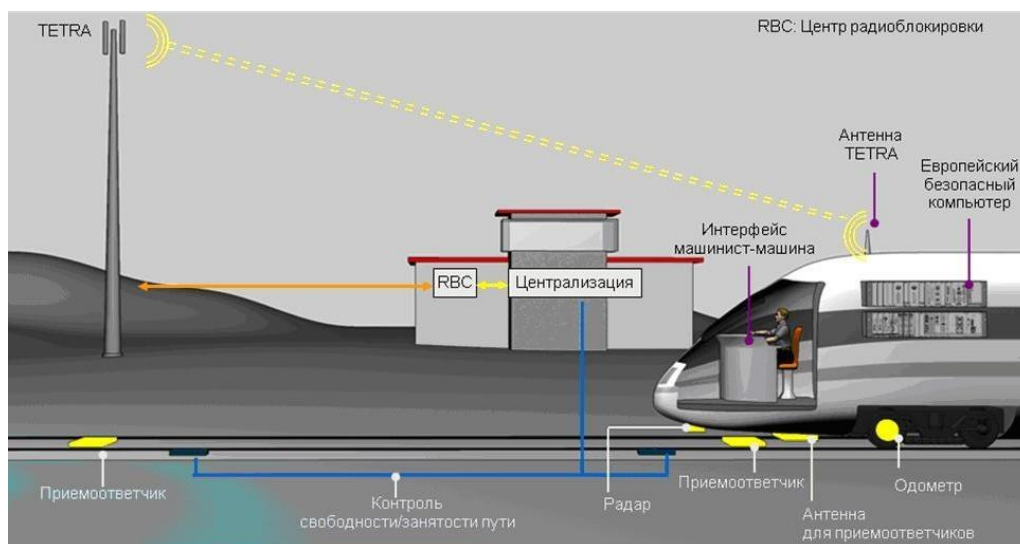
Ұсынылған шешім бекеттер арасына сигналдық-блоктаушы кабель төсеуді қажет етпейді, бұл құрылғы құнын ғана емес, сонымен бірге мыс кабель төсеуге, оған қызмет көрсетуге және жөндеуге кететін шығынды айтарлықтай үнемдетеді.

Пойыз қозғалысының маршруттары микропроцессорлық орталықтандыру жүйесімен орнатылады және бақыланады. Жол құрылғыларының күйі жөнінде ақпарат (мысалы, бұрмалық электр жетектерінің жағдайы, сигнал көрсеткіштері) микропроцессорлық орталықтандыру жүйесінен радиоблоктау орталығына жіберіледі. Орталықтандыру пойызға жүруге рұқсат беру үшін

радиоблоктау орталығына қажетті ақпаратты жібереді. Микропроцессорлық орталықтандырумен сигнал ашылған кезде радиоблоктау орталығы сол сигналды жүріп өтуге рұқсат береді де, сигналға жақындап келе жатқан немесе сигналдың алдында тұрған пойыздың борт компьютеріне берілген ақпаратты TETRA радиобайланыс жүйесі арқылы жібереді. Жіберілген ақпаратта жылдамдықты шектеу немесе тоқтау орнына дейінгі қашықтық (мысалы, тыйым салушы сигналға дейінгі қашықтық) және желі сипаттамалары (мысалы, жол профилі, сондай-ақ телімдегі тұрақты және уақытша жылдамдықты шектеулер) қамтылады. Борт компьютері машинист дисплейіне жүріп өтуге рұқсат береді. Осыдан кейін машинист сигналды жүріп өте алады.

Пойыз қозғалысы кезінде борт компьютері машинист жылдамдықты жоғарылатқан жағдайда оған ескерту бере отырып, рұқсат етілген жылдамдықты бақылайды. Егер машинист ескертуге қарамай, жылдамдықты азайтпаса, борт компьютері пойыздың автоматты түрде тоқтауын жүзеге асырады [51].

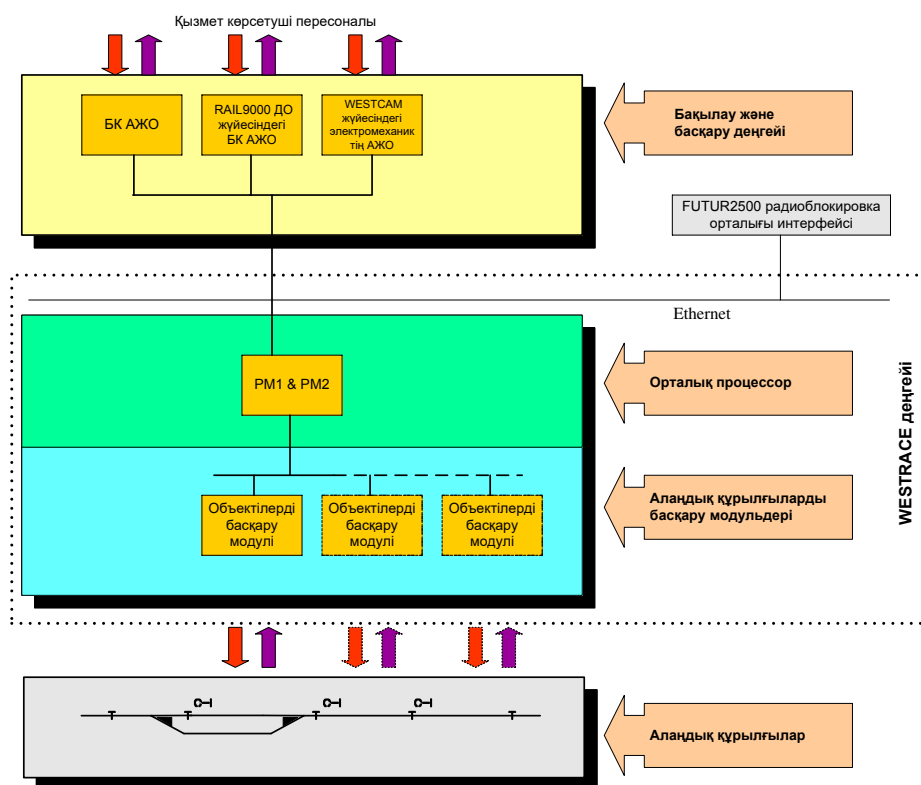
Пойыз циклдік түрде (кемінде әр 6 секунд сайын) радиоблоктау орталығына өзінің орналасқан жері туралы ақпарат жібереді. Одометрия қателігін түзету үшін желіге белгілі бір қашықтықта қондырылған тіркелген мәліметтері бар қабылдап-жауап берушілер пайдаланылады. Пойыздың орналасқан жері жөнінде есеп беру пойыздардың жол элементтерімен дұрыс арақатынасы үшін радиоблоктау орталығы ретінде қолданылады. Жүйенің жұмыс принципі 2.2 суретте түсіндіріледі.



Сурет 2.2 – KTCS жүйесінің жұмыс принципі

2.3 суретте бір бекет мысалында келтірілген МПО жеңілдетілген құрылымы ұсынылған. Басқару және бақылау жоғары деңгейінде бекет кезекшісі, пойыз диспетчері және ББОБ электрмеханигіне арналған АЖО бар. Орташа деңгейде радиоблоктау орталығымен біріктірілген екі РМ жинағы бар орталық процессорлық құрылғы орналасқан, одан төмен жол құрылғыларын

басқару модульдері бар. Осы деңгейде көршілес орталықтандырулармен интерфейс қамтамасыз етіледі.



Сурет 2.3 – Бір бекет мысалында келтірілген МПО құрылымы

Пойыздар қозғалысын басқару кезінде KTCS жүйесіндегі негізгі канал радиоканал болып табылады. KTCS жүйесі аясында диспетчерлік қозғалысты басқару орталығы мен жылжымалы құрам арасында да, диспетчерлік орталық пен жол құрылғысының арасында да мәлімет алмасу үшін TETRA стандартының сандық радиобайланысы пайдаланылады. Қос жабынды радиожелісін пайдалану қарастырылады [51].

TETRA транкингтік байланыс жүйесінің негізгі элементтері:

1. Басқару және коммутациялау инфрақұрылымы.

TETRA инфрақұрылымына:

- TETRA желісінің радиохабарын және қажетті функциялау режимдерін қамтамасыз ететін құрылғы жатады;

- коммутациялау/маршруттау орталығы;
- базалық бекеттер;
- диспетчер пульттері;
- жүйені басқару орталығы;
- басқа желі шлюздері;
- қосымша серверлері және т.б.
- абоненттік терминалдар.

TETRA стандарты абоненттік құрылғыны (радиостанциялар) функциялаудың екі режимін қарастырады [52]:

1. Транкингтік радиобайланыс режимі (Trunked Mode Operation, TMO).

ТМО режимі абонент базалық бекеттің әрекет ету аумағында орналасқан кезде мүмкін болады. ТМО режимі абонентке TETRA барлық мүмкіндігін жеткізе алады және келесі тапсырмаларды орындау үшін оңтайландырылған: а) дыбыс пен мәліметтерді бір уақытта жіберу (V+D), б) мәліметтерді топтық тарату (Packet data optimized).

2. Тікелей жіберу режимі (Direct Mode Operation, DMO).

DMO режимі TETRA базалық бекеттерінің әрекет ету аумағынан тыс жерде абоненттер арасында топтық өзара әрекеттесу үшін арналған. Абоненттер арасындағы байланыс жартылай дуплексті режимде жүзеге асырылады, бірақ бұл кезде жеке немесе топтық шақыру жасау мүмкіндігі сақталады.

TETRA стандарты жылжымалы радиобайланыс жүйелерінде максималды мүмкін болатын жиілік тиімділігін іске асырады – 4 логикалық канал 25 кГц-ты алады. Сонымен бірге TETRA стандарты жиілікті дуплекс технологиясымен (Frequency Division Duplex, FDD) бірге уақыт бөлігі бар (Time Division Multiple Access, TDMA) көпбекеттік қол жеткізу технологиясын пайдаланады. Радиоканал модульдеуінің типі – $\pi/4$ есе ығысуы бар қатыстық дифференциалдық фазалық манипуляция ($\pi/4$ DQPSK) [53].

TETRA стандарты аясында жүйе ресурстарын рұқсатсыз пайдалануды болдырмауға және желіге жіберілетін ақпараттың құпиялылығын қамтамасыз етуге бағытталған желіде қауіпсіздікті қамтамасыз ету қарастырылған [54].

Бұл келесі механизмдермен жүзеге асырылады:

- абоненттерді де, инфрақұрылымды да аутентификациялау;
- ақпаратты шифрлау;
- абонент параметрлерінің құпиялылығын қамтамасыз ету.

Абоненттерді аутентификациялау басты кілт (K-key) және TEI бірегей нөмір негізінде жүзеге асырылады. Идентификаторы дұрыс емес абоненттік терминал TETRA жүйесінің ресурстарына жіберілмейді.

Ақпаратты шифрлау TETRA стандартының әр нақты жүйесінің қосымша ерекшелігі болып табылады. TETRA стандартының радиоинтерфейсі алдын ала қорғалған болып саналады. Бірақ шифрлау бойынша басқа да қосымшалар болуы мүмкін:

- E2E (End-to-End) – радиостанция-радиостанция жеке шақыруларын шифрлау (шифрлау кілтінің ұзындығы 128 битті құрауы мүмкін);
- топтық шақыруларды шифрлау;
- TEA1, TEA2, TEA3 алгоритмдері (TETRA Encryption Algorithm) бойынша радиоинтерфейсті шифрлау [55].

Абонент параметрлерінің құпиялылығы абоненттік терминал құрылымын кодтық қорғау және идентификатор-жалған есімдер беру арқылы қамтамасыз етіледі.

Сонымен қатар координаталық интервалды реттеу жүйесін құру үшін координаталық реттеу тапсырмаларын орындау мақсатында локомотив пен басқару орталығы арасында ақпарат тарату жүйесіне қойылатын талаптарлы қалыптастыру қажет.

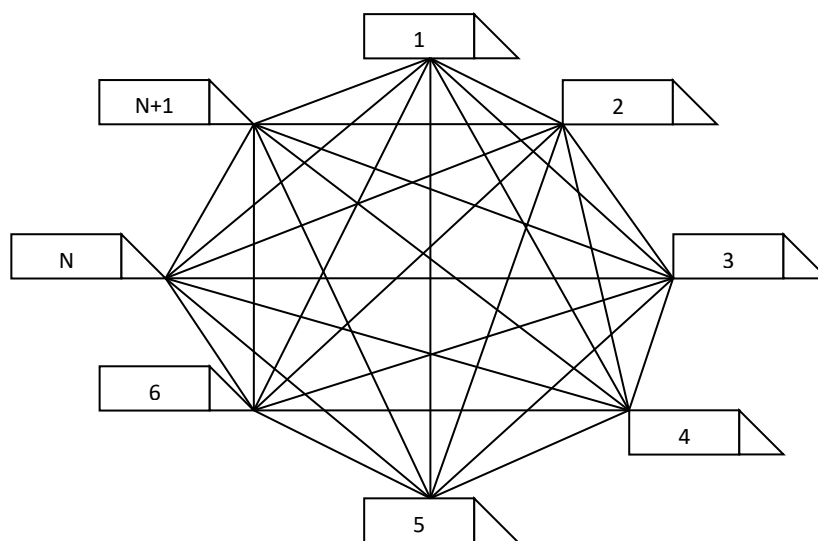
2.2 Сандық радиоканалдар базасындағы интервалды реттеу жүйелерінің ерекшеліктері

Сандық радиоканалдары бар ПҚИР жүйелерін шартты түрде орталықтандырылған, орталықсыздандырылған және аралас деп бөлуге болады.

Орталықтандырылған түрге, мысалы, 2 деңгейлі ERTMS/ETCS жүйесі жатады, онда радиоблоктау орталығын пайдалану арқылы орташа ұзындығы 80 км телімде пойыздар қозғалысын басқару қарастырылады. Бұл орталықта маңызды ақпарат мамандандырылған қауіпсіз компьютермен өңделеді де, кейін GMS-R стандартының сандық радиоканалдары арқылы жіберіледі [33, б. 58].

Радиоблоктау орталығында жалпы пойыз жағдайын, тұрақты және уақытша жылдамдық шектеулерді және жол профилін есепке ала отырып, әр жылжымалы бірлік үшін өзінің жауапты аумағында жеке қозғалыс жылдамдығы есептеледі [56].

Орталықсыздандырылған түрге біріктірілген пойыздарды тоқтаусыз қалыптастыру және тарқату операцияларын автоматтандыруды қамтамасыз ететін ПҚИР ұсынылатын жүйесін жатқызуға болады, оның функционалдық сұлбасы 2.4 суретте келтірілген. Бұл жүйеде радиоканалдар арқылы пойыздарды жалғау немесе ажырату операцияларын орындауға бұйрық алғаннан кейін, барлық қажетті бақылау және басқарушы ақпарат борттық қауіпсіз микропроцессорлық басқару блогында өңделеді.



Сурет 2.4 – Қозғалыс басқарудың орталықсыздандырылған құрылымы

Аралас жүйелерде қажетті ақпаратты өңдеу стационарлық орталықта қондырылған мамандандырылған қауіпсіз компьютер мен борттық бақылау және басқару құрылғылары арасында бөлінеді. Бұл, мысалы, General Electric фирмасының ITCS жүйесі, онда локомотивтер мыналарға жауап беретін борт бақылағышымен жабдықталады: бір метрге дейін дәлдікпен пойыздың орналасқан жерін анықтау, құрам бүтіндігін бақылау, жол құрылғыларының күйі жөнінде ақпарат өңдеу және жылдамдық шектеулерді қадағалау. ITCS жүйесінің бекет құрылғысының құрамына кіретін қауіпсіз логикалық

бақылағыш электрлік микропроцессорлық орталықтандыру функцияларын орындайды. Локомотив құрылғысымен мәлімет алмасу модулі басқару аумағындағы барлық локомотивке сигналдар, бұрмалар мен переездердің күйі жөнінде ақпарат таратады, ал спутниктік навигация координаталарын тексеру модулі пойыздардың географиялық координаталарын жолдағы пикеттерге есептеп шығарады.

Орталықсыздандырылған жүйелерде борт құрылғысының маңызды тапсырмасы [57] немесе [58] құжаттарының талаптарына сәйкес орындалатын пойыздың орналасқан жеріне байланысты тежеу қисықтарын динамикалық есептеу болып табылады. Ол үшін борттық электрондық картаға тіреуіш нүктелер координаталары бар сандық телім моделі енгізіледі, олар шынайы немесе «виртуалды» бализдер, сондай-ақ рельс тізбектерінің немесе ось санағыштарының генераторлары болуы мүмкін [56].

Нақты жол нүктесінде пойыз қозғалысының рұқсат етілген жылдамдығын динамикалық есептеу дәлдігі оның бас локомотивінің координатасын анықтау дәлдігіне байланысты. Пойыз басының координатасын дұрыс анықтамауға әкелетін қауіпті істен шығу қарқындылығы 10^{-9} сағ⁻¹ кем болуы қажет [56].

ПҚИР жүйелерінде сандық радиоканалдарды қолдану олардың сенімділігіне, қауіпсіздігіне және кедергіден қорғанысына қойылатын талаптарды жоғарылатады.

Радиоканалдар арқылы мәліметтер тарату сенімділігі EN 50159:2010 стандартының талаптарына сәйкес келуі тиіс [59]. Каналдарды коммутациялау режимінде радиоблок-орталығы мен борт құрылғысы немесе түрлі локомотивтердің борт құрылғысы арасында мәлімет тарату кезіндегі максималды кідіріс 99 % жағдайда 500 мс кем болуы, ал қосылу жоғалған істен шығу қарқындылығы – 10^{-2} сағ⁻¹ кем болуы тиіс.

Радиоканалдар арқылы жауапты ақпарат жіберу кезінде қауіпті қателіктерді минималдау талаптары да орындалуы қажет [60]. Статистикалық ақпарат негізінде, отандық пойыз байланысы жүйесінде сандық радиоканалдар арқылы аралықта және бекетте пойыз жағдайы жөнінде жауапты ақпарат тарату қателігі бір битке 2×10^{-2} -нен төмен болмағаны орнатылды [61].

Жауапты ақпарат тарату үшін негізгі құрал ретінде қолданған кезде сандық радиоканалдың кедергіге орнықты болу талаптары, мысалы, Рид – Соломон кодын пайдалану есебінен қамтамасыз етілуі мүмкін [60, 62].

ПҚИР жүйелерінде сандық радиоканалдарды қолдану пойыз аралық интервалды азайтуға мүмкіндік береді және пойыз жүргізудің көптеген операцияларын автоматтандыру мүмкіндігін қамтамасыз етеді, бұл локомотив бригадаларының пойыз қозғалыс қауіпсіздігіне әсерін азайтады. Осыған байланысты, «автомашинист» типті жүйелерді әзірлеу әбден шындыққа айналады деп тұжырымдауға болады [63]. Алайда мұндай жүйелерде олардың аппараттық және бағдарламалық құралдарын әзірлеу, дайындау және техникалық пайдалану сатысында «адам факторының» әсері жоғарылайды.

2.3 Радиоканал базасында пойыздарды басқару жүйелерін құрастыру құрылымдары

Радиоканал негізінде пойыздар қозғалысын координаталық реттеу принциптерін іске асыру белгілі бір құрылым бойынша жасалған аппараттық-бағдарламалық құралдар жинағының көмегімен орындалады. Нақты түрде, пойыздар қозғалысын координаталық реттеу принциптерін іске асыру үшін әр пойызда алда кетіп бара жатқан пойыз соңына дейінгі қашықтық жөнінде ақпарат болуы қажет. Бұл борт құрылғысына тоқтауды қамтамасыз ету үшін қозғалыс жылдамдығын бақылауға мүмкіндік береді.

Координаталық реттеу жүйесін құрудың теориялық мүмкін болатын принциптерінің бірі орталықсыздандырылған архитектура болып табылады. Мұндай тәсілде бірыңғай басқару орталығы болмайды, және жүйе пойыздан пойызға ақпарат жіберу арқылы жұмыс істейді. Яғни бірінші келе жатқан пойыз өзінің орналасқан жері жөнінде артындағы пойызға мәлімет жіберуі қажет. Сол уақытта борт құрылғысымен көрші пойызды анықтау тапсырмасы аса күрделі болып табылады. Басқару жүйесінің жұмысы үшін әр пойыз кең таратылатын форматта өзінің орналасқан жерін хабарлауы тиіс. Көрші пойыздардың мекен-жайын (идентификаторларын) анықтау мүмкіндігі болмағандықтан мекен-жайлық жіберу форматы мүмкін емес.

Нақты түрде, кең таратылған жіберу кезінде әр пойыз өзі жөнінде ақпарат таратады. Орталықсыздандырылған басқару жүйесі функциясының қарапайым құрылымы 2.5 суретте көрсетілген.

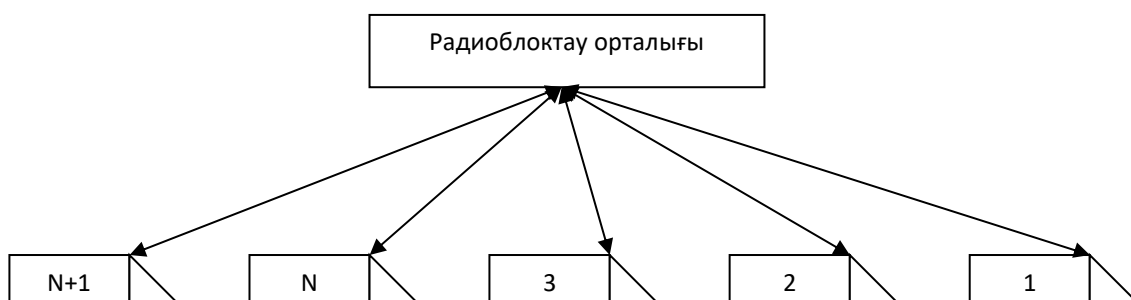
Мұндай жүйеде әр пойыздың қосылу саны радиобайланыс әрекет ету аумағындағы пойыздар санына тең. Яғни пойыздың борт құрылғысы кең таратылатын хабар алынған барлық пойыздың орналасқан жерін, жол нөмірін талдап, жүру бағытында алда келе жатқан пойызды және оған дейінгі қашықтықты анықтауы қажет.

Тәжірибеде мұндай жүйені құрастыру өте күрделі тапсырма болып табылады. Кең таралған хабар жіберу байланыс желісіне үлкен жүк түсіреді. Орталықсыздандырылған архитектура кезінде қосылу саны 2.5 суреттегі бағана қабырғасының санына тең және $n * (n - 1) / 2$ тең [64].

Борт құрылғысы барлық пойыздан жаппай хабарды өңдеуі тиіс, бұл есептеу мүмкіндіктеріне жоғары талаптар қояды. Ең болмағанда бір локомотивпен байланыстың жоғалуы орталықсыздандырылған жүйе үшін аса маңызды және апатқа әкеп соғуы мүмкін.

Тәжірибеде пойыз басқарудың орталықсыздандырылған жүйесін оның күрделілігі мен апат жағдайлары туындауының аса жоғары ықтималдылығынан ешқайда қолданбайды.

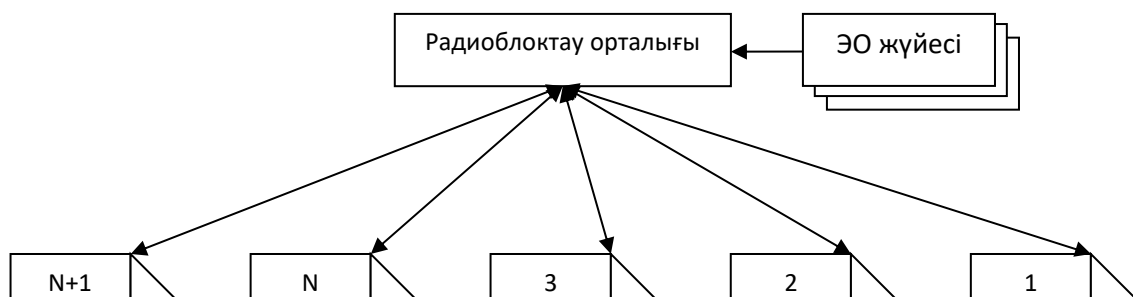
Радиоканал базасында қозғалысты интервалды реттеудің ең кеңінен таралған тәсілі радиоблоктау орталығы қолданылатын орталықтандырылған құрылым болып табылады. Радиоблоктау орталығы барлық локомотивтен мәлімет алу және тарату жолымен барлық ақпаратты шоғырлайды. Мұндай жүйе құрылымы 2.5 суретте көрсетілген.



Сурет 2.5 – Қозғалысты басқарудың орталықтандырылған құрылымы

Радиоблоктау орталығы пойыздар арасында бағыттас жүрудің қауіпсіз интервалын қамтамасыз ете отырып, телімдегі барлық пойызды бақылайды. Радиоблоктау орталығы жұмысының негізгі принципі пойыздардың орналасқан жері жөнінде ақпарат жинау, әр пойызға жүріп өту үшін рұқсат етілген қашықтықты есептеу және сол ақпаратты локомотивтердің борт құрылғыларына жіберу болып табылады [65].

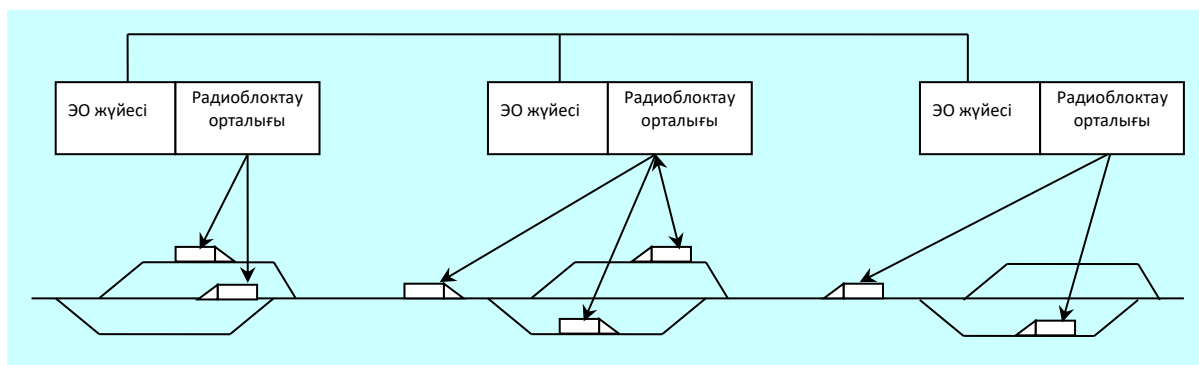
Пойыз бекет арқылы жүрген кезде орнатылған маршруттар жөнінде қосымша ақпарат қажет, сондықтан радиоблоктау орталығына электрлік орталықтандыру жүйелерін қосады. Мұндай жүйенің құрылымы 2.6 суретте көрсетілген.



Сурет 2.6 – ЭО жүйелері қосылған қозғалысты басқарудың орталықтандырылған құрылымы

Бірінші бос емес рельс тізбегіне дейін пойыздар қозғалысын реттеуді пайдаланған кезде радиоблоктау орталығына аралықтағы рельс тізбектерінің жағдайы жөнінде ақпарат қажет болады, бұл радиоблоктау орталығына автоматты блоктау жүйесін қосуға әкеп соғады. Бұл әрекет құнын азайту үшін бақылау режимінде жұмыс істейтін рельс тізбектерін ғана қосу мүмкін болады.

Пойыздар қозғалысын басқару жүйесінің аралас құрылымы әр электрлік орталықтандыру жүйесінің жанына бекет пен оған жанасқан аралықтар жартысының әрекет ету аумағында жергілікті радиоканал арқылы локомотивтерге ақпарат жіберуге және қабылдауға мүмкіндік беретін қосымша блок орнатуды қарастырады (2.7 сурет).



Сурет 2.7 – Қозғалыс басқарудың аралас құрылымы

Аралас құрылым кезінде бірқатар жағдайда функциялардың бір бөлігін борт құрылғысына көшіріп, пойыздар қозғалысын интервалды реттеу жүйесі жұмысының баламалы логикасын қолданады. Жергілікті радиоканал арқылы бекеттегі маршруттар, рельс тізбектерінің күйі жөнінде кең таралатын ақпарат жіберіледі. Борт құрылғысы алынған мәліметтер негізінде қозғалыс рұқсатын қалыптастырады [66].

2.4 Радиоканал қолдану арқылы пойыздар қозғалысын реттеу технологиясы

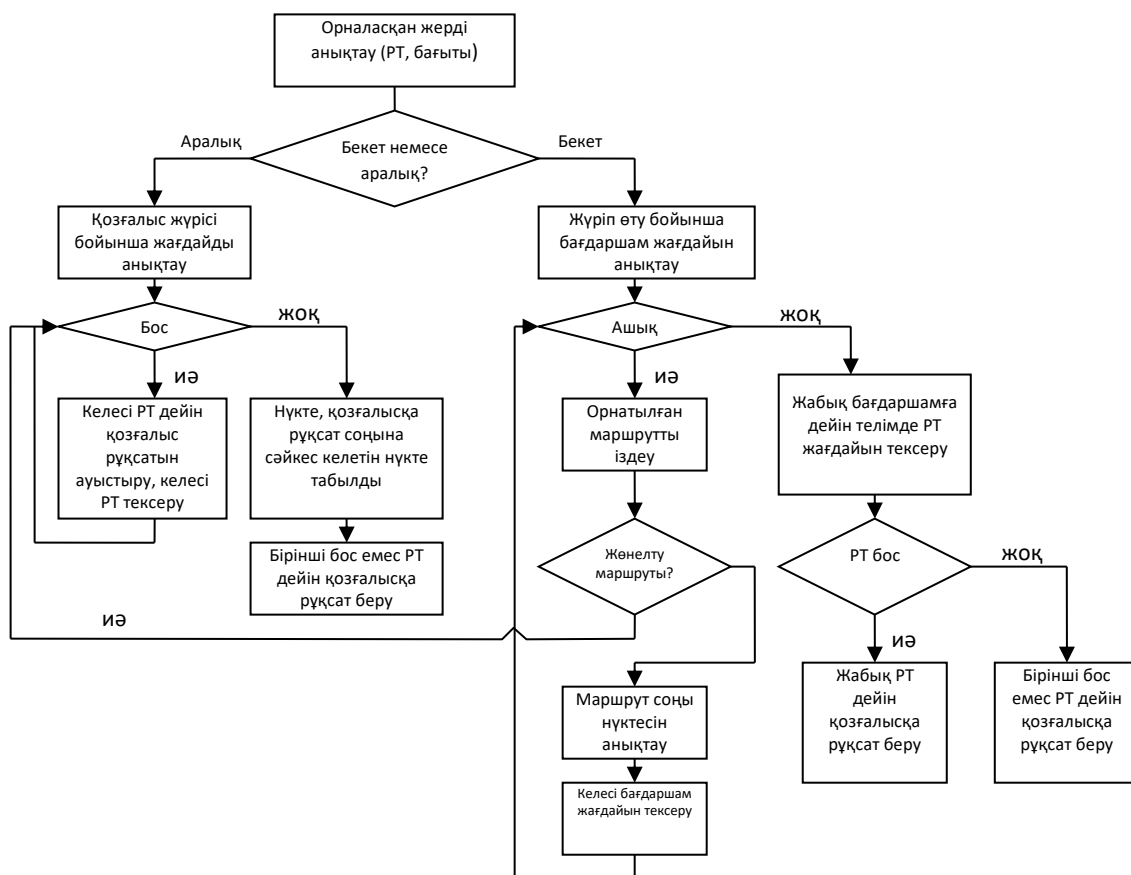
Қозғалыс рұқсатын қалыптастыру алгоритмі пойыздың орналасқан жері, бекет және аралық жоспарлары жөнінде ақпарат, сондай-ақ электрлік орталықтандыру жүйелері мен аралықтағы рельс тізбектерінің күйі жөніндегі мәліметтер базасында құрылады.

Аралықта пойыз қозғалысы кезінде бірінші бос емес және қозғалыс рұқсаты қалыптасатын рельс тізбегіне дейін жүріп өту барысында рельс тізбектерінің жағдайы тексеріледі.

Бекетте немесе бекетке келу кезінде қозғалыс барысында бағдаршам жағдайы тексеріледі. Егер бағдаршам рұқсат етуші көрсеткішке ие болса, онда орнатылған маршрут орналасқан және бекетте келесі бағдаршамға сәйкес келетін маршруттың аяқталу нүктесі анықталады. Маршрут аяқталу нүктесінде келесі бағдаршам күйі және әрі қарай цикл бойынша тексеріледі. Егер бағдаршам жабық болса, онда маршруттағы рельс тізбектерінің күйі тексеріледі және рельс тізбектері бос болса жабық бағдаршамға дейін қозғалысқа рұқсат беріледі. Қозғалыс рұқсатын қалыптастыру алгоритмінің блок сұлбасы 2.8 суретте келтірілген.

Орнатылған жөнелту маршрутында аралықтағы рельс тізбегінің күйін тексеру және қозғалыс рұқсатын қалыптастыру жүргізіледі.

Қозғалыс рұқсатын қалыптастыру үшін бекеттік сұлбалық жоспары, барлық маршруттар тізімі қажет болады. Аталған мәліметтер негізінде қозғалысқа рұқсат беру алгоритмі жұмыс жасайды [67].

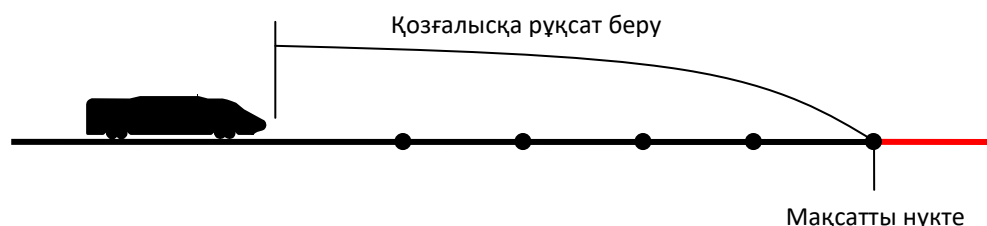


Сурет 2.8 – Қозғалыс рұқсатын қалыптастыру алгоритмінің блок сұлбасы

Радиоблоктау орталығы әр пойыз үшін 2.9 суретте ұсынылған алгоритм бойынша қозғалысқа рұқсат берілген жерге дейінгі нүктені анықтайды. Мақсатты нүкте өзгерген кезде пойызға жаңа нүктесі бар қозғалысқа рұқсат жіберіледі. Мақсат нүктесінің өзгеруі жүріп өту үшін рұқсат етілген қашықтық артқан жағдайда да, азайған жағдайда да, мысалы маршрут жойылған кезде орын алуы мүмкін. Қозғалысқа рұқсатпен бірге пойызға уақытша және тұрақты шектеулері бар жылдамдық профилі жіберіледі.

Жөнелту маршруты кезінде аралықтағы рельс тізбектерінің күйін тексеру және қозғалысқа рұқсат қалыптастыру жүргізіледі.

Қозғалысқа рұқсат қалыптастыру үшін бекеттің жоспар сұлбасы, барлық маршрут тізімі қажет болады. Аталған мәліметтер негізінде қозғалысқа рұқсат беру алгоритмі жұмыс істейді.



Сурет 2.9 – Қозғалысқа рұқсат беру сұлбасы

Мақсат нүктесі жіберілетін формат маңызды болып табылады. KTCS жүйесінде мақсат нүктесінің координаталары пойыз жүріп өткен евробализ соңғы тобынан қашықтығы ретінде жіберіледі. Осыған ұқсас, рельс тізбегі генераторларының өту мезетін анықтайтын әзірленген алгоритмді есепке ала отырып, мақсат нүктесінің координаталарын генератордың орналасқан жеріне қатысты беруге болады. Әрі қарай, пойыздар жүретін телімдердің жоғары дәлдікті электрондық карталарын құру кезінде жол нөмірін көрсету арқылы желілік жол координатасы түріндегі мақсат нүктесін беру мүмкін болады [68].

2.5 Сандық радиоканалда ақпарат қорғау әдістері

ПҚРЖ құрылғыларының техникалық мүмкіншіліктерін басшылыққа ала отырып, мыналарды анықтау қажет: оңтайлы телеграмма форматы, ашық канал арқылы жіберу кезінде мәліметтерді қорғау белгілі шараларының жинағы. Радиоканал арқылы ақпарат жіберу кезінде қауіпсіздікті қамтамасыз ету құралы мыналар болып табылады: қауіпсіздікті қамтамасыз ету процедуралары және қауіпсіздік кодын пайдалану [69, 70]. Келесі белгілі қорғаныс құралдарын қолдану есебінен: хабардың реттік нөмірі, уақыт мөртабаны, уақытты бақылау, кері байланыс (түбіртек), жіберуші және қабылдаушы идентификаторы, ұқсастыру әдісі, қауіпсіздік коды, криптографиялық әдістер, қауіпсіздікпен байланысты келесі сипаттамаларға қол жеткізіледі: хабардың дұрыстығы, хабардың бүтіндігі, хабардың уақытылы болуы, хабардың тізбегі.

2.5.1 Сандық радиоканалда ақпарат қорғау әдістерін анықтау

Еуропалық стандартқа сәйкес [70] қауіптер/қорғаныстар матрицасын құрамыз (2.1 кесте).

Кесте 2.1 – Сандық радиоканалдардағы қауіптер/қорғаныстар матрицасын

Қауіп түрі ¹⁾	Қорғаныс шаралары							
	Реттік нөмір $i^{(2)}$	Уақыт мөртабаны	Уақытты бақылау $y^{(2)}$	Жіберуші және қабылдаушы идентификаторы $ry^{(2)}$	Кері байланыс $c^{(2)}$	Ұқсастыру әдісі	Қауіпсіздік коды ²⁾	Криптографиялық әдістер
Қайталану	×	×						
Жоғалу	×			×	×	×		
Қосылу	×							
Жүру тәртібінің өзгеруі	×	×						
Бұрмалану							×	×
Кідіру		×	×					
Манипуляция					×	×		×

¹⁾ - [71] сәйкес, х – қолданылады,

²⁾ «автор әзірлеген борт және стационарлық құрылғылардың өзара әрекеттесу алгоритмінде қолданылған қорғаныс шаралары.

Жергілікті радиоканал ашық тарату жүйесі болып табылатындықтан, хабардың келесі нұсқалары мүмкін болады:

1) Мәліметтерді қорғау тарату кодының көмегімен жүзеге асырылады.

Тақырыбы	Пайдалы мәліметтер	Қосымша мәліметтер	Тарату коды
----------	--------------------	--------------------	-------------

Сурет 2.10 – Сандық радиоканалда ақпарат ұсыну құрылымы (1 нұсқа)

Бұл нұсқа ақпарат жіберу жүйесінде жауапсыз хаттама арқылы жіберілетін хабар құрылымын ұсынады. Қауіпсіздікті қамтамасыз ету үшін, жоғарыда айтылғандай, қауіпсіздікті қамтамасыз ету процедуралары мен қауіпсіздік коды қажет.

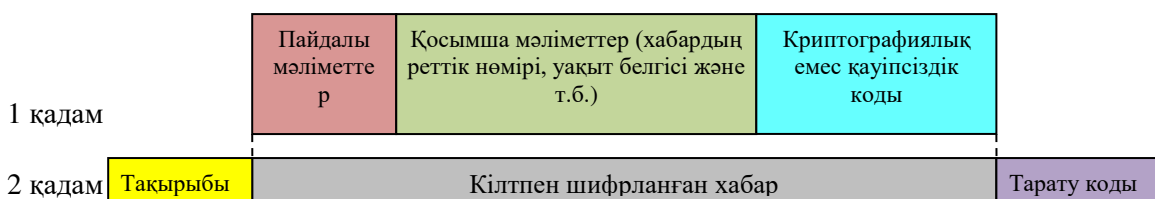
2) Мәліметтерді қорғау қауіпсіздік кодының көмегімен жүзеге асырылады.

Тақырыбы	Пайдалы мәліметтер	Қосымша мәліметтер (хабардың реттік нөмірі, уақыт белгісі және т.б.)	Қауіпсіздік коды	Тарату коды
----------	--------------------	--	------------------	-------------

Сурет 2.11 – Сандық радиоканалда ақпарат ұсыну құрылымы (2 нұсқа)

Қауіпсіздік кодының басты мақсаты мәліметтер бүтіндігін қамтамасыз ету, яғни мәліметтер аумағын кездейсоқ және әдейі бұрмаланулардан қорғау болып табылады. Бұл ретте мәселе бұрмаланудың алдын алуда емес, оларды анықтауда. Оның себебі электромагнит әсерлерінің салдарынан туындаған кедергілер де, тарату каналы компоненттерінің жүйелік немесе кездейсоқ істен шығулары, сондай-ақ саналы зиян келтіру болуы мүмкін.

3) Мәліметтерді қорғау қауіпсіздік кодының көмегімен жүзеге асырылады, ал кейін кілт көмегімен шифрланады, яғни мәліметтер ашық мәтін болып жіберілмейді. Кілт көмегімен шифрлау қасақана бұрмаланудан, ал код – кездейсоқ бұрмаланудан қорғауды қамтамасыз етеді (3 нұсқа).



Сурет 2.12 – Сандық радиоканалда ақпарат ұсыну құрылымы (3 нұсқа)

4) Кездейсоқ және қасақана бұрмаланулардан қорғау үшін түрлі кодтар қолдану. Алайда бұл нұсқаны пайдалану алдыңғы нұсқамен салыстырғанда хабардың артық бөлігінің ұзаруына әкеледі.

Тақырыбы	Пайдалы мәліметтер	Қосымша мәліметтер (хабардың реттік нөмірі, уақыт белгісі және т.б.)	Криптографиялы қ емес қауіпсіздік коды	Криптографиялы қ қауіпсіздік коды	Тарату коды
----------	--------------------	--	--	-----------------------------------	-------------

Сурет 2.13 – Сандық радиоканалда ақпарат ұсыну құрылымы (4 нұсқа)

Борт құрылғыларының шектелген ресурстарын ескере отырып хабар құрылымы ретінде «1 нұсқаны» таңдаймыз (сурет 2.10). МОСТ СМ1/ММ1 радиостанциясын пайдаланумен 160/460 МГц диапазонында жергілікті радиоканал арқылы жұмыс кезінде тарату коды сонымен бірге қауіпсіздік кодының функцияларын атқаратын болады. Желілік тораптарды (GSM-R/TETRA) пайдалануға көшу кезінде 2-4 нұсқа хабарларының құрылымын қолдану мүмкін болады.

Мәліметтер жіберу кезінде қорғаныс үшін ең кеңінен қолданылатын кодтар желілік кодтар класына жатады. Желілік кодтар белгілі бір санды, атап айтқанда d-1 (d Хэмминг қашықтығын құрайды) дара биттік қателіктерді сенімді анықтауды қамтамасыз етеді. Бұдан жоғары қателіктер тек белгілі бір ықтималдылықпен анықталады. Көптеген жағдайда қауіпсіздік кодына тәуелсіз дара биттік қателіктерді анықтау талабы ғана қойылмайды. Қолданылатын қауіпсіз емес тарату жүйесі (GSM, TETRA, DECT) мұндай қателіктерді анықтаудың өзіндік механизмдерін қамтып үлгерген. Қауіпсіздік коды кедергі әсері тарату жүйесі кодының мүмкіндігі жеткіліксіз болғанда немесе тарату жүйесі қателіктер арқылы жұмыс істеген жағдайда өзінің белсенділігін көрсетуі тиіс. Екі жағдайда да тек тәуелсіз дара биттік қателіктер орын алады деп есептеуге болмайды. Бақылау өрнегін есептеудің бұл әдісінде полиномдық арифметика қолданылады, яғни екілік сандар екілік коэффициенттері бар ресми полиномдармен көрсетіледі [72]. Бұл әдіс дара, екілік қателіктер, еркін тақ еселі қателіктер, сондай-ақ топтық түрдегі қателіктер, яғни бөлгіш ұзындығынан аспайтын топ ұзындығымен қатар келе жатқан биттердің кейбір санының бұрмалану түрінде көрінетін қателіктер табылатындығына кепілдік береді.

Мәліметтер тарату мысалын қарастырайық. Жергілікті радиоканал қолданатын стационарлық құрылғы кезек тәртібімен әрекет ету аумағында орналасқан локомотивтерге хабар жібереді де, локомотивтерден хабар алу жөнінде хабарлама түбіртектерін алады. Қосымша әрбір таратуда локомотив телеграммасында қамтылатын ақпараттың ұзындығы $M=252$ бит хабары ұзындығы $N=48$ CRC әдісімен кодталады (анықтау қабілеттілігі $3,6 \cdot 10^{-15}$ құрайды), пойызға радиоканал арқылы 900 бит/сек (яғни сағатына 10800 хабар) жылдамдықпен жіберіледі делік. Бұл ретте жіберу үрдісі таратудың қайталау механизмін және таратудың қайталау мерзімінде бортта алынатын мәліметтерді сәйкес кешігуші есепке алуды қарастырады.

Қайталауды есепке алумен тарату кезінде қауіпті істен шығу егер бірінші әрекет кезінде бақылау жағдайларының тексеруімен таратуда қателік анықталмаса, немесе бірінші қателік табылып, ал екіншісі табылмаса, немесе алғашқы екеуі анықталып, үшіншісі табылмаса және т.б. жағдайда туындайды.

CENELEC EN 50159 стандартына сәйкес [69, 70] CRC кодын қолданудың жалпы тиімділігі анықталмаған қателік ықтималдылығымен 2^{-N} бағаланады, мұндағы N – код разрядтылығы. Істен шығу ағыны параметрінің кеңінен таралған мәні 10^{-3} , 10^{-4} құрайды және жіберілетін тарату битіне бұрмаланудың орташа ықтималдылығын (дара болуы міндетті емес) ескереді. Бұл жерден ұзындығы $M+N$ таратудағы қателік ықтималдылығы (дара болуы міндетті емес) $(M + N) \cdot 10^{-4}$ формуласы бойынша есептеледі.

Олай болса, хабар жіберу кезінде қауіпті істен шығу ықтималдылығы құрайды:

$$P_{оп} = 2^N P_1 + 2^{N-1} P_1^2 + \dots + 2^1 P_1^L = 2^N P_1 \frac{1 - P_1^L}{1 - P_1} \quad (2.1)$$

мұндағы

$L=8$ – жол берілетін қайталаулар саны (МККТТ нормаларына сәйкес);

$P_1 = (M + N) \cdot 10^{-4}$ – жұмыс циклінде хабардың жіберілмеу ықтималдылығы.

Қауіпті істен шығу қарқындылығы мына формула бойынша есептеледі:

$$\lambda_{оп} = 10800 \cdot P_{оп} = 10800 \cdot 1,57 \cdot 10^{-16} = 1,7 \cdot 10^{-12} \text{ 1/ч} \quad (2.2)$$

Бұл әдістің артықшылықтарына мыналарды жатқызуға болады: іске асыру қарапайымдылығы, жоғарғы өнімділік, қателіктер анықтаудың жоғары ықтималдылығы. Кемшіліктері: белгілі бақылау саны кезінде нәтижесінде дұрыс мән шығатындай етіп мәліметтерді «түзететін» бағдарламаны жазу аса қиындық тудырмайды [73-75]. «Циклдік артық код» әдісі мәліметтердегі кездейсоқ өзгерістерді сенімді түрде анықтайды, бірақ ақпарат рұқсат етілмеген түрде өзгерген жағдайда тиімділігі жеткіліксіз болып саналады.

Қосымша канал ретінде ақпарат таратудың ашық радиоканалдарын пайдалануды есепке ала отырып, CENELEC еуропалық стандарт терминологиясына сәйкес қосымша кодты – хэширлеу алгоритмдерінің көмегімен қалыптасқан қауіпсіздік кодын қолдану қажет. Мұндай алгоритмдер арасында ең белгілі болып танылған [76]: MD5 алгоритмі (хэш ұзындығы – 128 бит), авторы Ron Rivest, RSA ашық кілті бар шифрлау алгоритмін құрушы; SHA-1 алгоритмі (хэш ұзындығы – 160 бит).

2.5.2 TETRA стандарты жүйесінің ақпарат қауіпсіздігі

TETRA стандартының сандық технологиялық радиобайланыс жүйесінде ақпарат қауіпсіздігі және ақпаратты қорғау сұрақтары ең өзекті мәселелердің бірі болып табылады. Бұл пойыздар қозғалыс қауіпсіздігін басқару және қамтамасыз ету жүйелері секілді сыни үрдістер мен жүйелерге қойылатын жоғары талаптармен байланысты.

TETRA стандартының сандық технологиялық радиобайланыс (СТР) жүйесінде ақпарат қауіпсіздігін қамтамасыз етудің негізгі мақсаттары мыналар:

- ақпарат қауіпсіздігі (құпиялылығы, бүтіндігі және қолжетімділігі) бұзылған жағдайда ақпарат қаупін, экономикалық және басқа да шығын түрлерін минималдау;

- TETRA стандартының СТР координаталық басқару және интервалды реттеу, пойыздар қозғалысы қауіпсіздігін қамтамасыз ету деңгейлерінің элементі ретінде пайдалану кезінде қозғалыс қауіпсіздігінің қажетті деңгейін ұстап тұру (ERMTS 2-ші және 3-ші деңгейлері).

Қорғалатын ақпараттық актив ретінде саналады:

- түрлі жүйе саласында қолданылатын ақпарат – функционалдық қауіпсіздікті анықтайтын жауапты командалар; «ҚТЖ «ҰК» АҚ-ның коммерциялық құпиясын құрайтын басқарушы және технологиялық ақпарат, жүйенің қызметтік ақпараты;

- СТР ақпараттық-коммуникациялық инфрақұрылымы – жылжымалы радиобайланыс радиоканалы; мобильдік, локомотивтік және стационарлық терминалдар, базалық бекеттер; желілік интерфейстер, базалық бекет бақылағыштарының, коммутациялау және басқару орталықтарының бағдарламалық-аппараттық кешендері; синхрондау желісінің каналдары және құрылғысы, СТР басқару жүйесінің каналдары және құралдары [77].

Қорғау маңызы жоғары негізгі жауапты командаларға мыналар жатады:

- машинист іс-әрекетіне тәуелсіз ДСП/ДНЦ бұйрығы бойынша пойызды мәжбүрлі тоқтату;

- диспетчер бұйрығы бойынша пойызға тыйым салушы сигналды жүріп өтуге рұқсат беру;

- локомотив машинистінің пойыз диспетчерін апаттық (шұғыл) шақыруы;

- екі жақты автоматты блоктау жүйесімен жабдықталған аралықта қозғалыс бағытын апаттық ауыстырудың көмекші режимін қосу;

- бұрмалық телімнің жалған бос еместігі кезінде бұрманы көмекші аудару;

- маршрутта тұйықталған жолдық және бұрмалық телімдерді жасанды ажырату.

TETRA стандартының СТР жүйесін ақпараттық қорғаныс объектісі ретінде талдау оның ақпарат қауіпсіздігінің бірқатар осал жерлері мен қауіптерін анықтады. Оның негізгілері мыналар:

- хабарды тікелей ұстап алу, трафикті талдау, рұқсат етілмеген кодтан ажырату және хабарды дешифрлау;

- радиоканалдарға бағытталған кедергілердің әсері және ақпараттық қайта жүктеудің құрылуы;

- жалған хабарлар, басқару командаларын және қызметтік ақпарат тарату;

- кері электромагнитті сәулелену мен көздеу арқылы техникалық ағын каналдарында ақпаратты, дауыс ақпаратын ұстап алу;

- базалық бекет бақылағыштарының, коммутациялау және басқару орталықтарының бағдарламалық-аппараттық кешендерінде зиянды бағдарламалар мен бүлдіруші әсерлерді енгізу;

- мобильдік және стационарлық құрылғыны рұқсатсыз пайдалану, қозғалысты көздеу, мобильді құралдарды ұрлау, радиобайланыс құралдарын бұзу және істен шығару.

Қауіптерді бейтараптандыру және ақпараттық ресурстарды рұқсатсыз пайдаланудың алдын алу үшін TETRA стандарты СТР жүйесінің ақпаратын қорғау және ақпарат қауіпсіздігін қамтамасыз ету принциптері, талаптары және ұсыныстары әзірленген [78].

Ақпарат қауіпсіздігін қамтамасыз ету принциптері мынада:

- қорғаныс нормативтік-құқықтық, ұйымдық-әкімшілік және бағдарламалық-техникалық шараларды пайдалануды қарастыратын кешенді сипатқа ие болуы тиіс;

- ақпарат қауіпіне барабар қорғаныс деңгейі бар жүйе құруды көздейтін қорғаныстың экономикалық мақсатқа сай болуы, сондай-ақ қолданушы құрылғысының бірдей болуын қосатын бағдарламалық-техникалық және криптографиялық механизмдерді тиімді пайдалану;

- жүйеде тіркелген қолданушыларды (абоненттерді) сәйкестендіру және аутентификациялау;

- мобильдік және базалық бекеттер арасында радиоканал арқылы жіберілетін ақпаратты шифрлау (трафикті криптографиялық қорғау);

- абоненттердің құпиялылығы және т.б.;

- жаңа қауіптің пайда болуына икемді әрекеттің қамтамасыз етілуі, рұқсатсыз әрекеттерді жедел анықтау және алдын алу.

Төрт ішкі жүйе аясында келесі талаптар орындалуы тиіс деп қарастырылады.

Кіруді басқару ішкі жүйесі үшін – қолданушы құрылғыны сәйкестендіру, қолданушыларды сәйкестендіру және аутентификациялау, кіру құқығын шектеу, сондай-ақ ақпарат ағындарын басқару.

Тіркеу және есепке алу ішкі жүйесі үшін – оқиғаларды мониторингтеу және тіркеу (хаттамалау), шабуылдарды анықтау, рұқсатсыз кіру әрекеттері жөнінде белгі беру және ақпараттық активтерді (ресурстарды) пайдалану, оқыс оқиғаларды тергеу, кіру субъектілері құзіреттерінің өзгеруі.

Криптографиялық ішкі жүйе үшін – жауапты ақпаратты (жауапты командаларды) шифрлау және трафикті кодтық қорғау, TETRA стандартындағы басқа криптографиялық механизмдерді пайдалану,

Бүтіндікті қамтамасыз ету ішкі жүйесі үшін – жіберілетін және өңделетін жауапты ақпараттың (жауапты командалардың) бүтіндігі, базалық бекет бақылағыштарының бағдарламалық құралдары, коммутациялау ішкі жүйелері, желіні бақылау және басқару, топтық коммутациялау мәліметтерін тарату, есептеуіш және коммуникациялық құралдарды, ақпарат тасымалдаушыларды физикалық қорғау, қауіпсіздік режимін қамтамасыз етуге ақпарат қорғау әкімшісінің (қызметінің) болуы; сертификатталған қорғаныс құралдарын пайдалану, оларды периодты түрде тестілеу және қалпына келтіру құралдарының болуы.

TETRA қондыру жүйесінде аутентификациялау және шифрлау функциялары бар мобильді терминалдар мен құрылғы нұсқаларын қолдану қажет. Бұл ретте құрылғы TETRA желісінде қауіпсіздік режимдерін басқару бойынша құжаттама мен бағдарламалық қамтамасыз етудің толық орыстандырылған жинағымен жабдықталуы тиіс. Жүйені функциялаудың және басқарудың бағдарламалық құралдары анықталған ақаулардан кейін жүйенің жұмысын қалпына келтіру үшін қосымша көшірмелерге ие болуы қажет.

Сонымен бірге TETRA жүйесінің құрылғысы және бағдарламалық қамтамасыз ету жарияланбаған мүмкіндіктердің жоқтығы жөнінде сертификаттаудан өтуі, магистральді және технологиялық сегменттер желісіне қосылу және кіру каналдарын ұйымдастыру кезінде желіаралық өзара әрекеттесуді қорғау қамтамасыз етілуі қажет.

Пойыздар қозғалысы жылдам және жоғары жылдам телімдерде қозғалыс қауіпсіздігін басқару және қамтамасыз ету жүйелерінің ерекше жауапты командаларын жіберу кезінде ақпарат қауіпсіздігін TETRA стандарты желісінің қорғаныс жүйесіне қойылған қолданбалы (пайдаланушы) деңгейде қосымша қорғаныс механизмдері құруы қажет [79].

Ол үшін «нүкте-нүкте» режимінде дыбыстық ақпарат және қолданушылардың белгіленген категориялары арасындағы мәліметтерді қорғауды қамтамасыз ететін кіріктірілген сертификатталған ақпаратты аутентификациялау және криптографиялық қорғау элементтері бар арнайы әзірленген жер және локомотивтік терминал құрылғыларын қолданған жөн. Бұл құралдар ГОСТ 28147–89, ГОСТ Р 34.10-2001, ГОСТ Р 34.11–1994 криптографиялық қорғаныстың ресейлік стандарттарын қанағаттандыруы тиіс.

Сонымен бірге қауіпсіздік әкімшілігінің қызметі «ҚТЖ» ҰК» АҚ технологиялық байланысын мониторингтеу және әкімшілеудің Бірыңғай жүйесі қызметімен тығыз әрекетте жұмыс істеуі қажет. Бұл ретте сыни технологиялық және басқарушы ақпаратты қорғау арқылы жіберу бойынша нұсқаулықтар әзірленіп, лауазымды тұлғалардың функционалдық міндеттері анықталуы тиіс.

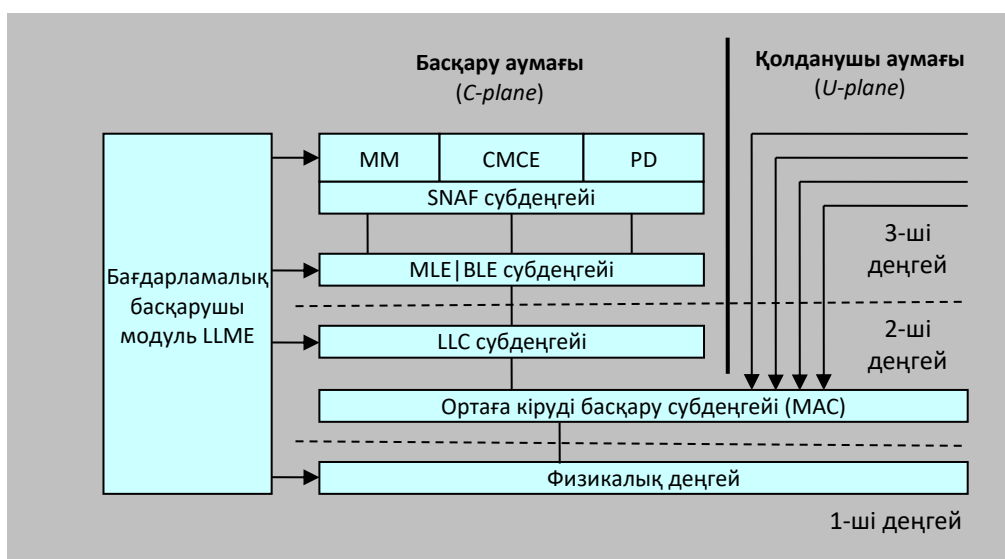
Қауіпсіздік әкімшілігі қызметінің негізгі тапсырмалары мыналар: ақпарат қауіпсіздігі бойынша әрекет етуші нормативтік базаны орындау, желіге кіруді басқару; бағдарламалық қамтамасыз етуді периодты түрде жаңарту, бағдарламалық және техникалық құралдарды конфигурациялау, қосымша көшірмелеу және жүйенің жұмысқа қабілеттілігін автоматты қалпына келтіру, оқиғалар журналын талдау, мүмкін болатын ақаулар жөнінде куәлік ететін жазбаларды анықтау және тергеу жүргізу, TETRA жүйесінің арнайы параметрлерін басқару, соның ішінде радиоинтерфейсте шифрлау режимін қосу/ажырату және TMSI уақытша нөмірін ауыстыру режимдерін таңдау, криптографиялық мәліметтер қорғау кілттерінің өмірлік циклін басқару.

TETRA стандартының СТР жүйесін жобалауға, енгізуге және пайдалануға қатысатын қызметкерлер қойылған талаптарды орындауға жеткілікті білімге және тәжірибеге ие болуы тиіс. Ақпарат қауіпсіздігін қамтамасыз ету функцияларын атқаратын қызметкерлер арнайы курстарда тұрақты оқудан өтіп тұрулары қажет. Қызмет көрсетуші тұлға ақпарат

қауіпсіздігі бойынша нормативтік құжаттармен танысқаннан (қол қойып) кейін ғана жұмысқа кірісе алады.

2.6 TETRA стандартының жүйелік хаттама моделі

TETRA стандартында радиоинтерфейсті сипаттау түрлі функциялар мен үрдістер мобильді, базалық бекеттер мен диспетчер пульттерінің өзара әрекеттесу хаттамаларының иерархиялық жүйесін құрайтын жүйелік хаттаманың түрлі деңгейімен сәйкестендірілетін модель негізінде құрылған. Жүйелік хаттама архитектурасы (өзара әрекеттесу хаттамаларының жиынтығы) 2.14 суретте көрсетілген [80].



Сурет 2.14 – TETRA жүйелік хаттамасы архитектурасының моделі

TETRA жүйелік хаттамасы үш деңгейлі болып табылады, яғни жүйедегі барлық өзара әрекеттесу хаттамаларының жиынтығын сигнал өңдеу сипаты бойынша 3 деңгейге бөлуге болады:

- 1-ші деңгей – физикалық;
- 2-ші деңгей – каналдық;
- 3-ші деңгей – желілік.

2-ші деңгейден бастап қызмет көрсетілетін мәліметтер түрі бойынша жүйелік хаттама 2 бөлікке (аумаққа) бөлінеді: қолданушы аумағы (U-plane) және басқару аумағы (C-plane). U-plane ақпараттық мәліметтерді тасымалдау үшін арналған және адрестеу құралдары болмайды. C-plane LLME басқарушы бағдарламалық модуль көмегімен адрестеу мүмкіндігі бар басқарушы хабарлармен алмасуды қамтамасыз етеді.

1-ші деңгей

Физикалық деңгей жүйелік хаттаманың төменгі деңгейі болып табылады және жіберуге және қабылдауға жарамды биттер мен символдардан (дибиттерден) тұратын физикалық топтарға қызмет көрсететін интерфейсті сипаттайды. Физикалық деңгей келесі функциялар құрамын іске асырады:

- радиоканалмен байланысты функциялар;
- биттер мен символдарды өңдеу функциялары;
- топтарды ұйымдастыру функциялары.

Радиоканалмен байланысты функциялар мыналарды қосады:

- модуляция/демодуляция;
- қабылдау және тарату режимдерін ауыстырып қосуды басқару;
- радиожиіліктік параметрлерді басқару:

а) каналдарға жиілік орнату;

б) радиосигналдарға шығыс деңгейін индикациялау.

- радиотехникалық параметрлерді дәл реттеу;

а) жиілікті түзету (синхропакетте орналасқан арнайы түзетуші тізбек көмегімен мобильді бекеттің тіреуіш жиілігін базалық бекетпен синхрондау);

- қуатты басқару (таратушы каналда жіберілетін базалық бекет параметрлеріне сәйкес мобильді бекет қуатының деңгейін, және мобильді бекетте орындалатын сигнал деңгейін өлшеуді басқару).

Биттер мен символдарды өңдеу функциялары символдық (тактілік) синхрондауды жүзеге асырады және физикалық топтың шекарасын (басы және соңы) анықтайды. Физикалық топтарға синхрондау үшін қабылданатын символдарды дәл анықтауды қамтамасыз ететін арнайы оқытушы синхротізбектер қосылады, бастапқы синхрондау кеңейтілген оқытушы тізбек көмегімен қамтамасыз етіледі [81].

Топтарды ұйымдастыру функциялары қосады:

- каналдық деңгеймен (МАС субдеңгеймен) мәлімет алмасу, яғни жіберу кезінде – 2-ші деңгей ақпаратын, сондай-ақ 1-ші деңгейлі ерекше ақпаратты физикалық топтың сәйкес орындарына орналастыру, қабылдау кезінде – 1-ші деңгейлі ерекше ақпаратты шығару, ақпараттық блоктарды қалпына келтіру және оларды 2-ші деңгейге айналдыру;

- кодтау/кодтан ажырату ұялы туын орнату;

- шифрлау/шифрдан ажырату.

2-ші деңгей

Каналдық деңгей логикалық жалғануларды басқарады және физикалық орта (радиоресурстар) мен желілік процедуралар арасындағы бөлім шекарасы болып табылады. Ол 2 субдеңгейге бөлінеді:

- MAC (Medium Access Control) – ортада кіруді басқару;

- LLC (Logical Link Control) – логикалық буынды басқару.

MAC субдеңгейі радиоканалдарға кіруді және радиоресурсты таратуды басқарады. MAC келесі функциялар тобын іске асырады:

- каналдық кодтау;

- радиоканалдарға кіруді басқару;

- радиоресурстарды әкімшілеу.

Каналдық кодтауға келесі функциялар жатады:

- кезектесу/кезектесуді болдырмау, яғни радиоканалдарда туындайтын топтық қателіктерді жою мақсатында бір немесе екі блок шамасында биттерді қайта реттестіру;

- қателіктерді тікелей түзету жолымен ақпаратты қорғау мақсатында пайдаланылатын 2/3 жылдамдықпен түйінді кодтау (FEC);

- белгілі бір қателіктер санын анықтауға және оларды түзету шараларын қабылдауға мүмкіндік беретін артық кодты циклдік кодтау (CRC).

Радиоканалдарға кіруді басқару келесі функцияларды қосады:

- кадрларды синхрондау, яғни мультикадр аясында кадрларды нөмірлеу тізбегін бақылау;

- кездейсоқ кіру процедураларын басқару;

- хабарларды фрагменттеу және жинау;

- мәліметтер тобының барлық құрамдас бөліктерін қалыптастыру үшін логикалық каналдарды мультиплексирлеу/ демуплексирлеу;

- мультикадрды қалыптастыру, яғни кадрларды мультикадрға біріктіру.

Радиоресурстарды әкімшілеу құрамы әр мобильді немесе базалық бекет үшін жеке анықталатын функциялар тобын құрайды, және желілік деңгейге шықпай кез келген уақытта радиоресурсты тиімді басқаруды қамтамасыз етеді. Бұл топ функцияларының толық жинағы мыналарды қосады:

- қателіктер коэффициенттерін биттер (BER) және блоктар (BLER) бойынша өлшеу;

- байланыс желісінде жоғалуды есептеу, қызмет көрсетуші аумақты мониторингтеу, көрші аумақтарды мониторингтеу және сканерлеу;

- жеке, топтық және жалпы шақырулар мекен-жайларын басқару;

- жиілік пен уақыт интервалын таңдау;

- байланыс каналдарын беру;

- жіберу режимі аяқталғанға дейін басқарушы және дыбыстық ақпаратты буферде сақтау.

LLC субдеңгейі логикалық буынды басқарады, яғни мобильді және базалық бекеттер арасында «нүкте-нүкте» типті логикалық каналдар ұйымдастырады. LLC-те логикалық каналдардың екі түрлі типіне қызмет көрсету іске асырылуы мүмкін:

- қосуды орнату сатысын талап етпейтін базалық логикалық канал;

- қызмет көрсету жағдайын жақсарту үшін пайдаланылатын «хабарлаушы» логикалық канал.

LLC субдеңгейі келесі негізгі функцияларды қамтамасыз етеді:

- желілік деңгей MLE/BLE субдеңгейімен мәлімет алмасу;

- логикалық каналды (базалық немесе хабарлаушы) басқару;

- мәлімет таратуды жоспарлау;

- қайта жіберу;

- сегменттеу және қалпына келтіру (тек хабарлаушы каналда);

- ағынды басқару (тек хабарлаушы каналда);

- мәліметтер қабылдауды растау (каналдың екі типінде де);

- MAC субдеңгеймін логикалық каналды беруді келісу (тек хабарлаушы).

3-ші деңгей.

Желілік деңгей желілік процедураларды басқару үшін арналған. Ол екі субдеңгейге бөлінеді:

- MLE/BLE (Mobile/Base Link control Entity) – мобильді және базалық бекеттер арасындағы байланысты басқару үшін;

- SNAF – субжеліге кіруді қамтамасыз ету үшін.

MLE/BLE субдеңгейі тек C-plane басқару аумағында қолданылады және келесі функцияларды қамтамасыз етеді:

- хаттаманы тану;
- базалық және мобильді бекеттер тобында қосылуды орнату;
- сәйкестендіруді басқару;
- қызмет көрсету шарттарын басқару;
- кең таратылатын ақпаратты қабылдау және жіберу.

SNAF субдеңгейі мыналарды басқаруды қамтамасыз етеді:

- мобильділікті (MM – Mobile Management);
- каналдармен коммутациялау режимін (CMCE – Circuit Mode Control Entity);
- мәліметтер тобын (Packet Data).

Мобильділікті басқару режимі мобильді бекеттерді жылжытумен байланысты процедураларды қамтамасыз етеді: желіні таңдау, аумақты таңдау, тіркеу, аутентификациялау, қолданушыны бекіту [82].

Режимді басқаруды топтармен коммутациялау тапсырмаларының кешені қызметтің үш тобын қолдайды:

- қысқа хабарлар жіберу;
- шақыруларды басқару;
- қосымша қызметтер.

Мәліметтер тобын басқару режимі екі түрлі хаттамаға сәйкес топтар тарату қызметін қолдайды:

- қосылуды орнатуға бейімделген желілік хаттама (CONP);
- қосылуды орнату болмайтын арнайы желілік хаттама (S-CLNP).

3 KTCS ЖҮЙЕСІ МЕН БАСҚАРУ ОРТАЛЫҚТАРЫ АРАСЫНДА СЫМСЫЗ МӘЛІМЕТТЕР ЖІБЕРУДІ ҚАМТАМАСЫЗ ЕТЕТІН TETRA САНДЫҚ РАДИОКАНАЛ АРҚЫЛЫ МӘЛІМЕТТЕР ТАРАТУ КЕЗІНДЕ КІЛТТЕРДІ АУТЕНТИФИКАЦИЯЛАУ ЖӘНЕ ТҮРЛЕНДІРУ

Соңғы онжылдық телекоммуникациялық салада, соның ішінде теміржол көлігінде белсенді технологиялық дамуды көрсетті. Техникалық ерекшеліктерді өзекті ету үшін «ҚТЖ «ҰК» АҚ-да теміржол көлігінде инновацияларды іске асыру бойынша теориялық және тәжірибелік зерттеулер жүргізеді, бұл оларға жыл сайын ерекшеліктерін жаңартуға мүмкіндік береді.

Бұл ерекшеліктерде ақпараттық қауіпсіздік бөлімі маңызды рөл ойнайды. Жыл сайын ақпараттық және басқарушы жүйелердің киберқауіпсіздігі бойынша зерттеулер саны өсіп келеді, бұл теміржол жүйелері үшін ақпараттық қауіпсіздік саласында жаңа зерттеу бағыттарын анықтауға итермелейді.

Ұлттық жүйенің негізгі компоненттері KTCS Қазақстандық пойыздар қозғалысын басқару жүйесі және пойыздар мен басқару орталықтары арасында сымсыз мәліметтер жіберуді қамтамасыз ететін TETRA сандық байланыс жүйесі болып табылады. TETRA байланыс желісі ашық байланыс желілеріне жататындықтан, EN 50129-2 стандартының талаптарына сәйкес [40] ашық байланыс желілерін қолданумен қозғалыс қауіпсіздігін қамтамасыз етумен байланысты қосымшаларда жүйені енгізу, түрлендіру және хабар алмасу қаупінен қорғайтын арнайы құралдар пайдаланылуы қажет.

Қазіргі уақытта радиоканал арқылы ақпарат тарату үрдісінің тиімділігін арттыру үшін жіберілетін хабарларды аралас кездейсоқ кодтау көмегімен іске асырылған радиоканалдарды кодтық шулату әдісі әзірленген және кеңінен қолданылады.

Сандық жүйелер құру кезінде бір уақытта ақпарат басқару және тарату радиоканалдарының кедергіден қорғалуын және ақпарат қауіпсіздігін жоғарылатуды қамтамасыз ететін нақты кодтау сұлбалары мен түзетуші кодтарға тәуелсіз нәтижелер алуға мүмкіндік беретін кодтық шулатуы бар радиоканал арқылы ақпарат тарату үшін аралас код параметрлерін таңдау алгоритмі әзірленді [83].

Әрі қарай радиоканал арқылы мәліметтер тарату принципін қарастырамыз. Басқа жабық жүйелерге сипатты сандық мәліметтер таратудың баламалы тәсілдерінен келесідей айырмашылықтары бар [84]:

1. Шеңберлі құрылымы бар иерархиялық желі. Орталықтандыру компьютері басқарушы элемент ретінде шеңбер құрылымынан бөлінген, алайда барлық атқарушы элементтер сым (SHDSL) немесе талшықты-оптикалық кабель көмегімен түйіндік принцип бойынша жалғанады. «Нүкте-нүкте» принципі бойынша жұлдызша тәрізді жалғаулардың классикалық сұлбасынан көшу мына жағдайларға мүмкіндік береді:

- кабель қажеттілігін азайту;
- шеңбер көмегімен екі тәуелсіз мәліметтер тарату жолын қамтамасыз ету.

2. Екі тәуелсіз каналдан тұратын және орталықтандыру компьютерін объекталық бақылағыштар арқылы жол құрылғыларына жақын орналасқан топты басқаруды қамтамасыз ететін шеңберлермен жалғайтын Ethernet стандартының талшықты-оптикалық кабелі бар тіреуіш желісі. Артықшылықтың бұл типі физикалық каналдардың кез келгені зақымданған кезде жүйенің орнықтылығына кепілдік береді. Тіреуіш желі ұзындығы ондаған және тіпті жүздеген километрге жетуі мүмкін.

3. Объекталық бақылағыштарға салынған диагностика тапсырмалары. Атқарушы сандық элементтерді тікелей жол құрылғыларының жанына немесе тіпті ішінде орналастыру арқасында, пост компьютері «алғашқы қолдан» басқару және бақылау объектілерінің күйі жөнінде толық ақпарат алады. Бұл ретте қарастырылатын мәліметтер тарату желісінде маңыздылық принциптерін қарай отырып, басқару/бақылау тапсырмаларын диагностикадан бөлу қажет.

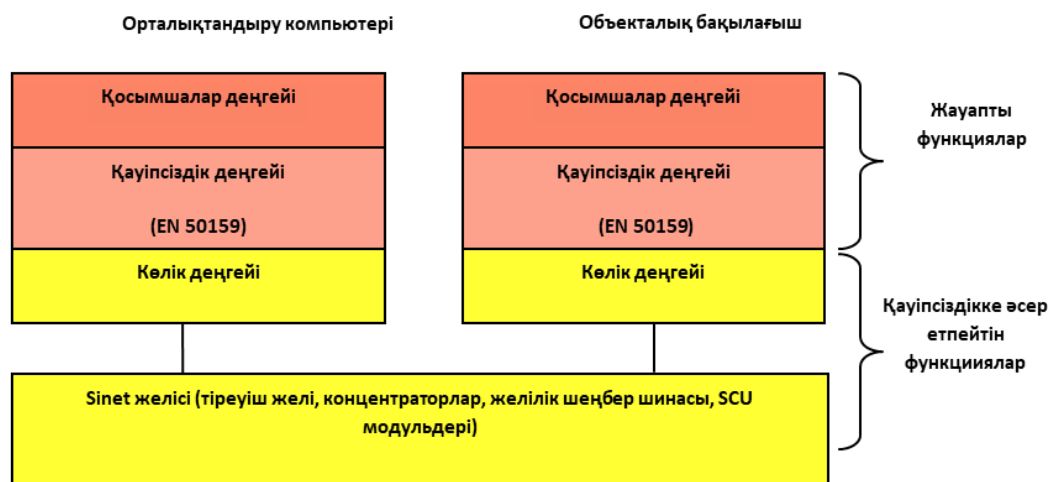
4. Әр басқарушы немесе атқарушы элемент алдындағы желілік модульдер. Олардың тапсырмасы нақты уақыт режимінде мәліметтер ағындарының таратудың жылдамдық бойынша маңызды каналын анықтау және маңызы төмен каналды жол құрылғыларынан диагностикалық хабар тарату үшін пайдалану болып табылады. Сонымен қатар, желілік модульдер тіреуіш желімен қосарланған жалғануды қамтамасыз етеді, хаттамалар (SHDSL үстінен Ethernet) түрлендіреді, сандық сигнал күшейткіштері бола отырып, мәліметтер тарату көлемі бойынша шектелген желілік шеңбер шинасында трафикті сүзгілейді, соның арқасында жоғары байланыс қашықтығы қамтамасыз етіледі.

5. Екі канал арқылы да команда жіберу кезінде атқарушы элементтің желілік модулі алғашқы хабарды алып, оның нөмірін тіркейді де, команданы орындайды. Ұқсас нөмірде қосымша канал арқылы кейін келетін екінші хабар желілік модульде өшіріледі.

6. Келешекте ТОВЖ тіреуіш желісі радиоканалға (мысалы GSM-R) ауыстырылуы мүмкін, ал желілік модульдер әрекет етуші радиотаратқыштарға қосылатын болады.

7. Заманауи энергия үнемдеуіш технологияларды дамытуды, сондай-ақ жергілікті электрмен қоректендірудің баламалы көздерін әзірлеуді есепке ала отырып, қоректендіруші желі бірте-бірте өзінің мәнін жоғалтады, және жергілікті энергия көздері посттан қашықтатылған құрылғылардың автономды жұмысы үшін жеткілікті болады.

Сандық орталықтандыру ішінде мәліметтер тарату кезінде кез-келген қате хабар немесе қате команда жүйені қауіпті күйге әкелуі мүмкін екендігін есте ұстаған жөн. Бұл жағдайды болдырмау үшін TCP/IP хаттамалар жинағында сигналдар жіберуге жауапты және қауіпсіздік жағынан маңызды емес аумақ белгіленеді. Осылайша, қауіпсіздіктің жауапты функциялары қосымшалар деңгейінде болады, ал көліктік деңгей тіреуіш желімен, желілік шеңбер шинасымен және желілік модульдермен (сурет 3.1) бірге мәліметтер таратудың сенімділігі жоғары каналының тапсырмаларын орындайды [85, 86].



Сурет 3.1 – Қауіпсіз мәліметтер таратудың көпдеңгейлі моделі

Сандық компьютерлік пойыздарға белгі беру жүйесін құрайтын Қазақстандық пойыздарды басқару жүйесі (KTCS) заманауи темір жолдардың елеулі элементі болып табылады. KTCS темір жолды пайдалану қауіпсіздігін, тиімділігін және үнемділігін айтарлықтай арттыратын көптеген функцияларды ұсынады. Басқалардың арасында жүйе қамтамасыз етеді: кабина ішінде белгі беруді, пойызды автоматты қорғауды және жылжымалы құрамды басқаруды. Осы функциялар арқасында пойыздар жоғары жылдамдықта жұмыс істей алады, жолдың өткізу қабілеттілігі артады және адам қателіктерінің қаупі азаяды. KTCS темір жол мобильді байланыстың қолдаушы желісіне мұқтаж болуы негізгі себептерінің бірі болып табылады. Сондықтан TETRA-ны теміржол байланысының мүмкін болатын технологиясы ретінде бағалаудың негізгі критерилері мыналар:

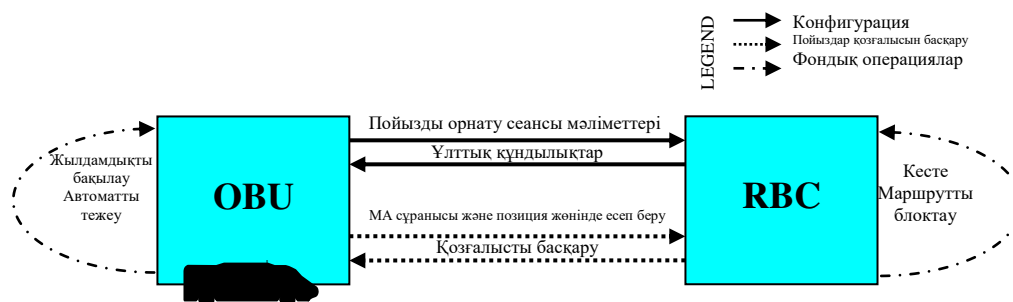
- TETRA KTCS жүйесіне ұсына алатын тарату сипаттамалары қандай. Бұл таратуға енгізу стратегиясы (базалық бекеттердің тығыздығы тұрғысынан), пойыздар қозғалыс жылдамдығы және трафиктің жұмыс істеуі қалай әсер етеді.

- Түрлі жағдайда таратудың кідіруі және мәліметтердің жоғалу ықтималдылығы тұрғысынан TETRA KTCS талаптарына сай келе ме.

- TETRA жалпы радиоресурстар арқылы сыни және сыни емес қосымшалар жеткізе ала ма

3.1 KTCS жүйесінде сандық байланыстың рөлі

KTCS – таратылған жүйе, оның негізгі логикасы екі элементке бөлінген: OBU және RBC (сурет 3.2). 2 тарауда айтылғандай, жүйеде көптеген элементтер бар, бірақ, олардың жұмысы мобильді байланыстың базалық технологиясына тікелей байланысты болмағандықтан, олар бұл зерттеу периметріне кірген жоқ.



Сурет 3.2 – KTCS элементтері арасында ақпарат алмасу

KTCS жұмысын бастау үшін, яғни пойыздар қозғалысын бақылау үшін, OBU және RBC арасында KTCS сессиясы қондырылуы қажет. Қондыру кезінде KTCS екі элементі де кезекті жұмысқа қажетті конфигурациялық параметрлермен алмасады. Мысалы, OBU пойыз жөнінде мәліметтер жібереді (мысалы, жүріс нөмірі, пойыз ұзындығы, машинист ID және т.б.). Кері бағытта RBC ұлттық мәндер жібереді (мысалы, әдеттегі жылдамдықтың шекті мәндері, кері қозғалыстан қорғау және т.б.) [87]. Сеансты орнату RBC және OBU мобильді желі арқылы мәлімет алмасуы тиіс болатын алғашқы жағдай болып табылады.

RBC пойыздар қозғалысын басқаруға және бақылауға жауап береді. Ол үшін RBC статикалық және динамикалық ақпаратқа қатысты өзекті жағдайға ие болуы тиіс [88]. Мұның негізін қалаушы бөлігі пойыздар позициясы болып табылады. Соған байланысты әр OBU бірнеше мәрте RBC-ке пойыздар позициясы жөнінде хабар жібереді. Көптеген жағдайда есеп беру қозғалысты басқару (ҚБ) сұранысымен бірігеді [88].

Позиция және басқа ақпарат (кесте, іліну маршруттары, пойыздың басқа позициялары) жөнінде есеп беру негізінде RBC пойыз үшін ҚБ шығарады. ҚБ жылдамдық шегі мен пойыз жүре алатын қашықтықты анықтайды. Пойыз қозғалысы кезінде жағдайы жөнінде есеп беру және ҚБ бірнеше мәрте жаңартылады да, OBU және RBC арасында ақпарат алмасу объектілері болып табылады.

KTCS жүйесі RBC және OBU арасында нағыз уақыт режимінде өзара әрекеттесуге негізделгендіктен, бұл екі элемент арасындағы тұрақты байланыс қажет болып табылады. RBC-OBU қосусыз KTCS негізгі функционалдылығын, яғни ҚБ таратуды, ішкі кабинкалық белгі беру және ATP қамтамасыз ету мүмкін болмас еді.

OBU-RBC коммуникациясы әсіресе ҚБ кеңейту секілді KTCS белгілі бір процедуралары кезінде сапаға қойылатын белгілі бір талаптарға сәйкес келуі тиіс. Егер пойыз қозғалыс соңында Басқару (ҚСБ) нүктесіне жақындаса, ал жаңартылған ҚБ алу мүмкін болмаса, онда пойыз жылдамдығын баяулатып, соңында тоқтауы қажет, себебі OBU жаңартылған ҚБ келмейінше машиниске ҚСБ өтуге мүмкіндік бермейді. Сондықтан OBU-RBC байланысының бұзылуы немесе ұзақ кідіруі кейін пойыздар қозғалысының барлық жүйесіне таралуы мүмкін және басқа пойыздар жүру кезінде әрі қарай кідіруге алып келуі мүмкін

пойыз қозғалысының кідіруін туғызады [89], бұл сонымен бірге жолдың рұқсат етілген өткізу қабілеттілігінің төмендеуіне әкелуі мүмкін [87].

ҚБ таратудың келтірілген үлгісі базалық коммуникациялық желісінің QoS KTCS жүйесінің QoS әсер етуін суреттейді. Бұл, өз кезегінде, теміржол пайдалану QoS әсер етеді (мысалы, жолдағы кідірулер тұрғысынан) [87]. Осылайша, Қазақстан Республикасының темір жолында KTCS жүйесін енгізу кезінде қауіпсіз және сенімді мәліметтер тарату тиімді және үздіксіз тасымалдау үрдісі негіздерінің бірі болып табылады.

Дегенмен, базалық коммуникация секілді байланыс маңыздылығына қарамастан, пойыздар қозғалыс қауіпсіздігі толықтай KTCS жүйесімен бақыланатындығын айта кеткен жөн [90]. OBU-RBC элементтері арасында байланыс толықтай жоқ болған жағдайдың өзінде KTCS процедуралары пойыздар қозғалысы апаттық жағдайдың туындауына әкелмейтініне кепілдік беруі қажет. Тәжірибеде бұл байланыс қалпына келтіріліп, RBC жаңартылған ақпарат бөлігін алғанға дейін пойыздар ескертулі түрде тоқтайтындығын білдіреді.

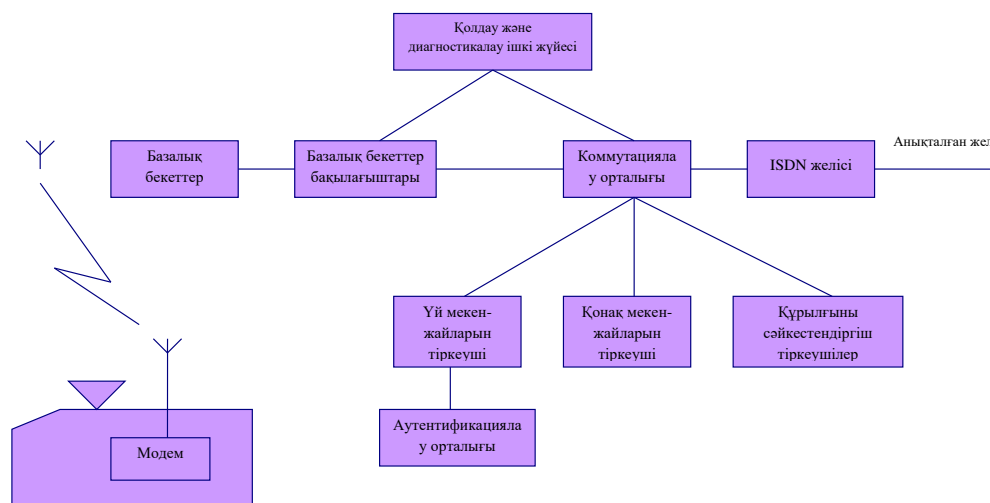
3.2 Байланыс желілерін зерттеу

Радиоканал негізінде ПҚИР жүйелерін құру кезінде басты сұрақтардың бірі байланыс желісін таңдау болып табылады. Ең кеңінен таралған байланыс желілері GSM, TETRA, DMR болып саналады. GSM және LTE технологиясы базасында GSM-R және LTE-R тек темір жолда қолдану үшін арналған мамандандырылған байланыс желілері құрылды, мұндағы R әрібі Railway (теміржол) дегенді білдіреді. Байланыс желілеріне қойылатын негізгі талаптар қосылудың жоғалу ықтималдылығы сағатына 10^{-2} төмен жоғарғы жұмыс сенімділігі, 500 мс аспайтын пакеттер жіберу кезінде аз кідіру уақыты, қозғалыс телімін жабу толық аумағы, тәулік бойы байланысқа қол жеткізу болып табылады. Сонымен қатар, базалық бекеттердің бірі істен шыққан жағдайда жұмыс сенімділігін арттыру үшін базалық бекетті жабу аумақтарын екілік жабу дұрыс болады. Сонымен бірге байланыс желісін таңдау кезінде енгізу кезіндегі капиталдық шығындарды есепке алу маңызды фактор болып саналады.

Құнын азайту мақсатында GSM қоғамдық желі базасында қозғалысты интервалды реттеу жүйесін құру әрекеттері жасалады [91].

ПҚИР жүйелерінде теміржол көлігінде қолдану үшін GSM желісі негізінде арнайы жобаланған GSM-R байланыс желісі кең қолданыс тапты. Бұл байланыс желісі EIRENE – MORANE ерекшеліктеріне негізделген және 500 км/сағ дейін жылдамдықта орнықты байланысқа кепілдік береді. Ерекшеліктерге сәйкес GSM-R мәліметтер мен дыбыс тарату үшін қорғалған платформа болып табылады. GSMR ерекшелігі топтық шақыруларды және кең таралатын байланысты, орналасқан жері бойынша байланысты жүзеге асыру мүмкіндігі болып саналады. GSM-R жұмысы 7-15 км қашықтықта темір жол бойында орналасатын базалық бекеттер негізінде құрылған, бұл базалық бекеттердің бірі істен шыққан жағдайда резервтеуді қамтамасыз етеді.

GSM-R байланыс жүйесінде уақытша канал бөлуі бар GMSK түрлендіру қолданылады. Мобильді желі архитектурасы 3.3 суретте көрсетілген.



Сурет 3.3 – GSM-R желісінің архитектурасы

GSM-R құрылғысының жұмыс режимін баптау құжатқа [9, б. 11] сәйкес жүзеге асырылады. 9600 бит/с мәліметтер тарату жылдамдығымен тікелей коммутациялау режимі пайдаланылады.

Құжатта [92] GSM-R желісінің жұмыс сапасына қойылатын талаптар келтірілген. Байланыс сапасының негізгі параметрлері 4.2 кестеде көрсетілген.

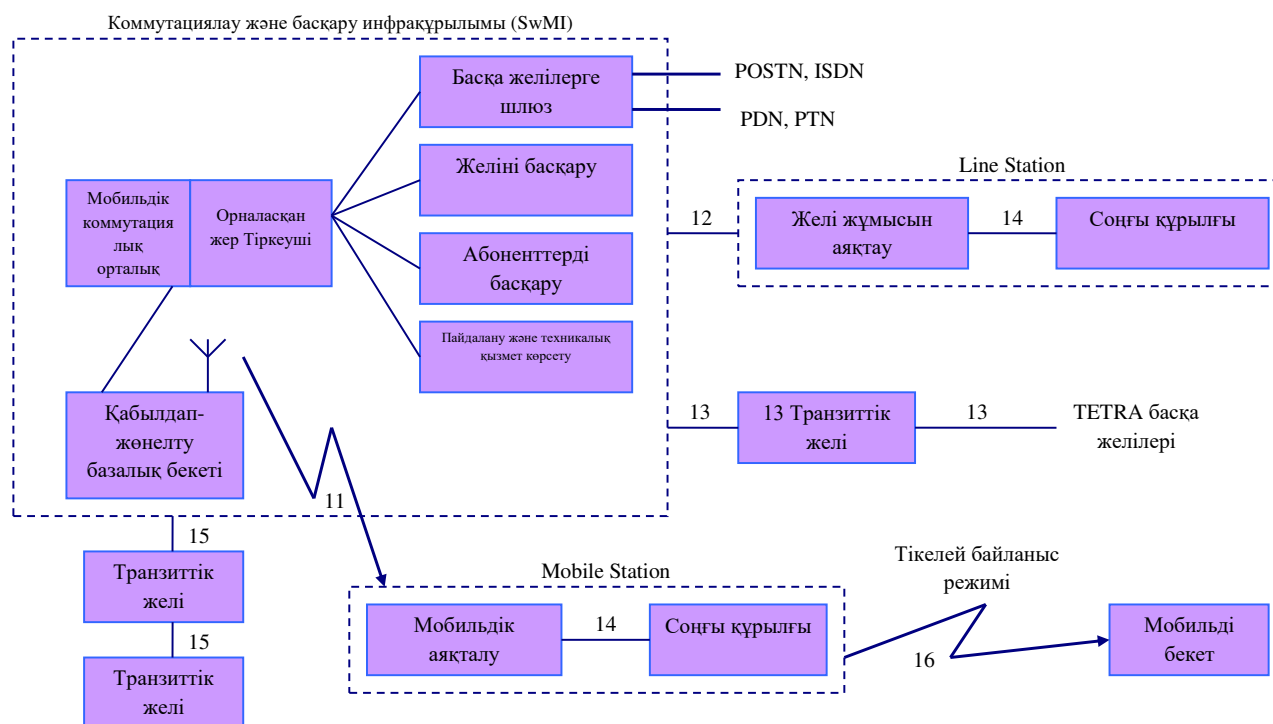
Кесте 3.1 – GSM-R желісіндегі байланыс сапасының параметрлері

QoS параметрі	Мәні
Мобильді шығыс қоңырауларын қосуды орнату кідіруі	<8,5с (95%), ≤10с (100%)
Қосуды орнату қателігінің коэффициенті	<10 ⁻²
Максималды өтпелі жіберу кідіруі (мәліметтер блогының 30 байты)	≤0,5с (99%)
Қосудың жоғалу жылдамдығы	<10 ⁻²
Жіберудің интерференция мерзімі	<0,8с (95%), <1с (99%)
Қате-тегін мерзім	>20с (95%), >7с (99%)
Желіні тіркеудегі кідіру	≤30с (95%), ≤35с (99%), ≤40с (100%)

3.1 кестеде көрініп тұрғандай, 100 сағат ішінде бір реттен де аз байланыс үзілуі орын алады (Connection loss rate параметрі). Сондай-ақ тек 99% жағдайда 30 байт жіберу уақыты 0,5 секундтан аз болады, яғни жіберу уақыты 0,5 секундтан көп жағдайлар болуы мүмкін. Кідірулер мен байланыстың үзілу жағдайларын бақылау үшін байланыс жүйесі жұмысының ақауларын реттеуге қабілетті арнайы хаттама қажет болады.

Әрі қарай дыбыстық байланысты, мәліметтер таратуды қамтамасыз ететін және арнайы қызметтер мен ірі корпорацияларда бүткіл әлемде кең қолданыс

тапқан TETRA (Terrestrial Trunced Radio) радиобайланыс желісін қарастырамыз. Еуропалық телекоммуникациялық стандарттау институты (ETSI) 1995 жылы TETRA стандартының алғашқы нұсқасын жариялады. TETRA желісі көрші каналдарды 25 кГц жолақпен бөлу арқылы елге байланысты 300 – 500 МГц жиілік жолағында ережеге сай каналдарды уақытша бөлу принциптері негізінде жұмыс жасайды. Тасымалдау жиілігінің төменгі диапазоны GSM-мен салыстырғанда базалық бекеттер жұмысының үлкен радиусын қамтамасыз етеді. 3.4 суретте TETRA байланыс желілерінің желілік инфрақұрылымы келтірілген.



Сурет 3.4 – TETRA желілік архитектурасы

TETRA желісі сонымен бірге байланысты үзбей бір базалық бекеттен екіншісіне көшуді қамтамасыз етеді. TETRA желісінде мәліметтер тарату жылдамдығы 7,2 кбит/с құрайды, ал шифрлау пайдалану кезінде 4,8 кбит/с немесе 2,4 кбит/с дейін азаяды, бұл желінің функционалдық мүмкіндіктерін қатты шектейді. TETRA желісі үш режимде жұмыс істей алады: каналдарды комутиациялау, топтық тарату және SDS қысқа хабарлар тарату. 3.2 кестеде [33, б. 59] сәйкес GSM-R және TETRA радиобайланыс желілерін салыстыру келтірілген.

Сондай-ақ [33, б. 60] TETRA желісінде каналдарды комутиациялау арқылы мәліметтер тарату әдісінің болуы, радиобайланыс желісіне RBC қосу үшін ISDN желісінің PRI интерфейсі болуы, сонымен бірге қосуды орнату ұзақтығы (95% қоңыраулар үшін 5 секундтан кем), екі шеткі құрылғылар арасында мәліметтер таратудың максималды кешігуі (0,5 секундтан артық емес), қосылудың үзілуін анықтау уақыты (1 секундтан артық емес) бойынша талаптарды орындау TETRA желісін жылжымалы құрамды басқару тапсырмалары үшін пайдалануға мүмкіндік беретіндігі көрсетіледі. TETRA

желісін қолдану нұсқалары әр түрлі, мысалы, [93] жұмыс режимдерін салыстыру кезінде басқару тапсырмаларының ең жақсысы SDS тарату режимі қабылданған, Bombardier компаниясы өзінің жобаларында TETRA желісін топтық тарату режимінде пайдаланады.

Кесте 3.2 – GSM-R және TETRA радиобайланыс желілерін салыстыру

Көрсеткіш	GSM-R (Еуропалық электр байланысын стандарттау институты)	TETRA (Еуропалық электр байланысын стандарттау институты)
ETSI стандарты жарияланған жыл	1997ж. басы	1995ж. (алғашқы жариялану)
Қолданылатын жиіліктер, МГц	876–880, 921–925, 1800	150, 380–400, 410–430, 450– 470, 870–876, 915–921
Түрлендіру тәсілі	Минималды жиіліктік ығысуы бар Гаустық (GMSK)	$\pi/4$ фазалық ығысуы бар дифференциалдық квадраттық фазалық манипуляция ($\pi/4$ DQSPK)
Каналдық өткізу жолағының әдеттегі ені	200 кГц жиілікте 8 канал	25 кГц жиілікте 4 канал
Каналдар арасындағы интервал (60 дБ деңгей). кГц	300	25
Уақыт ұясына пайдалы ақпарат жіберу жылдамдығы, кбит/с	13	7,2
Максималды ақпарат тарату жылдамдығы	9,6 кбит/с (EDGE қолдану кезінде 384 кбит/с)	28,8 кбит/с
Жылдамдықта мәліметтер мен дыбыс тарату, км/ч	350	200
Мәліметтер тарату қауіпсіздігі	A5 шифрлау алгоритмдері, кілт 256 бит, GEA3 (GPRS- те шифрлау)	E2E («толассыз шифрлау», кілт 128 бит), TEA (TETRA Encryption Algorithm)
Базалық бекеттерді қолданусыз абоненттер арасындағы байланыс	–	+ (жартылай дуплексті режим)
Базалық бекетті жабудың максималды аумағы, км	34,5	60
Ұяның әдеттегі радиусы (тегіс жерде), км	5 – 10	10 – 25
Негізгі ерекшелігі	ETCS/ERTMS еуропалық пойыздар қозғалысын басқару жүйесімен толық біріктірілу	Базалық бекет қолданусыз және желіге тәуелсіз абонент құрылғылары арасында DMO тікелей тарату режимінің болуы

Шет елдерде радиоблоктау жүйелері GSM-R жиіліктерінде сымсыз мәліметтер тарату жүйесін жиі қолданады. Қазақстанда бұл жиіліктерді

пайдалануға рұқсат жоқ, сондықтан жалғыз шешім TETRA стандарты мәліметтер таратудың жиіліктік спектрін қолдану болып табылады.

3.3 Мәліметтер тарату хаттамаларын зерттеу

Мәліметтер тарату хаттамалары стационарлық және борт құрылғысы арасында алмасуды іске асыру, жіберілетін мәліметтерді қорғау үшін арналған және OSI желілік модель базасында құрылады (кесте 3.3). ETCS/ERTMS жүйесінде, сондай-ақ KTCS жүйесінде қолданылатын Euroradio хаттамасы кең танымалдылыққа ие болды. Мәліметтер таратуды қорғауға қойылатын талаптар сипаты EN 50159 еуропалық стандартында мазмұндалады [69], ол темір жолда тарату желілерінде қолдану үшін ақпарат негізгі қауіптері мен қорғау әдістерін анықтайды.

Кесте 3.3 – OSI моделі

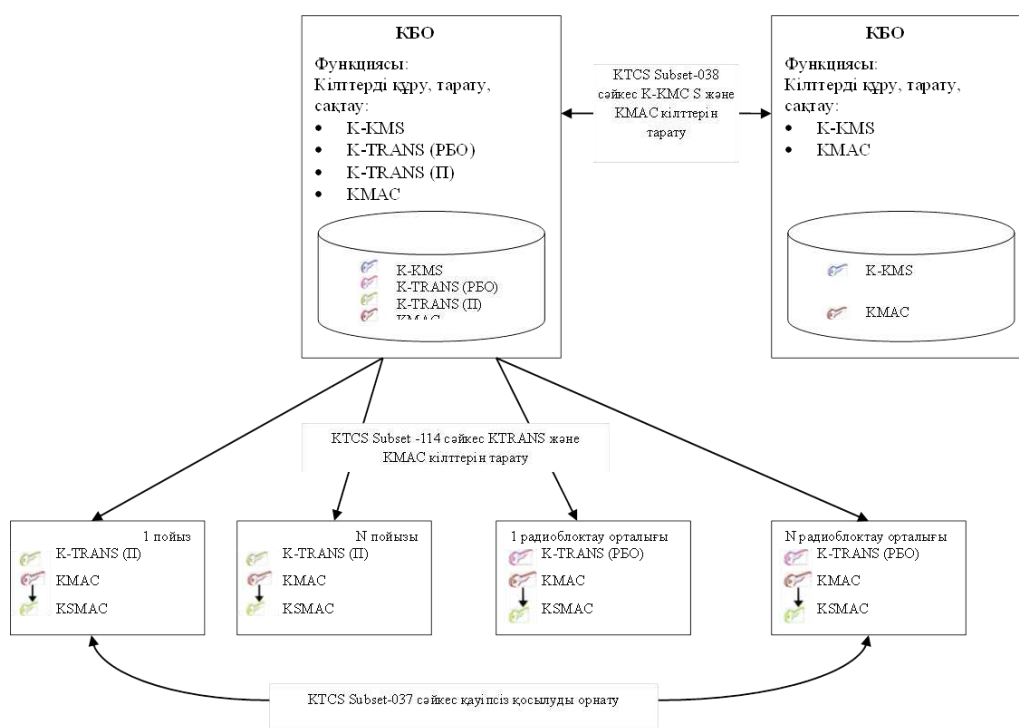
OSI моделі			
№	Деңгейі	Мәліметтер типі	Функциялары
7	Қолданбалы	Мәліметтер	Желілік қызметтерге кіру
6	Ұсыну деңгейі	Ағын	Мәліметтерді ұсыну және шифрлау
5	Сеанстық	Сеанстар	Байланыс сеансын басқару
4	Көліктік	Сегменттер	Соңғы пункттер арасындағы тікелей байланыс
3	Желілік	Пакеттер/датаграммалар	Маршрутты анықтау және логикалық адрестеу
2	Каналдық	Кадрлар	Физикалық адрестеу
1	Физикалық	Биттер	Тарату ортасымен, сигналдармен және екілік мәліметтермен жұмыс

Жұмыс режиміне байланысты OSI моделінің төменгі деңгейлерін іске асыру кезінде екі тәсіл кездеседі: каналдарды коммутациялау және топтық тарату. Каналдарды коммутациялау режимі борт және стационарлық құрылғы арасындағы белгіленген қосылуды қамтамасыз етеді. Мұндай режим ETCS, KTCS жүйелерінде пайдаланылады. Каналдарды коммутациялау режимін каналдық деңгей ретінде пайдалану кезінде әдетте HDLC (High - Level Data Link Control) хаттамасы қолданылады – ISO әзірлеген OSI желілік моделі каналдық деңгейінің бит-бейімделген хаттамасы. Бұл хаттама ғаламторда кеңінен пайдаланылатын PPP хаттамасында кадрлық механизмдер әзірлеу кезінде база болып табылады. Коммутациялау режимінің кемшілігі бір қосылу үшін толық каналды пайдалану болып табылады, бұл байланыс желісін қолдана алатын абоненттер санын азайтады.

Топтық тарату режимі мәліметтер бір-бірінен тәуелсіз шағын көлемді топпен жіберілетін жалпы желіге бірнеше абонентті кіргізуді жүзеге асыруға мүмкіндік береді, әрі қарай қабылдау-торабында жіберілген хабар топтардан жиналады. Каналдарды коммутациялау режимінің үлкен артықшылығы бір физикалық желі арқылы бірнеше абонентпен мәлімет алмасу мүмкіндігі болып табылады, бұл ретте әрекет етуші технологияның кемшілігі тарату кезіндегі топтардың күрделі бақыланатын кідірулері болып саналады. Желілік деңгей ретінде T.70 хаттамасы, көліктік деңгей ретінде байланыс қызметінің қажетті сапасын қамтамасыз ету үшін арналған X.224 хаттамасы пайдаланылады.

3.4 KTCS кілттер тарату жүйесі

KTCS кілттерді басқару жүйесіндегі негізгі буын кілттерді басқару орталығы (КБО) болып табылады [94, 95] (сурет 3.5). КБО радиоблоктау орталығын және оған қосылуды орындайтын тартымды жылжымалы құрамды қосқанда, теміржол көлігі объектілері үшін кілттер құруға жауап береді. Қалыптасқан кілттер пойыз бен радиоблоктау орталығы арасында қауіпсіз қосылуды құру үшін пайдаланылады. Сондай-ақ КБО орнатылып болған кілттерді таратуға, жаңартуға және өшіруге жауап береді, себебі әр берілген кілт үшін жұмыс істеу мерзімі қойылады, ол мерзім аяқталған кезде аталған процедуралардың бірі жүргізіледі.



Сурет 3.5 – KTCS кілттерді басқару жүйесінің архитектурасы

KTCS кілттерді басқару жүйесі 3.4 кестеде ұсынылған кілттер иерархиясын құрайды.

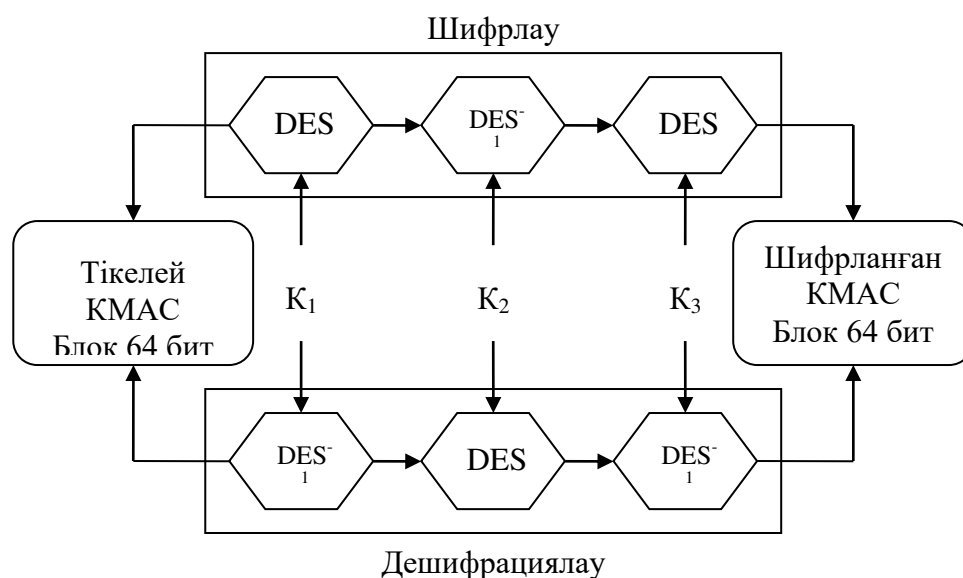
Кесте 3.4 – KTCS кілттер иерархиясы

Иерархия деңгейі	Кілт атауы	Кілттің тағайындалуы
3	К-КМС	Көлік кілті кілттерді басқару орталықтары (КБО) KTCS арасында қауіпсіз алмасуды қамтамасыз ету үшін пайдаланылады.
	KTRANS	Көлік кілті аутентификацияланған кілттерді құру, жаңарту немесе өшіру үшін КБО мен стационарлық немесе борт құрылғысы арасында қауіпсіз алмасуды қамтамасыз ету үшін пайдаланылады
2	КМАС	Аутентификациялық кілт KTCS екі объектісі арасында сессиялық кілт құру және қауіпсіз қосылуды орнату үшін пайдаланылады
1	КСМАС	Сессиялық кілт KTCS екі объектісі арасында бір сессия кезінде қорғалған ақпараттық алмасу үшін пайдаланылады

Иерархияның үшінші деңгей кілттері ақпараттық алмасудың барлық объектілері үшін алдын ала таратылған болуы қажет. Үшінші деңгей кілтін толығырақ К-КМС кілтінің үлгісінде қарастырамыз [96]. К-КМС кілті екі бөліктен тұрады:

- К-КМС1 (192 бит) КБО және КТCS объектілерін аутентификациялау үшін, сондай-ақ КБО жіберетін хабарлардың (мысалы, кілттерді басқару командаларының) бүтіндігін растау үшін пайдаланылады. Жіберілетін хабарды қорғау үшін аутентификациялық хабарлар кодын (MAC) есептеу процедурасы қолданылады, оны орындау нәтижесі хабардың бүтіндігін және хабар көзінің дұрыстығын тексеру үшін пайдаланылады;

- К-КМС2 (192 бит) екінші деңгей кілттерін – КТCS барлық нысандары арасында таратылатын аутентификациялау кілттерін (КMAC) шифрлау үшін пайдаланылады. Сондай-ақ К-КМС2 әрқайсысының ұзындығы 64 бит болатын К3, К2, К1 үш ішкі кілтке бөлінеді. КMAC кілтін шифрлау/дешифрлау процедураларын орындау кезінде кілт үш блокқа бөлінеді, оның әрқайсысына 3.6 суретте ұсынылған сұлба бойынша TripleDES шифрлау алгоритмі қолданылады.



Сурет 3.6 – Аутентификациялау кілттерін шифрлау/дешифрлау сұлбасы

ERTMS кілттерді басқару жүйесінде келесі функцияларды орындау қарастырылған:

- 1) КБО баптау.

Жүйе әкімшілігі борт және стационарлық құрылғыны баптаумен байланысты барлық процедураларды орындауды қамтамасыз етуі тиіс, яғни:

- кілттерді түрлендіру;
- кілттерді басқа КБО-ға жіберу;
- басқа КБО-дан кілттер алу;
- кілттерді өшіру;
- кілттерді архивтеу;
- кілттерді тексеру;

- логтар құру.

2) К-КМС кілттерін тарату.

Әкімшілік кілтпен алмасу процедурасы қажетті әр КБО үшін К-КМС кілттерін таратуы қажет. К-КМС кілттерін таратудың негізгі тәсілі сенімді байланыс каналдарын пайдалану болып табылады.

3) К-TRANS кілттерін тарату.

Әкімшілік берілген КБО жауапкершілігі аумағына кіретін ERTMS әр объектісі үшін К-TRANS таратуы қажет. К-TRANS кілттерін таратудың негізгі тәсілі сенімді байланыс каналдарын пайдалану болып табылады.

4) КМАС кілттерін түрлендіру.

Кілтті түрлендіруді КБО құпиялылық талаптарына сәйкес орындайды. Түрленетін кілттер «әлсіздікке» тексеруге жатады, КМАС әр түрлендірілген кілтіне бірегей реттік нөмір беріледі.

5) КМАС басқа КБО-мен алмасу;

- кілтті беру: жіберуші әкімшілік кілт арналған борт құрылғысын және онымен өзара әрекеттесетін радиоблоктау орталықтарының тізімін белгілеуі тиіс;

- кілтті алу: кілтті алушы әкімшілік кілтті алғанын растап, оны пайдалану үшін қажетті әрекеттер жасауы қажет.

Беру кезінде кілт К-КМС кілтінің көмегімен шифрланған болуы тиіс.

6) КМАС жаңарту.

КБО әкімшілігі кілтті жаңарту шешімін қабылдайды. Бұл процедура алдын ала дайындалған жоспар бойынша да, таратылған кілттер құпиялылығына қауіп төнген кезде де орындалуы мүмкін.

7) КМАС өшіру.

Әкімшілік кілтті өшіру үшін басқа әкімшіліктерге сұраныс жіберу мүмкіндігіне ие болуы қажет. Кілтті өшіруге сұраныс берген жағдайда КБО әкімшілігі кілттің барлық көшірмесінің өшірілгендігіне көз жеткізуі тиіс.

8) кілттер және кілттерді басқарумен байланысты әрекеттерді архивтеу. Әкімшілік тапсырмасына түрлендірілген кілттер жөнінде барлық ақпаратты сақтау кіреді, соның ішінде:

- кілттердің ERTMS борт және стационарлық құрылғыларына сәйкес келуі;

- әр кілттің ағымдағы жағдайы (қазіргі мезетте пайдаланылады, өшірілген және т.б.);

9) К-КМС өшіру.

КБО әкімшілігі басқа КБО әкімшіліктерін К-КМС кілттерін өшіру туралы ақпараттандыруы қажет, сонымен бірге әкімшілік кілттің барлық көшірмесінің өшірілгендігіне көз жеткізуі тиіс.

[97] сипатталған аутентификациялау хаттамаларын пайдаланумен, КБО ERTMS жалғанатын объектілерін сәйкестендіреді және екінші деңгей кілттерін құруды және уақытылы жаңартуды қамтамасыз етеді. ERTMS объектілері Euroradio хаттамасын пайдалана отырып, аутентификациялау процедурасын

орындайды, соның нәтижесінде тек бір сессия кезінде (шамамен 1 сағат) әрекет ететін бірінші деңгей кілттері түрленеді.

Қазіргі уақытта теміржол көлігі объектілері үшін KTRANS кілттерін таратудың негізгі тәсілі сенімді каналдар немесе курьерлік қызмет көмегімен кілттерді физикалық тарату болып табылады. Бұл тәсілді пайдалану көп уақыт алады және белгілі бір қауіп тасымалдайды [98]. Сонымен, бір борт құрылғысында сенімді курьерлік қызмет көмегімен кілт ақпаратын орнату немесе жаңарту уақыты мына формула бойынша анықталуы мүмкін:

$$T_k = T_{TO-2} + T_{дост} + T_{уст} [\text{ч}], \quad (3.1)$$

мұндағы

T_{TO-2} – ТПС техникалық қызмет көрсету мерзімі;

$T_{дост}$ – ТПС қызмет көрсету депосына дейін кілт ақпаратын жеткізу уақыты;

$T_{уст}$ – арнайы құрылғы көмегімен ТПС борт құрылғысына курьерлік қызмет көмегімен кілт ақпаратын орнату уақыты.

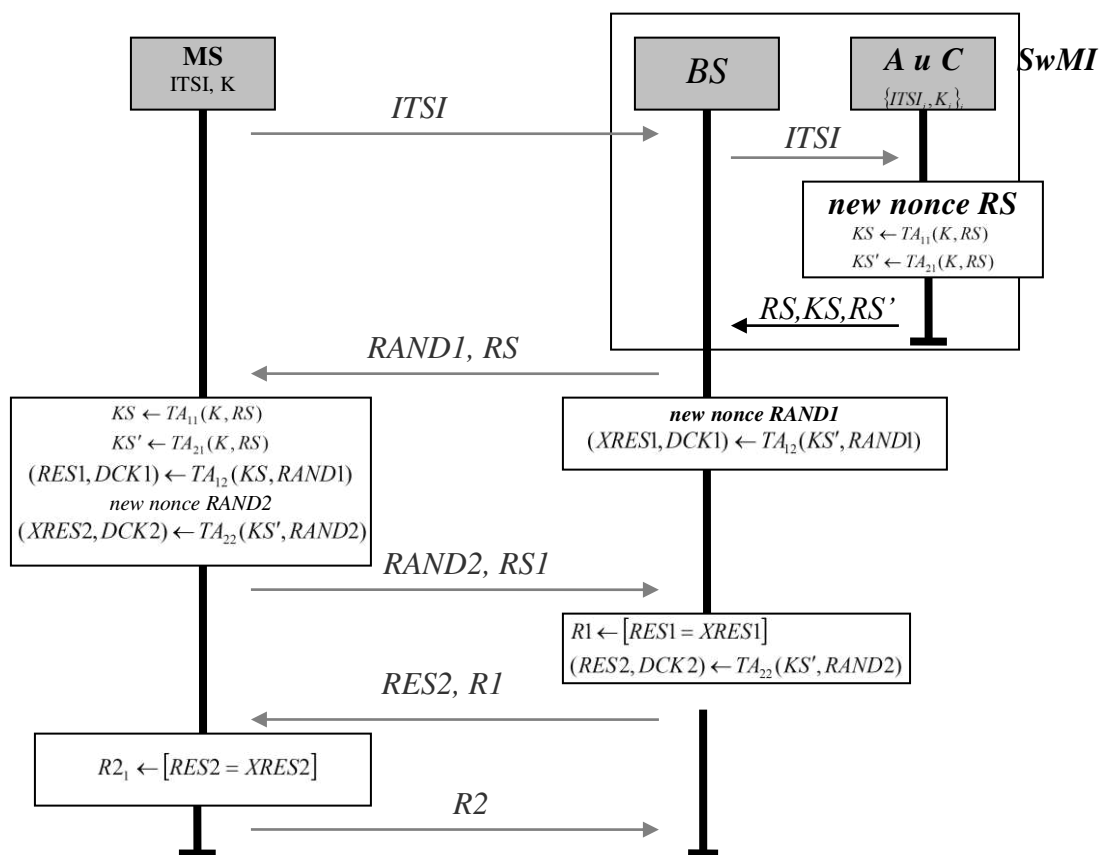
Германия темір жолының нормативті құжаттарында әр 9 күн сайын ТПС техникалық қызмет көрсету мерзімі көрсетіледі [99]. Келтірілген формула арқылы кілт ақпаратын орнату немесе жаңарту максималды уақыты ~219 сағатты құрайды деп есептеу оңай, бұл ақпараттық қауіпсіздік тұрғысынан өте көп болып саналады.

3.3. Жер үсті транкингік радионы аутентификациялау хаттамасының қауіпсіздігін талдау (TETRA)

Осы жұмыста келтірілген талдау мақсаттары үшін біз үш негізгі ішкі жүйені қосатын TETRA жүйесін пішіндейміз: қолданушылардың мобильді бекеттері (MS), радиокіру желісі ретінде базалық бекеттер (BS) және Аутентификациялау орталығы (AuC) кіретін базалық желі ретінде коммутациялау және басқару инфрақұрылымы (SwMI). MS TETRA құрылғысының идентификаторымен (TEI) сәйкестендірілген және әр құрылғы үшін бірегей болып табылатын физикалық соңғы құрылғыны және абонентті сәйкестендіру модулін (SIM) құрайды. SIM-карта рұқсатсыз кіруден қорғалған жады бөлігінде TETRA қолданушысын/жазылушысын бірегей сәйкестендіруді және сонымен байланысты симметриялық криптографиялық кілтті сақтайды, сондай-ақ аутентификациялау хаттамасында қолданылатын криптографиялық примитивтерді орындауы мүмкін.

TETRA аутентификациялау хаттамасы [100] көрсетілген. TETRA кез келгенімен басталуы мүмкін терминалдар мен мобильді желі арасындағы бір жақты және өзара аутентификациялауды қолдайды. Осы жұмыс аясында біз тек өзара аутентификациялаудың толық хаттамасын қарастырамыз, себебі бұл аутентификациялаудың ерекшеліктерге толы ең елеулі қасиеті болып табылады. Сонымен қатар, желі арқылы басталатын процедура бөлшекті түрде қарастырылатын болады (3.7 сурет). Алайда одан да әлсіз бір жақты

аутентификациялау хаттамаларында аутентификациялауды, сондай-ақ MS бастайтын өзара аутентификациялауды бұзу үшін төменде келтірілген соққыларды қарапайым модельдеу мүмкін болады (3.8 сурет).

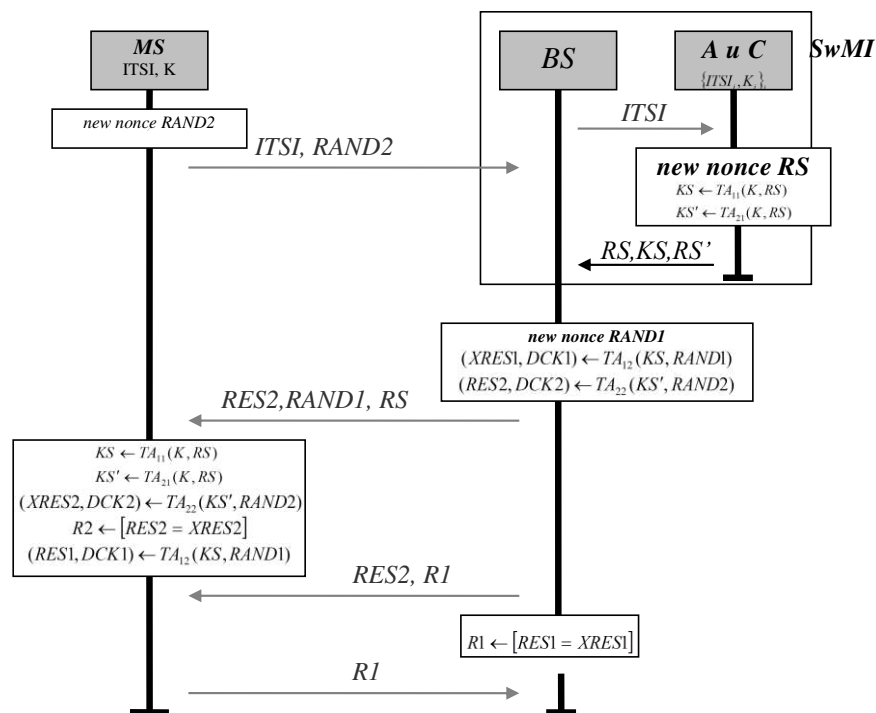


Сурет 3.7 – TETRA аутентификациялау хаттамасы; SwMI желісімен басталған өзара аутентификациялау. MS және BS TB4 сеанс кілтін келіседі (DCK1; DCK2). $\{ITSI, K_i\}$

Аутентификациялау үрдісіне жұмылдырылған жақтар MS, AuC және BS болып табылады. AuC және BS арасындағы байланыс каналы қауіпсіз болып саналады деп болжам жасалады, және артынша, AuC және BS-ты бірге бір SwMI ретінде қарастыруға болады.

3.7 суретте SwMI арқылы басталатын TETRA өзара аутентификациялау хаттамасы хабарларының диаграммасы көрсетілген. AuC TETRA (ITSI) MS абонентінің жеке сәйкестендірілген ақпаратын алғаннан кейін, ол оның ITSI сәйкес келетін қолданушының аутентификациялау K кілтін таңдайды. ITSI жеткізу [100] аутентификациялау хаттамасының бөлімі ретінде көрсетілмегендігін айта кетейік, және артынша, бұл бөлімдер төмендегі талдаудан жойылады (3.7 суретте сұр түспен кескінделген). ITSI ескере отырып, AuC кейін кездейсоқ бастапқы RS түрлендіріп, сәйкесінше TA11 және TA21 алгоритмдерінің көмегімен KS және KS' сеанс кілттерінің жұбын түрлендіру үшін оны K-мен пайдаланады. KS, KS0 және RS BS-қа жіберіледі, ол RAND1 кездейсоқ санын түрлендіреді және XRES1 күтілетін жауапты, сондай-ақ TA12 алгоритмі бойынша KS және RAND1-ден DCK1 шифрлау

алынған кілтін есептейді. Кейін BS MS үшін RAND1, RS жібереді. Әрі қарай MS сондай-ақ KS және KS' түрлендіреді де, RES1 және DCK1 жауабын есептейді, олардан RES1 BS-қа кері қарай жіберіледі. Қолданушы жағынан сонымен бірге RAND2 кездейсоқ саны түрленеді де, BS-қа жіберіледі. BS RES1-ді XRES1-мен салыстырады, және егер екі мән тең болса, R1 мәнін true-ге орнатады. Сонымен қатар, BS TA22 алгоритмі бойынша RES2 жауабын және KS' пен RAND2-ден алынған DCK2 шифрын есептейді. Кейін ол RES2 қайтарады да, аутентификациялау нәтижесі $R1 \leftarrow \text{true}$ болады. Әрі қарай MS RES2-ні XRES2 күтілетін жауабымен салыстырады, және егер олар тең болса, MS соңында $R2 \rightarrow \text{true}$ мәнін қайтарады. Егер екі жақ та өздерінің аралықтарын сәтті аяқтаған жағдайда, екеуі де DCK сеансы жалпы кілтінің TB4 алгоритміне сәйкес есептеу үшін DCK1 және DCK2 пайдаланады.



Сурет 3.8 – TETRA аутентификациялау хаттамасы; MS мобильді бекетпен басталған өзара аутентификациялау. MS және BS TB4 сеанс кілтін келіседі (DCK1; DCK2)

TA11; TA12; TA21, TA22 және TB4 алгоритмдері көрсетілмеген, себебі оператор қауіпсіз жұмысты таңдауы қажет. [100] ерекшеліктер кейбір бір жақты қасиеттерін¹. функцияларын қанағаттандыру талаптарын ашпайды.

TETRA аутентификациялау хаттамасын талдау Dolev-Yao қауіпсіздік моделін есепке ала отырып жүргізіледі [101]. Бұл модельде құқық бұзушы желіні толықтай бақылауға алады. Ол кез келген жіберілген хабарды ұстап, оны таратып жібере алады, бұл ретте шексіз әрекет ете алатын құқық бұзушы

¹ Мысалы, [100] «Алгоритм Кіріс 2 және Шығыс білімдерінен Кіріс 1 жөнінде кез келген ақпарат алу күрделі болатындай (алгоритм бөлшектері белгілі болса да) жобаланған болуы тиіс» деп TA11 жөнінде бекітілген.

сонымен бірге ұсталған хабардан және жаңа тұрақтылардың шектелмеген санынан білген ақпараттан өзі хабар құрып, оны тарата алады. Сонымен қатар ол хаттамалық сеанстардың шексіз санын бір уақытта орындауды бастай алады. Алайда криптографиялық примитивтер тіптен қауіпсіз деп саналады: мысалы, құқық бұзушы егер оған сәйкес дешифрлау кілті белгілі болса, берілген шифрланған мәтіннің ашық мәтіні жөнінде қандай да бір зат білуі мүмкін. Хабардың негізгі компоненттері, мысалы, кілттер немесе бір реттік нөмірлер жөнінде ішінара ақпарат болмайды.

Жүргізілген қауіпсіздік талдауында екі жақты хаттамалардың²: аутентификациялау және құпиялылығының келесі негізгі қасиеттері бізді қызықтырады және қанағаттандырады ма:

Әлсіз келісу. Егер А хаттамасының барлық аралығы үшін ол көздеген серіктеспен Б байланысы арқылы аяқталса, ал Б жағы көздеген серіктеспен аралықты шынымен А байланысы арқылы орындаған болса, хаттама А жағына әлсіз келісімге кепілдік береді.

Объективтік емес келісім (Ni-келісім). Егер А хаттамасының барлық аралығы үшін ол көздеген серіктеспен Б байланысы арқылы аяқталса, сондай-ақ В көздеген А серіктеспен орындаған хаттама бар болса, онда хаттама А жағы үшін ni-келісімге кепілдік береді, сондықтан осы аралықтардағы алынған хабарлар мазмұны болжамды серіктестің сәйкес аралығымен жіберілген хабарлар мазмұнымен бірдей болады.

Мәліметтер құпиялылығы. Хаттама А жағы аяқталатын цикл соңында сақтайтын мәліметтер бөлігінің, мысалы, осы цикл кезінде келісілген сеанс кілтінің құпиялылығына кепілдік береді.

3.7 суретте кескінделген TETRA аутентификациялау хаттамасында өте айқын әлсіз жер бар: R1 және R2 растау биттері үшін бүтіндікті қорғау жоқ, артынша, радиоинтерфейс арқылы байланысты басқаратын құқық бұзушы қалауы бойынша бұл биттерді жинауы мүмкін.

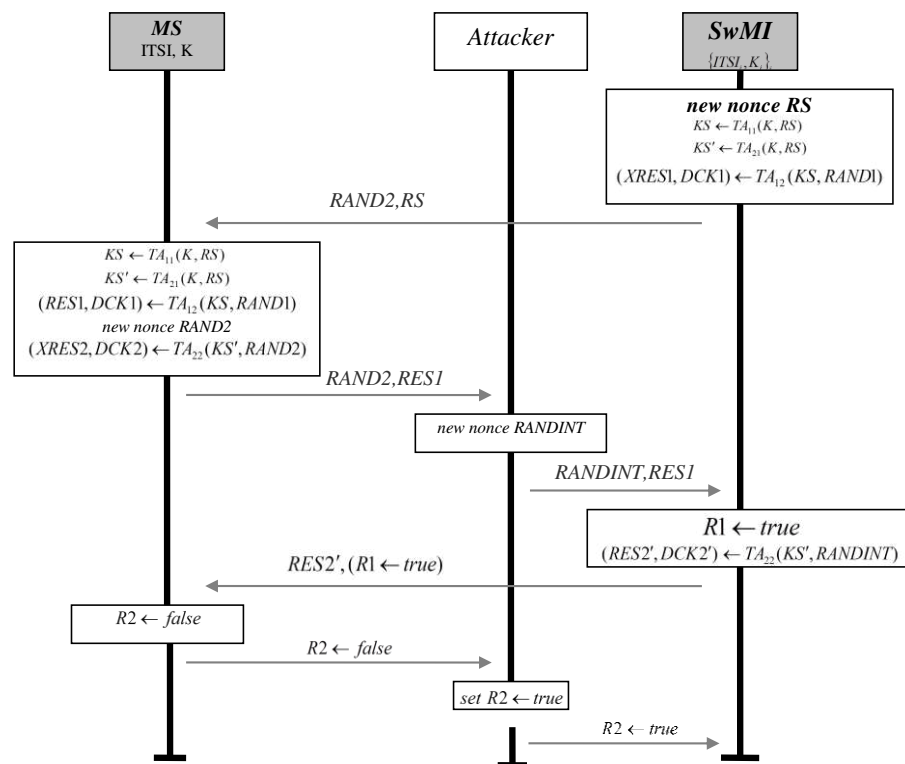
Одан төмен көрінетін әлсіз жер SwMI-ге MS жіберетін RES1 жауабы RAND2 кездейсоқ санымен байланысты емес екендігінде. Бұл кемшіліктер келесі соққыларда пайдаланылады:

1 соққы. Құқық бұзушы TETRA аутентификациялау хаттамасының орындалуын бақылайды және тек іске қосылған MS жіберетін R2 соңғы хабарын ұстап алады да, оны өзгертеді яғни құқық бұзушы R2-ni true-ден false-ге өзгертеді. Соның салдарынан, MS желіде өзі дұрыс аутентификацияланған және сеанс кілтімен бөліседі деп санайды, ал желі аутентификация сәтті болмаған аралық аяқталды деп есептейді. Бұл MS рөліндегі Ni-Agreement және Ni-Synch-ті бұзады. Бұл ретте ол құқық бұзушы соңғы хаттама хабарын лақтырып (бұл әрқашан мүмкін), және ол хабарды болжамды алушы бұл

² Бұл ерекшеліктер формальды түрде анықталған және Scyther көмегімен автоматты түрде тексеріледі.

сеансты ешқашан аяқтамайтын кезде соңғы хабарды кесіп тастаумен соққылардан ерекшеленетіндігі маңызды.

2 соққы. 3.9 суретте кескінделген бұл соққыда құқық бұзушы MS-тен RES1 және RAND2-ден тұратын SwMI-ге жіберілетін хабарды ұстап алады. Әрі қарай RES1 таңдайды да, RAND2 мәнін RANDINT қайта түрлендірілген бір реттік нөміріне ауыстырады. SwMI өзгертілген хабар MS-тен жіберілді деп есептейді, және қате кездейсоқ мәннен және $R1 \leftarrow \text{true}$ есептелген RES2 қамтитын хабарды қайтарады. Артынша, RES2 және XRES2 салыстыруларын тексеру MS жағында өтпейді, ал $R2 \leftarrow \text{false}$ ³-ке орнатылады. Бірақ құқық бұзушы соңғы хабарлы ұстап алады да, R2 орнына true мәнін SwMI-ге жібереді. SwMI рөлінің тұрғысынан, Ni-Synch және Ni-Agreement қауіпсіздік ерекшеліктері сақталмайды.



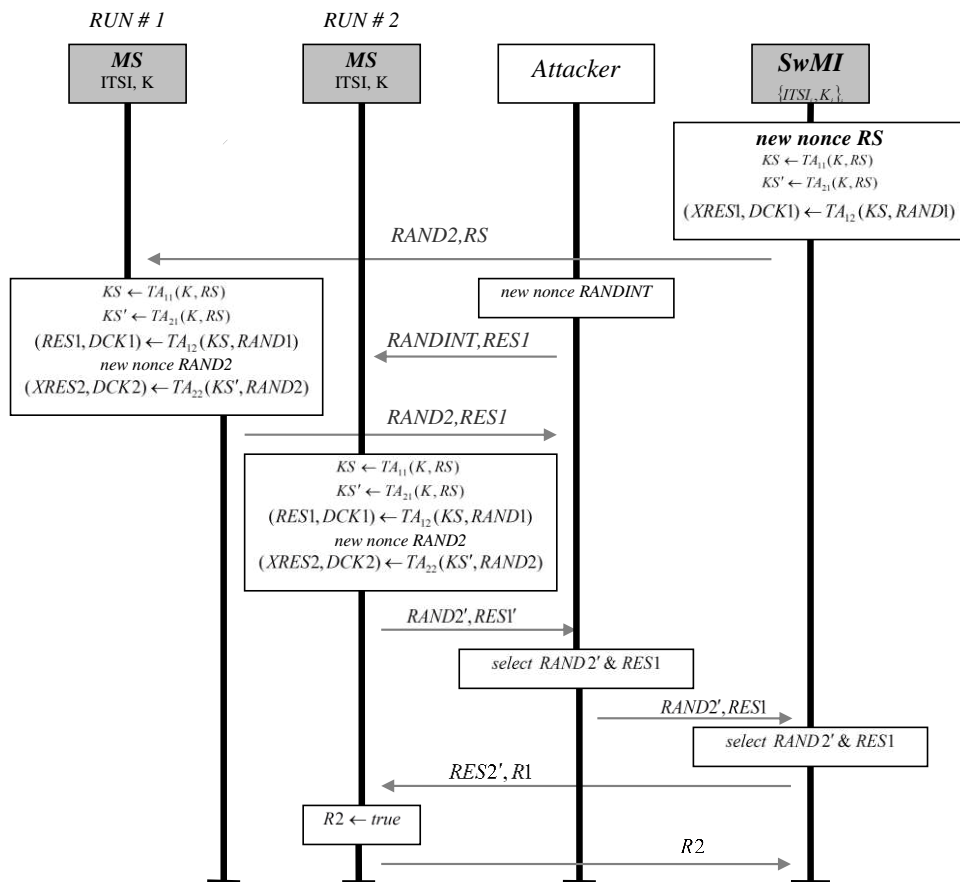
Сурет 3.9 – SwMI бастаған TETRA өзара аутентификациялауға қарсы 2 соққы.

3 соққы: 3.10 суретте көрсетілген ⁴бұл соққыда MS SwMI коммуникациялау бойынша болжамды серіктеспен екі бір уақытты сеансын қосады, сол кезде SwMI MS болжамды серіктеспен бір сеансты қосады. Соңында құқық бұзушы SwMI және MS бірдей сеанс кілтін келісті деп қате есептеуге әкеледі. Біріншіден, SwMI RS байланысының алғашқы сеансынан MS-ке дейін RAND 1 жіберген кезде, құқық бұзушы RS таңдап, RANDINT жаңа

³ Баламалы түрде құқық бұзушы RAND2 ауыстырмай, RES2 тікелей өзгертуі мүмкін.

^{4 4} Алғашқы екі соққыға қарағанда, бұл соққы Scyther көмегімен анықталған.

бір реттік нөмірін түрлендіреді де, RANDINT, RS-ті MS екінші сеансына жібереді. MS алғашқы сеансы RES1 дұрыс жауабын белгілейді де, RAND2' жаңа бір реттік нөмірімен RES1, RAND2 қайтарады, бұл уақытта MS екінші сеансы RES1' қате жауабын белгілейді де, RAND2' жаңа бір реттік нөмірімен RES1', RAND2' қайтарады. Енді құқық бұзушы бірінші сеанстан RES1 және екінші сеанстан RAND2' таңдайды да, SwMI-ге RES1, RAND2' хабарын жібереді. RES1 XRES1-ге тең болғандықтан, SwMI инфрақұрылымы R1-ді true мәніне орнатады да, RAND2'-ден RES2' жауабын белгілеп, RES2'; R1-ге жібереді. Бұл хабар кейін MS екінші сеансына соққы болып бағытталады; ал сол уақытта бірінші сеанс соққы ретінде жойылады. RES2' MS екінші сеансында түрленген RAND2' кездейсоқ бір реттік нөмірінен есептелгендіктен, ол расында екінші сеанста күтілетін жауапқа тең. Осылайша, MS екінші сеансы R2 true жібереді. Бұл сатыда MS екінші сеанста SwMI-ден хаттама қосу сәтті аяқталды деп санайды, ал SwMI MS-тен хаттама қосу сәтті аяқталды деп есептейді. Алайда тек алынған хабарлар осы сеанстарда жіберілген хабарларға ғана емес, сонымен бірге сеанста есептелген кілттер де тең емес. Сеанс кілті DCK1 және DCK2-дан есептелетіндігін еске сала кетейік. Бірақ DCK1 мәні RAND1-ден SwMI сеансында есептеледі, ал сол уақытта MS екінші сеансында ол RAND1'-ден есептеледі. Бұл MS және SwMI рөлдерінің Ni-Келісімін және Ni-Synch бұзады.



Сурет 3.10 – SwMI бастаған TETRA өзара аутентификациялауға қарсы 3 соққы

Қарастырылған үш соққының тәжірибелік мәнін анықтау мақсатында TETRA⁵ ерекшеліктерінен одан да толығырақ ақпарат оқып-білу қажет. Тәжірибеде TETRA аутентификациялау хаттамасы егер MS қосымшасы мобильділікті басқару қызметіне (TNMM-SAP) кіру нүктесі арқылы аутентификациялау сұранысын жіберген жағдайда іске қосылатын мобильділікті басқару қызметі (MM) арқылы орналасқан жерді жаңарту/тіркеу процедуралары аясында орындалады.

Тіркеу процедурасы MS жүйеге U-LOCATION UPDATE DEMAND хабарын жіберуден басталады. Жүйе кейін (міндетті түрде емес) MS-ке D-AUTHENTICATION DEMAND хабарын, яғни аутентификациялау хаттамасының алғашқы хабарын жіберіп, аутентификациялау үрдісін бастауы мүмкін. U-AUTHENTICATION нәтижесін, яғни аутентификациялау хаттамасының соңғы хабарын алғаннан кейін, жүйе MS-ке D-LOCATION UPDATE ACCEPT хабарын қайтарады. ACCEPT D-LOCATION UPDATE хабары мәліметтерінің хаттамалық блогы (PDU) R1 аутентификациялау нәтижесінен, шифрлау кілтімен (СК) алмасу ақпаратынан және TEI инфрақұрылымының сұранысы MS-тен екенін көрсетумен TEI сұраныс жалаушасынан тұрады. Өзара аутентификациялау үшін (яғни 3 қауіпсіздік класында) СК жалпы шифрлау кілтін (ССК) көрсетеді. Әр орналасқан жер аумағы (LA) кез келген уақытта бір ССК пайдаланады, яғни ол бірдей LA-да барлық мобильді бекеттер үшін жалпы болып табылады. ССК инфрақұрылымнан мобильді бекеттерге дейін трафик пен белгі беру тізбегін қорғау үшін; немесе ССК-ны тікелей шифрлау кілті ретінде пайдалану жолымен, немесе, ССК-дан алынған топты шифрлаудың сәйкес түрлендірілген кілтін (MGСК) пайдалану жолымен топтық қоңыраулар кезінде қолданылады.

Әрі қарай үш соққының орындалуы қарастырылған.

1 тәжірибелік соққы. Орналасқан жерді жаңарту/тіркеу кезінде. Құқық бұзушы хаттаманың соңғы хабарында R2 мәнін true-ден false-ге өзгерткеннен кейін, желі аутентификациялау өтілген жоқ деп есептейді де, D-LOCATION UPDATE REJECT хабарын жібереді. MS-ке аутентификациялау/тіркеу сәтті аяқталды деп есептету үшін құқық бұзушыға D-LOCATION UPDATE ACCEPT хабарын қолдан жасап, оны D-LOCATION UPDATE REJECT хабарымен ауыстырып қою керек. TETRA ерекшеліктеріне сәйкес PDU D-LOCATION UPDATE ACCEPT мұндай қолдан жасаудың алын алатын хабар бөлігін қамтуы міндетті емес. MS U-LOCATION UPDATE DEMAND хабарында ССК сұрау мүмкіндігі бар, және бұл жағдайда D-LOCATION UPDATE ACCEPT хабары DCK сеансының кілтімен шифрланған ССК-ны қамтуы тиіс [100]. Бұл D-LOCATION UPDATE ACCEPT PDU қолдан жасау мүмкіндігін болғызбайды, себебі құқық бұзушы DCK-ны біле алмайды. Алайда U-LOCATION UPDATE DEMAND хабарында ССК сұрату міндетті болып табылмайтындығын айта

⁵ Балама ретінде нақты түрде соққы жасап көруге болады, бірақ ол үшін TETRA тестілік желісіне кіруге рұқсат болу қажет, сондай-ақ жұмыс кезінде TETRA желілеріне зиян келтіру ықтималдылығы бар.

кетейік. [100] ерекшелікке сәйкес бір рет тіркелген MS егер желіден ажыраса және артынша қайта тіркеу кезінде ССК сұратпаса, бір немесе бірнеше ССК сақтай алады. Тәжірибеде құқық бұзушы артынша қайтадан қосылу/тіркелу әрекетін жасап көретін берілген базалық бекетте мобильді бекеттерді уақытша ұстап тұру жолымен қайта тіркеуді орындай алады, бұл құқық бұзушыға 1 соққыны қосуға мүмкіндік береді. Соның салдарынан, мақсатты мобильді бекеттер (және оның қолданушылары) олар желіге қосылған және хабар қабылдауға дайын деп қате есептеуі мүмкін. Бұл, кем дегенде, осы мобильді бекеттердің иесі өзінің координаторымен және әріптестерімен сөйлесе алмайтын алтын уақыттың жоғалуына әкелуі мүмкін.

Қосымша арқылы сұралатын аутентификациялау кезінде. MS-те жұмыс істейтін қосымша арқылы тікелей сұралатын аутентификациялауға мұндай D-LOCATION UPDATE ACCEPT хабарын жібермейді. [100] диаграммада көрсетілгендей, MS R2 аутентификациялау нәтижесін SwMI-ге жібергеннен кейін бірден пайдаланушы қосымша TNMM AUTHENTICATE растау хабарын алуы қажет. Бұл осы жағдайда MS SwMI-ден сеанс кілтін пайдаланумен түрленетін хабар күтпейтіндігін білдіреді. Артынша, 1 соққы тікелей тәсілмен қолданылуы тиіс және қолданушы өзінің пайдалану қосымшасынан аутентификациялаудың оң нәтижелерін алуы қажет, бұл ретте онда соққыға ұшырауы мүмкін терминал құрылғысының дұрыс жұмысы жөнінде ақпарат болмайды.

2 тәжірибелік соққы. Хаттама деңгейінде соққы салдары SwMI аутентификациялау сәтті өтті деп, ал MS керісінше есептеуі болып табылады, бұл MS пен SwMI арасында байланыстың жоғалуына әкеледі. Бірақ тәжірибеде MS егер [100] көрсетілгендей, RES2 тексеру орын алмаса, яғни MS басқа базалық бекет арқылы желіге қосылу әрекетін жасаса, бекетті қайта таңдауды бастайды. Бұл бекетті қайта таңдау орналасқан жерді жаңартуға/тіркеуге де, пайдаланушы қосымша бастаған аутентификациялауға да қолданылады. Бұл осы соққыны тәжірибеде орындауды қиындатады, себебі құқық бұзушыға мақсатты орналасу аумағында бірнеше базалық бекетті басқару қажет болады.

3 тәжірибелік соққы. Жоғарыда ұсынылған үш соққының ішінде 3 соққы тәжірибеде ең аз жүзеге асырылатыны болып табылады. Бұл соққы екі бір уақыттағы сеансты қосу үшін MS талап етеді. Тағы да, бұл орналасқан жерді жаңартуға/тіркеуге де, пайдаланушы қосымшасы бастаған аутентификациялауға да қатысты. Бұл MS-ке аутентификациялау хаттамасының екі бір уақытты сеансын қосуға мүмкіндік бермейді. Осылайша, бұл соққы егер жүйе ерекшелікке сәйкес дұрыс іске асырылған болса, пайдаланыла алмайды.

TETRA аутентификациялауды дұрыстау бойынша ұсыныс. TETRA-ға соққы болу мүмкін екендігі анық, себебі R2⁶-де (1) бүтіндікті қорғау және RES1 және RAND2⁷ (2) байланысы жоқ. (1) 1 және 2 соққыларды, ал (2) 3

⁶ Хаттамадағы R1 3.8 сурет

⁷ Хаттамадағы RES2 және RAND1 2 сурет

соққыны қосатынын оңай тексеруге болады. Сондықтан мыналардың көмегімен TETRA аутентификациялау хаттамасын дұрыстау ұсынылады:

(А) аутентификациялау функциясына R2 және RAND2 бір реттік нөмірі үстімен және KS'' кілтімен TC1 хабарларының мәнін қосу жолымен R2 бүтіндігін қорғауды қосу; яғни MS жіберген соңғы хабар R2-ден R2,TC1-ге өзгеруі қажет (R2; RAND2; KS'').

(В) аутентификациялау функциясына RES1 және кілті KS'' болып табылатын RAND2 бір реттік нөмірі үстімен TC1 хабарларының мәнін қосу жолымен RES1 және RAND2 байланысын қосу; яғни RES1, RAND2 орнына MS RES1; RAND2; TC1 жібереді (RES1; RAND2; KS'').

(В)-да және (А)-да KS'' TA11 мен TA21-ден ерекшеленетін кілт шығару функциясын пайдалану арқылы RS және оның K ұзақ уақыттық кілтімен MS және AuC бойынша түрленуі қажет. Ұсынылған түзетулер мобильді бекет бастапқыда кілттерді тек AuC-мен бөлісетін, бірақ жасырын базалық бекеттермен бөліспейтін кезде тәжірибеде желілік инфрақұрылымды ескереді. Ұсынылған түзетулер хабарды аутентификациялау үшін кілт алудың қосымша функциясын (KS'' түрлендіру үшін, сондықтан KS; KS'; KS'' ешқайсысы бірнеше криптографиялық примитивтер үшін пайдаланылмайды) және TC1 қосымша функциясын енгізуді талап етеді. Бұл ретте қосымша хабарлар енгізілмейді, және қосымша есептеу шығындары қатысты түрде аз болуы мүмкін. Өзара аутентификациялау кезінде R1 жіберу артық болып табылады, себебі ол RES1 тексеріс жүргізу жөнінде ақпарат сұрату үшін RAND2 сұранысын жіберуді қарастырады. Дәл солай R2 жіберу қажеттілігі жоқ, тек TC1 нәтижелеуші мәні (R2; RAND2; KS'').

```

role MS {
  var RS: Nonce;
  var RAND1: Nonce;
  fresh RAND2: Nonce;
  recv_1 (SwMI, MS, RAND1, RS);
  send_2 (MS, SwMI, TA12(TA11(k(MS, SwMI), RS), RAND1), RAND2,
          TC1(TA12(TA11(k(MS, SwMI), RS), RAND1), RAND2, TAX1(k(MS, SwMI), RS)));
  recv_3 (SwMI, MS, TA22(TA21(k(MS, SwMI), RS), RAND2), R1);
  send_4 (MS, SwMI, R2, TC1(R2, RAND2, TAX1(k(MS, SwMI), RS)));
  claim_MS1 (MS, Niagree);
  claim_MS2 (MS, Weakagree);
  claim_MS3 (MS, Nisynch);
  claim_MS4 (MS, Secret, TB4(TA12b(TA11(k(MS, SwMI), RS), RAND1),
                             TA22b(TA21(k(MS, SwMI), RS), RAND2)));
}

```

Сурет 3.11 – Scyther аспабына енгізу үлігі

TETRA аутентификациялау үшін ұсынылған түзетулер қауіпсіздігін тексеру Scyther көмегімен жүргізілді (3.11 сурет). MS үшін Scyther-де пі-келісім, әлсіз келісім және пі-синхрондау ерекшелігін тексеру, сондай-ақ MS рөлінің соңына дейін Iaim_MS1 (MS; Niagree), Claim_MS1 (MS; Niagree), Claim_MS3 (MS; Nisynch) және Request_MS4 (MS; Құпия, TB4 (TA12b (TA11b

(k (MS; SwMI); RS); RAND1) , TA22b (TA21 (k (MS, SwMI), RS), RAND2)))
қосу жолымен сеанс кілт құпиялылығы тапсырмасы қойылды.

3.4 Радиобайланысты ашудың KTCS-ке әсері

TETRA желісін жобалау кезінде темір жол үшін анықтау қажет негізгі параметр қажетті радиожабынын қамтамасыз ету үшін пайдаланылатын базалық бекеттер саны болып табылады. Қуатты таратқыштары бар базалық бекеттердің қатысты шағын санын (eNodeBs) ашу жөнінде шешім қабылдануы мүмкін. Осылайша теміржол желісі тек бірнеше ірі радио-ұяшықтармен жабылатын болады. Балама ретінде, бірдей теміржол желісі қуаты аз таратқыштары бар базалық бекеттердің көп санымен жабылуы мүмкін. Осылайша, жабу көптеген салыстырмалы шағын радио-ұяшықтармен жүзеге асырылатын болады.

Базалық бекеттерді ашудың таңдалған стратегиясы өткізу қабілеттілігіне, трафиктің ұяшыққа қатысты жүктемесіне, кедергілер мен тарату жиілігіне әсер етеді, яғни жабу тәсілі KTCS-те мәліметтер тарату өнімділігіне әсер етуі мүмкін.

Осы бөлімде ұсынылған зерттеу мақсаты eNodeB тығыздығы мен eNodeB тарату қуаты тұрғысынан TETRA радиостанцияларын ашу стратегиясын талдау болып табылады. KTCS-те мәліметтер таратудың кешігуіне және олардың бүтіндігіне әсер ету тұрғысынан eNodeB түрлі санымен бірқатар сценарийлерге бағалау жүргізілді. Осы бөлімде ұсынылған талдау алдында жарияланған жұмысқа негізделген.

Теміржол байланыс желісі KTCS-пен жабдықталған пойыздар жұмыс істейтін темір жолдың барлық аумағында қабылданатын сигнал қуаты тұрғысынан жеткілікті жабуды қамтамасыз етуі қажет.

KTCS радиожабыны талаптарына сәйкес төменгі байланыс желісінің қабылданатын сигналының минималды рұқсат етілген қуаты – 92 дБм құрайды. Мұндай қуаттың минималды талабы ($P_{\min} = -92$ дБм) осында ұсынылған талдауда қолданылды.

Алайда TETRA-де қабылдағыш сезімталдылығы жолақ ені, түрлендіру және қабылдағыш шу коэффициенті секілді көптеген факторларға байланысты екендігін айта кеткен жөн. Мысалы, жолақ ені 5 МГц, қуаты – 92дБм түрленуі 16QAM және кодталуы 1/2 канал сигналды қабылдауға жеткілікті деп болжауға болады. Одан да сенімді түрлендіру жағдайында, мысалы, QPSK, тіпті қабылдау қуаты – 100 дБм сигнал қол жеткізілген өткізу қабілеттілігі есебінен пайдаланылуы мүмкін [102]. Артынша, TETRA желісінде, тіпті егер мақсатты мәнге – 92 дБм қол жетпесе, қосылу сонда да мүмкін болады.

TETRA ұяшықтарының диапазоны eNodeB тарату қуатының функциясы секілді. Радиожабынын жоспарлау мақсаты үшін тарату қуаты мен ұяшық диапазоны арасында байланыс табылуы қажет.

P_t – бұл eNodeB таратқышы шығысындағы қуат. Кеңістік арқылы радиосигналдың таралу шамасына қарай ол бос кеңістіктік жоғалуы, кескін және т.б. секілді түрлі физикалық құбылыстар салдарынан әлсірейді. Бұл әсер

сигнал жолының жоғалуы деп аталады. Жолдың жоғалуы әсерінен, қабылдағыш таратқыштар неғұрлым қашық болса, соғұрлым қабылданатын сигналдың қуаты төмен болады. Артынша, радиоэлемент сигналдың қажетті деңгейі болатын әрекет етудің шектелген радиусына ие болады.

Жабуды жоспарлау үшін eNodeB (P_t) қабылданатын сигнал қуатын (P_r) тарату қуатының функциясы ретінде және eNodeB (d) қашықтықты табу қажет. Бұл ұяшықтар диапазонын (P_r) қабылданатын сигнал $P_{\min} = -92$ дБм мәнге жақындайтын (d) қашықтық ретінде бағалауға мүмкіндік береді.

Жолдың жоғалуынан басқа, антеннаның күшеюі, кабельдегі жоғалулар және интерференциялық қосымша секілді сигнал қабылдауға әсер ететін басқа да маңызды факторларды ескерген жөн [103]. Сондықтан дБм шкаласында (P_r) қабылданатын қуат келесі формуламен өрнектелген көптеген салымдардың қосындысын құрайды:

$$P_r = P_t + G_{\text{enb}} - L_{\text{enb}} + G_{\text{ue}} - L_{\text{ue}} - L, \quad \text{дБм} \quad (3.2)$$

мұндағы:

P_t – eNodeB тарату қуаты;

G_{enb} – eNodeB таратқыш антеннасының күшеюі;

L_{enb} – таратқышта фидер кабелінің жоғалуы;

G_{ue} – UE-қабылдағыш антеннасының күшеюі;

L_{ue} – қабылдағышта қуаттың жоғалу қосындысы, мысалы, кіруге кеткен жоғалулар әсерінен;

M – кедергілер мен өшуге арналған алаң;

L – сигнал жолының жоғалуы.

Сигнал жолының жоғалуы түрлі тарату модельдерінің көмегімен бағалануы мүмкін. Бұл жұмыста 3GPP стандартына сәйкес анықталған түрде COST231 Hata түрлендірілген моделі пайдаланылған [60]. COST231 Hata моделі қоршаған ортаға (қалалық, қала маңындағы) байланысты түрлі факторларды құрайды. Модель ретінде «Қала маңындағы макрожолдың жоғалуы» жолдың жоғалу моделі таңдалған. Бұл модельде (L) сигналы жолының жоғалуы келесі формуламен өрнектеледі [60]:

$$L = (44,9 - 6,55 \cdot \log_{10}(h_{\text{enb}})) \cdot \log_{10}\left(\frac{d}{1000}\right) + 45,5 + (35,46 - 1,1 \cdot h_{\text{ue}}) \cdot \log_{10}(f_c) - 13,82 \cdot \log_{10}(h_{\text{ue}}) + 0,7 \cdot h_{\text{ue}} + C, \quad \text{дБ} \quad (3.3)$$

мұндағы

d – eNodeB және UE арасындағы қашықтық (м),

h_{enb} – eNodeB антеннасының биіктігі (м),

h_{ue} – UE антеннасының биіктігі (м),

f_c – тасымалдаушы жиілік (МГц),

C – тұрақты коэффициент, қала ішінде 3 дБ және қала маңында 0 дБ тең.

Ұяшықтар диапазоны олардың арасындағы қашықтық ретінде бағаланады, онда $P_r = P_{min}$. d_r табу үшін L жолдың жоғалуы (3.2) теңдеуде (3.3) жолдың жоғалуымен ауыстырылады, ол келесі түрде өрнектеледі:

$$P_{min} = P_t + G_{enb} - L_{enb} + G_{ue} - L_{ue} - M - L = P_t + G_{enb} - L_{enb} + G_{ue} - L_{ue} - M - (44,9 - 6,55 \cdot \log_{10}(h_{enb})) \cdot \log_{10}\left(\frac{d}{1000}\right) - 45,5 - (35,46 - 1,1 \cdot h_{ue}) \cdot \log_{10}(f_c) + 13,82 \cdot \log_{10}(h_{ue}) - 0,7 \cdot h_{ue} - C, \quad \text{дБм}$$

Жоғарыда келтірілген теңдеуді түрлендіре отырып, d_r ұяшықтар диапазонын анықтауға болады:

$$d_r = 10^{\left(3 + \frac{x}{44,9 - 6,55 \cdot \log_{10}(h_{enb})}\right)}, \quad \text{м} \quad (3.4)$$

мұндағы:

$$x = P_t + G_{enb} - L_{enb} + G_{ue} - L_{ue} - M - P_{min} - 45,5 - (35,46 - 1,1 \cdot h_{ue}) \cdot \log_{10}(f_c) + 13,82 \cdot \log_{10}(h_{ue}) - 0,7 \cdot h_{ue} - C \quad (3.5)$$

Бұл теңдеу радиохабарын ашуды жоспарлау үшін пайдаланылатын негізгі құрал болып табылады.

3.5 Радиоканал арқылы мәліметтер тарату кезінде кілттерді аутентификациялау және түрлендіру

Теміржол көлігінде басты талаптардың бірі қауіпсіздік болып табылады. Басқару жүйелерінде мәліметтерді қорғауды қамтамасыз ету жүйе қауіпсіздігіне әсер ететін тапсырма болып саналады. Сондықтан радиоканал арқылы жіберілетін мәліметтер рұқсатсыз әсерлер мен бұрмаланудан қорғалған болуы тиіс. Жүйе қауіпсіздігін қарастыру кезінде мүмкін болатын қауіптер талданады. EN 50159 стандартына сәйкес мәліметтер тарату кезінде келесі қауіптер орын алуы мүмкін [69]:

- хабардың қайталануы;
- хабардың жойылуы;
- хабардың қойылуы;
- хабардың жіберілу ретінің өзгеруі;
- хабардың бұрмалануы;
- хабардың кідіруі;
- хабардың жасырынуы.

Бұл қауіптер EN50159-2 еуропалық стандартымен анықталған [70] және қазіргі мезеттегі ақпарат жіберу кезіндегі барлық белгілі қауіптерді сипаттайды.

Аталған қауіптерден қорғануды қамтамасыз ету үшін мәліметтер тарату хаттамасында іске асырылатын қауіпсіздіктің арнайы әдістері пайдаланылады [69].

Хабардың қайталануы, хабардың жойылуы және хабардың жіберілу ретінің өзгеруі секілді қауіптерден қорғау үшін хаттамада осы типтегі қауіпті оңай анықтауға мүмкіндік беретін қосымша жол – хабардың реттік нөмірі енгізілетін әдіс қолданылады.

Хабардың кідіруінен қорғау үшін хаттамаға хабарды жеткізудің кідіруін бақылауға мүмкіндік беретін уақыт мөртабаны – жолы қосылады.

Хабардың бұрмалануынан және хабардың жасырынуынан қорғау үшін криптографиялық қорғау әдістері пайдаланылады.

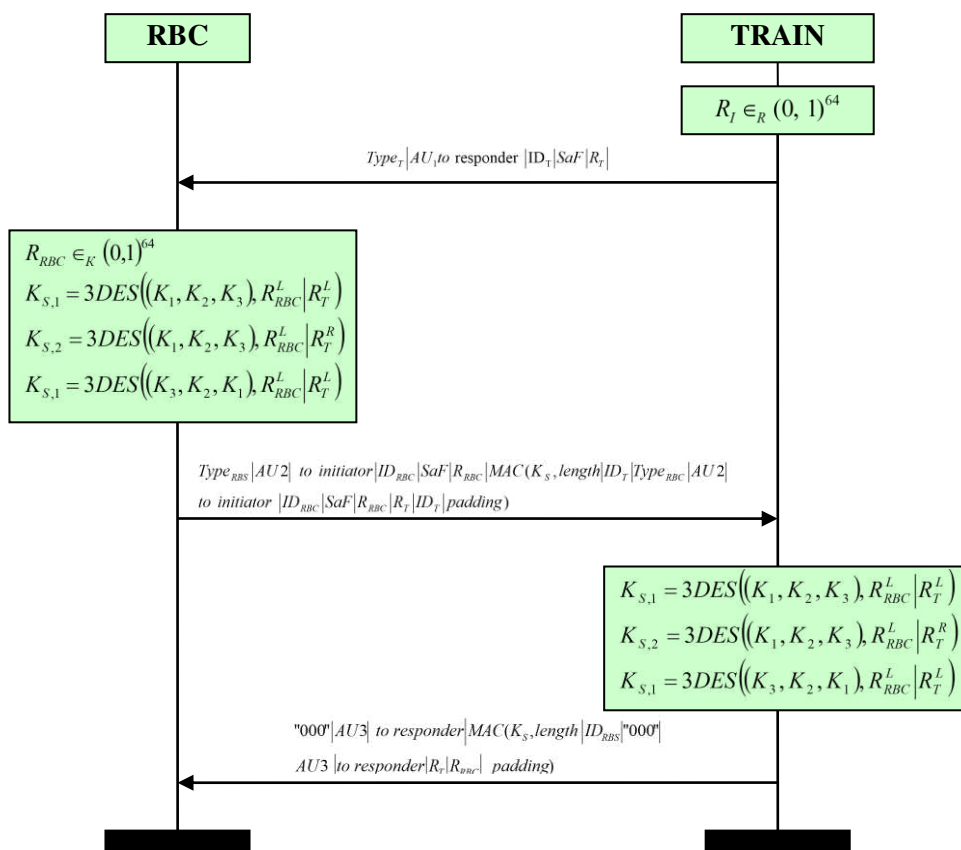
Хабардың қойылуынан қорғау үшін хабар көзі мен қабылдаушы идентификаторлары – жолы қосылады.

Криптографиялық әдістер негізінде KTCS жүйесінде пайдаланылатын Euroradio хаттамасындағы аутентификациялау іске асырылады. Криптографиялық қорғау әдістерін іске асырудың толық сипаты [104] келтірілген. Хабардың бүтіндігі Euroradio хаттамасында құқық бұзушыға хабарды қолдан жасауға кедергі келтіретін санды құрайтын MAC (message authentication code) хабарды аутентификациялаудың арнайы кодымен қорғалады. MAC мәні құпия кілт пен хабар мәтіні негізінде есептеледі. Хабар мәтінінің кез келген өзгеруі құқық бұзушыға қол жетімсіз құпия кілтінің көмегімен есептелетін MAC мәнінің өзгеруін талап етеді. Теорияда хабарды аутентификациялау кодын есептеу функциясы барлық мүмкін болатын кіріс мәндерін көптеген n -биттік шығыс мәндерге кездейсоқ кескіндеу болып табылады. Euroradio хаттамасында MAC функциясы ретінде CBC-MAC деп аталатын блоктық шифр негізіндегі әдіс қолданылады. CBC-MAC алгоритмінің негізгі идеясы шифрланған блоктарды байланыстыру (CBC – cipher block chaining) және соңғысынан басқа шифрланған мәтіннің барлық блоктарын лақтыру режимінде блоктық шифрлау көмегімен m хабарын шифрлау болып саналады. $P_1, \dots, P_k$ блоктарынан тұратын хабар үшін MAC мәні келесі формулалар негізінде есептеледі:

$$\begin{aligned} H_0 &= 0; \\ H_i &= E_k(P_i \oplus H_{i-1}) \\ MAC &= H_k. \end{aligned} \tag{3.6}$$

Қосу кезінде сессия орнатқан кезде 3.12 суретте көрсетілген аутентификациялау процедурасы жүргізіледі.

Б жағы Б-мен түрленетін ұзындығы 64 бит Rb кездейсоқ санын жібереді. Rb саны Б жағында сақталады. Осы хабарды алғаннан кейін А жағы ұзындығы 64 бит Ra кездейсоқ санын түрлендіреді де, Текст3 алаңы, Ra және Rb кездейсоқ сандары бойынша MAC-ты, DA идентификаторын және толтыру биттерін анықтайды. MAC (message authentication code) – құқық бұзушыға хабарды қолдан жасауға кедергі келтіретін санды құрайды. Нақты түрде хабарды аутентификациялау коды (MAC) – бұл кірісіне екі аргумент (ұзындығы анықталған К кілті және еркін ұзындықтағы m хабары) қабылдайтын және анықталған ұзындық мәнін беретін функция.



Сурет 3.12 – Кілттерді аутентификациялау және түрлендіру тізбегі

MAC анықтау үшін келесі процедураға сәйкес R_A , R_B параметрлері мен K_{AB} аутентификациялық кілті негізінде K_S сессиялық кілті есептеледі:

- R_A , R_B сандары 32 биттік блокқа бөлінеді.

$$\begin{aligned} R_A &= R_A^L | R_A^R \\ R_B &= R_B^L | R_B^R \end{aligned} \quad (3.7)$$

K_{S1} , K_{S2} , K_{S3} үш 64 биттік кілті мына формулалар арқылы есептеледі:

$$\begin{aligned} K_{s1} &= MAC(R_A^L | R_B^L, K_{AB}) = DES(K_3, DES^{-1}(K_2, DES(K_1, R_A^L | R_B^L))) \\ K_{s2} &= MAC(R_A^R | R_B^R, K_{AB}) = DES(K_3, DES^{-1}(K_2, DES(K_1, R_A^R | R_B^R))) \\ K_{s3} &= MAC(R_A^L | R_B^L, K_{AB}') = DES(K_1, DES^{-1}(K_2, DES(K_3, R_A^L | R_B^L))) \end{aligned} \quad (3.8)$$

мұндағы $KMAC = (K_1, K_2, K_3)$.

Euroradio хаттамасында MAC-ты анықтау симметриялық блоктық шифр болып табылатын TripleDES шифрлау стандартын пайдалануға негізделген. «Қазақстан темір жолы «Ұлттық компаниясы» АҚ қажеттілігі үшін хаттаманы жобалау кезінде TripleDES-ті «Ақпарат өңдеу жүйелері. Криптографиялық қорғаныс. Криптографиялық түрлендіру алгоритмі» ГОСТ 28147-89 [105] симметриялық шифрлау стандартына ауыстыру көзделеді.

KTCS жүйесінде жіберілетін мәліметтерді қорғауды ашық байланыс желілерін пайдаланумен радиоканал арқылы қауіпсіздікпен байланысты мәліметтер тарату үшін арналған Euroradio хаттамасы жүзеге асырады.

Бұл хаттама ашық желілер арқылы жауапты мәліметтер тарату кезінде қорғанысты регламенттейтін EN 50159-2 стандарты негізінде құрылған [70].

Euroradio хаттамасы OSI моделі негізінде құрылған және келесі деңгейлерге ие (кесте 3.5):

Кесте 3.5 – Euroradio хаттамасының OSI деңгейлері

Атауы	Іске асыру
Қосымшалар деңгейі	7Subset-026 (7,8)
Қауіпсіздік деңгейі	Euroradio (Subset-037)
Көлік деңгейі	X.224 хаттамасы
Желілік деңгей	T.70 хаттамасы
Каналдық деңгей	HDLC хаттамасы
Физикалық деңгей	Модем

Каналдық деңгейде ISO әзірлеген OSI желілік моделінің HDLC (High-Level Data Link Control) бит-бейімделген хаттамасы пайдаланылады. HDLC үшін ағымдағы стандарт ISO13239 болып табылады. HDLC мәліметтер тарату каналын басқару хаттамасы болып табылады және үздіксіз жылжымалы терезе арқылы ағынды басқару механизмін іске асырады. HDLC жартылай дуплексті және толық дуплексті таратуды, бірнүктелі және көпнүктелі конфигурацияны, сондай-ақ коммутацияланатын және коммутацияланбайын каналдарды қолдайды.

Euroradio HDLC хаттамасын іске асыруда жүргізуші және жүргізілетін функцияларды біріктіретін және командаларды да, жауаптарды да өндіретін аралас бекеттер үшін нүкте-нүкте қосылу типі қолданылады. Бекеттің әрқайсысы әр уақытта үш логикалық жағдайдың бірінде болуы мүмкін:

- логикалық ажыратылу жағдайы;
- басталу жағдайы
- ақпарат тарату жағдайы.

HDLC хаттамасы логикалық қосылудың үш режимін қолдайды. Euroradio хаттамасының құрамында HDLC іске асыру үшін асинхронды теңдестірілген режим пайдаланылады, онда тарату кез келген жақтан басталуы мүмкін және толық дуплексте жүргізіледі. Бұл режимде екі құрылғы да тең және кадрлар-командалар мен кадрлар-жауаптар болып бөлінетін кадрлармен алмасады.

HDLC кадрларын синхронды және асинхронды қосылуды пайдалана отырып жіберуге болады. Қосылулардың өзінде кадрдың басталуын және аяқталуын анықтау механизмдері жоқ, бұл мақсатта хаттама аясында бірегей болып табылатын биттік тізбек (FD – Frame Delimiter) «01111110» (0x7E он алтылық қойылымда) пайдаланылады, ол әр кадрдың басына және соңына орналастырылады. Жалаушаның бірегейлігіне байтстаффинг қолданумен кепілдік беріледі.

Байтстаффинг кезінде арнайы тізбек пайдаланылады, мұнда – «01111101» (0x7D он алтылық қойылымда), яғни FD(0x7E) байты кадрдың ортасында (0x7D, 0x5E) байттарының тізбегімен, ал (0x7D) байты – (0x7D, 0x5D) байттарының тізбегімен ауыстырылады. HDLC кадрының құрылымы 3.6 кестеде ұсынылған.

Кесте 3.6 – HDLC кадрының құрылымы

FD жалаушасы	Мекен-жай	Басқарушы алаң	Ақпарат алаңы	FCS	FD жалаушасы
8 бит	8 бит	8 немесе 16 бит	0 немесе одан да жоғары бит, 8 есе	16 бит	8 бит

FD жалаушалары – 01111110 кодтарын құрайтын ашушы және жабушы жалаушалар, қабылдағышқа кадрдың басы мен соңын анықтауға мүмкіндік беріп, HDLC-кадрын қоршайды. Осы кадрлар арқасында HDLC-кадрда кадр ұзындығының алаңы болмайды. Кейде бір кадр соңының жалаушасы (бірақ міндетті түрде емес) келесі кадрдың бастауыш жалаушасы болуы мүмкін.

Мекен-жай өзінің әдеттегі тек нүкте-көпнүкте конфигурацияларында бірнеше мүмкін болатын құрылғылардың бірін сәйкестендіру функциясын атқарады. Қоснүктелік конфигурацияда HDLC мекен-жайы тарату бағытын белгілеу үшін пайдаланылады – желіден қолданушы құрылғысына (10000000) немесе керісінше (11000000).

Басқарушы алаң 1 немесе 2 байтты құрайды. Оның құрылымы жіберілетін кадрдың типіне байланысты. Кадр типі басқарушы алаңның алғашқы биттерімен анықталады: 0 – ақпараттық, 10 – басқарушы, 11 – нөмірленбеген тип. Барлық типті кадрлардың басқару алаңы құрылымына P/F биті кіреді, ол кадр-командаларда және кадр-жауаптарда әр түрлі қолданылады. Мысалы, қабылдаушы бекет таратушы бекеттен P орнатылған биті бар кадр-команда алған кезде тез арада F битін орнатып, басқарушы кадр-жауаппен жауап беруі тиіс.

Ақпарат алаңы желі арқылы жоғары деңгейлі хаттамалар тобын жіберу үшін арналған – IP, IPX, AppleTalk, DECnet желілік хаттамалары, сирек жағдайда – өзінің хабарларын тікелей каналдық деңгейге жіберген кезде қолданбалы хаттамалар. Ақпарат алаңы басқарушы кадрларда және кейбір нөмірленбеген кадрларда болмауы мүмкін.

FCS (FrameCheckSequence) алаңы – тарату қателіктерін анықтау үшін қажетті бақылау тізбегі. Оны анықтау негізінен CCITT V.41 ұсынысына сәйкес $X^{16}+X^{12}+X^5+1$ (CRC-16) өндіруші полиномы бар циклдік кодтау әдісімен жүргізіледі. Алынған CRC бит арқылы түрленеді де, кері тізбекте жазылады. Бұл дара қателіктен туатын ұзындығы 16 битке дейін барлық мүмкін болатын қателіктерді, сондай-ақ 99,9984 % одан да ұзын барлық мүмкін болатын қателіктер тізбегін анықтауға мүмкіндік береді. FCS келесі алаңдар бойынша құрылады: Мекен-жай, Басқарушы алаң, Ақпарат алаңы. Сирек жағдайда циклдік кодтаудың басқа әдістері пайдаланылады. Қабылдағыш жағында FCS

есептегеннен кейін ол оң немесе теріс түбіртекпен жауап береді. Жіберуші жақтың кадрын қайталау теріс түбіртектің келуі бойынша немесе тайм-аут аяқталған кезде орындалады.

Euroradio хаттамасында желілік деңгей үйлестіруші функциялар деп аталатын және T.70 хаттамасының базасында іске асырылған. Үйлестіруші функциялар B/Bmi хаттамаларының мәліметін сигналдық хаттама мәліметімен пайдалану кезінде талап етілетін синхрондау механизмдерін қамтамасыз етеді.

Үйлестіруші функциялар келесі тапсырмаларды орындайды:

- сұралатын GSMPLMN тіркеу;
- GSM 07.07 және ETS300102 сигналдық хаттамалары арқылы желілік қосылуды негіздеу;
- QoS сапасының сұралатын параметрлерін кескіндеу;
- қажет кезде қоңырау кезінде қосылудың ауытқуы;
- сигналдық хаттамалардың GSM07.07 және ETS 300102 арқылы қосылуды ажырату;
- қосымша сервистік ақпараттың GSM/ISDN өңдеу.

Көлік деңгейі TP2 деңгейінің X.224 хаттамасымен ұсынылған және келесі қызметтерді атқара отырып, түйіндер арасында сенімді топтар таратуды қамтамасыз етеді:

- хабарды қосу және бөлу;
- сегменттеу және кері сегменттеу;
- мультиплексирлеу және демultipлексирлеу;
- ағынды анық бақылау.

Қауіпсіздік деңгейі [106] құжатына негізделген және аутентификациялау процедурасы мен CBC-MAC есебін қосады.

Теміржол инфрақұрылымының күйін мониторингтеу және диагностикалау жүйесін жетілдіру кезінде рельс тізбектері жоқ, бірақ пойыздың бүтіндігін бақылау бар радиоблоктау жүйесіне көшу мүмкін болады.

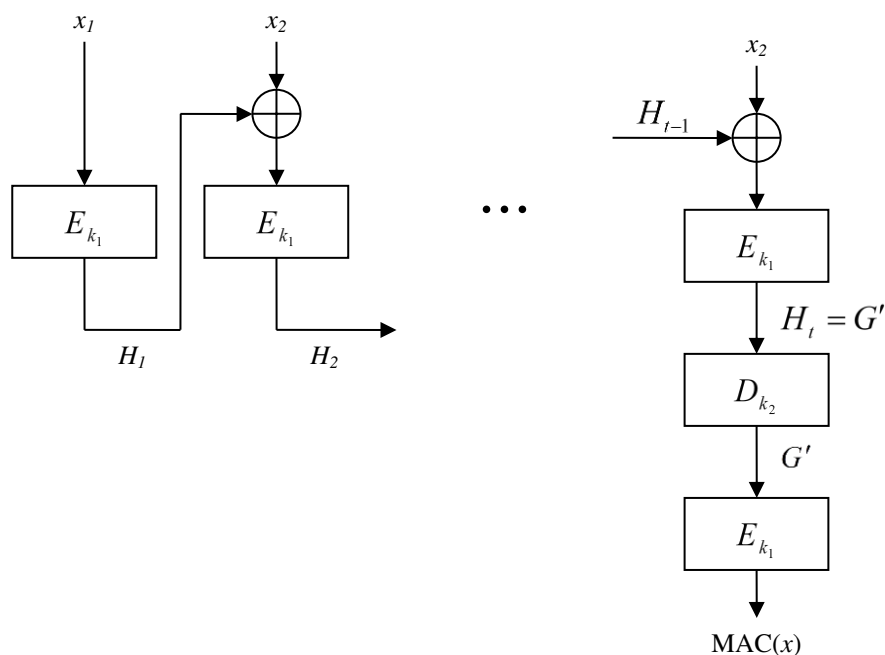
Егер көрші телімде осы жүйе бар болса және жүретін жылжымалы бірліктерде соңғы тетіктермен бірге борт құрылғылары орнатылған болса, радиоблоктау жүйелерін қолдану ұсынылады.

АБ немесе радиоблоктау жүйесін таңдау нақты телімді жаңғырту бойынша жобалық жұмыстар орындау кезінде техникалық тапсырма негізінде жасалады.

3.8 MAC криптографиялық талдау

Шифрлау сұлбаларын талдау қолжетімді әдебиеттің елеулі көлемі бар білімнің зерттелген саласы болып табылады. 2 бөлімде айтылғандай айтылғандай, KTCS жүйесінде қолданылатын MAC ISO-9797-1 Алгоритмінің түрлендірілген нұсқасы болып саналады [107]. Бұл алгоритм, ISO стандартында көрсетілгендей, оның алдында Митчеллмен [108] және Перенел [109] талданған. Пеппин мен Вилиотти [110] EuroRadio MAC өте тығыз байланысты болса да, олар осы алгоритм қолданылатын ERTMS, кілттерін тарату талдауын жүргізді, ал Франкелова [111] EuroRadio MAC арнайы талдауы жүргізілді.

Аталған MAC алгоритмін ISO-9797 талдау Митчеллмен [108] және Перенел [109] орындалды, оның нәтижесі бойынша келіспеушілік негізінде кілтті қалпына келтіру соққысы анықталды, онда кілтті алу үшін 232:5 ашық мәтін мен MAC белгілі жұбы және 3256 автономды операция қажет болды. Бұл зерттеу ерекшеліктерінің бірі стандартта көрсетілгендей MAC көңіл бөлу болып табылады. Алдында айтылғандай, EuroRadio MAC алгоритмі нақты түрлену үшін 3 ISO-9797 MAC алгоритміне негізделген, артынша, бұл авторлар сипаттаған соққылар сол уақытта пайдалы болса да, алайда екі түрлі кілті бар DES екілік түрленуден үш түрлі кілті бар 3DES түрленуге көшуге байланысты өзектілігін жоғалтты.



Сурет 3.13 – ISO-9797 MAC-алгоритмі 3

MAC, Smart екі нұсқасы арасында нақты түрленуді қарастыра отырып, екі кілті бар 3DES түрлену таңдалған ашық мәтінмен соққы жасау көмегімен тоқтатылуы мүмкін екендігіне дәлелдер анықталды (сәйкесінше 264 жоғарылатылған уақытша және кеңістіктік күрделілігі бар) [112]. Бұл соққыда таңдалған ашық мәтіні бар болжам әр анықтау сатысында сәйкес келетін кілттер жұбын іздеу үшін пайдаланылады, және кейін кілт-үміткерлер (жұп ретінде) қайтып келеді. Соңында Smart 3DES қызмет ету мерзімі факторына көрсетеді, оның кілтінің ұзындығы 168 бит екенін ескере отырып, «біз күткендей қауіпсіз емес» болып табылады.

Франкелова және басқалары, бір жағынан, EuroRadioMAC және кілттерді шифрлау сұлбасын бағалайды [111], бірақ 3DES алгоритмінің компонентіне орталықтанады. Сондықтан кез келген анықталған соққылар кілттер таратумен және EuroRadio өзара алмасудың бір бөлігімен шектеледі. Өздерінің алдыңғы жұмысында авторлар «өрескел күш» әдісімен іздеуге қарағанда аса тиімді үш әлеуетті соққыны, атап айтқанда, дифференциалдық криптоталдау, желілік криптоталдау және белгілі мәтін бойынша соққы, «Дэвис соққысы»

сәйкестендіруден бұрын, кілттерді басқару иерархиясын сипаттайды. Олар DES үшін криптоталдаудың ең күшті типі желілік криптоталдау болып табылады деп көрсетеді, онда кілтті қалпына келтіру үшін 239-224 аумағында уақытша қиындығы бар 243 белгілі ашық мәтін қажет болады. Ал сол уақытта бұл Митчеллмен [108] және Перенел [109] анықтаған соққыға қарағанда белгілі ашық мәтін үшін аса жоғары талапқа ие, атап айтқанда аз уақыт қажет етеді. Кейін авторлар пернетақта кеңістігін азайтатын Митчелл және Пренел және тең авт. тәсіліне ұқсас туған күн соққысын қарастырады. Франкелова [111] соңғы жұмысында авторлар олардың алдыңғы жұмысындағы мүмкін болатын қақтығыстардың ұқсас нәтижелерімен осы соққыны анықтау үшін UML қолданады. Келіспеу мысалдары аталған сипаттамалардың ешқайсысында көрсетілмегендіктен, қосымша тексеріс қажет болуы мүмкін.

KTCS компонентін талдауында Лопес және Агуадо 3DES шектелген өмір ұзақтығын және туған күнге соққы жасау қаупі екі көзден туындайтынын белгілейді: бірнеше пойыз үшін бірдей KMAC кеңінен пайдалану және кездейсоқ сандардың әлсіз генераторы [113]. Соңғы қауіп EuroRadio қол алысу үшін шешуші мәнге ие, себебі пойыз да, РБК да біріккен кезде пойыз бен бекет арасында сеанс кілтін шығаратын бір реттік нөмірлермен алмасады. Егер кездейсоқ сандар генераторы белгілі болса, бұл соққы күрделілігін айтарлықтай төмендетеді. Авторлар сонымен бірге беттік деңгейде, терең талдаусыз әлеуетті баламаларды қарастырады.

Пепин және Вилиотти [110] KTCS қолданылатын кілттерді тарату механизмін талдайды да, 3DES алгоритміне оның стандартты соққыларына орнықтылығын бағалайды. Олар соққыны байланысқан кілт бойынша әдейі пайдаланады және ресурстық шығындар мен ERTMS кілттерін басқаруда қолданылатын 3DES шифрлауды бұзу мүмкіндіктері тұрғысынан құқық бұзушы үшін құнды сандық түрде бағалайды. Алайда олар елестететін соққы қазіргі уақытта миллион долларға бағаланатын қаржы шығындары әсерінен мақсатқа сай емес болып есептеледі. Жұмыста сонымен бірге кілттер таратуға қолданатын 3DES сұлбасына көңіл бөлінеді, онда Евро-Радио сеанстық кілттерімен салыстырғанда айтарлықтай аз кілт болады.

Smart хэштеу / MAC функциясы қанағаттандыруы тиіс үш негізгі ерекшелікті белгілейді [112]:

- Үлгіге кедергі болу – хэш/MAC ескере отырып, құқық бұзушы тек шағын ықтималдылықпен бастапқы кіріс хабарын қалпына келтіру мүмкіндігіне ие болуы тиіс.

- Екінші үлгіге кедергі болу – хэш/MAC ескере отырып, құқық бұзушы тек осы хэш/MAC шағын ықтималдылығына әкелетін кіріс хабарын қалпына келтіру мүмкіндігіне ие олуы тиіс.

- Қақтығысқа кедергі болу – бірдей хеш / MAC әкелетін екі хабарды табу жеткілікті түрде күрделі болу қажет.

Осы ерекшеліктерді пайдаланып, орнатылған ерекшеліктердің алгоритмдеріне қанағаттанғанын растайтын сәйкес қауіпсіздік түрленуін жүзеге асыра отырып, берілген сұлба қауіпсіздігін анықтауға болады. Smart сонымен

бірге game – негіз болған және символдық ретінде пайдалануға болатын екі талдау әдістері жөнінде пікір ұсынудан бұрын, үлгі ретінде Needham-Schroeder және Kerberos секілді хаттамалар келтірілетін орнатылған ұзақ мерзімді симметриялық кілттен жаңа кілттердің түрленуі жөнінде түсінік береді.

EuroRadio MAC пайдалы жүктемелерді аутентификациялаумен және шифрлаумен байланысты зерттеу аумағынан тыс, Карстенсен базалық бекет пен мобильді құрылғы арасындағы мәліметтерді шифрлау үшін GSM және GSM-R пайдаланылатын A5/1 шифрында артықшылық әдісімен қалпына келтіру үшін криптоталдаудың одан да күрделі әдісін қолданады [114]. Массалық соққы ашық мәтін және шифрланған мәтін жұбын ұстап алуды қосады және A5/1 шифрын қосу жолымен түрлі түсті кестені құрады (себебі бұл сұлба кері байланысты жылжытудың желілік регистрі негізінде (LFSR)), кейін трафикті дешифрлау үшін әлеуетті кілт-үміткерлерін шығарады. С. Лу және тең авт. түрлі түсті кестені пайдаланып, соққы уақытын алдында жетілген сағаттар мен минуттардан 9 секундқа дейін қысқартып, уақыт және жады байланысында байланысқан соққыны қолданады, бұл ретте аппараттық қамтамасыз етуі бар коммерциялық дайын өнімде (COTS) 55 күнге уақытты алдын ала есептеу және шамамен 81% сәттілік ықтималдылығы келтіріледі.

3.9 EuroRadio кілттерін қалпына келтіру

Бұл бөлімде біз бір әдісті қарастырамыз, оның көмегімен құқық бұзушы EuroRadioMAC алгоритмімен пайдаланылатын DES үш кілттерінің бірін k_1 қалпына келтіре алады. Осы тарауда ертерек анықтағандай, бұл соққы DES және 3DES шифрлар блогының шағын өлшемін қолдану есебінен мүмкін болады, бұл кезде құқық бұзушыға жай MAC-мекен-жайлар арасындағы қақтығыстарды күту қажет.

3.14 суретте көрсетілгендей, бір кілт екі бірегей хабар бірдей сәйкес MAC ие болатындай етіп құрылуы мүмкін DES дара мерзімдері үшін қолданылады.

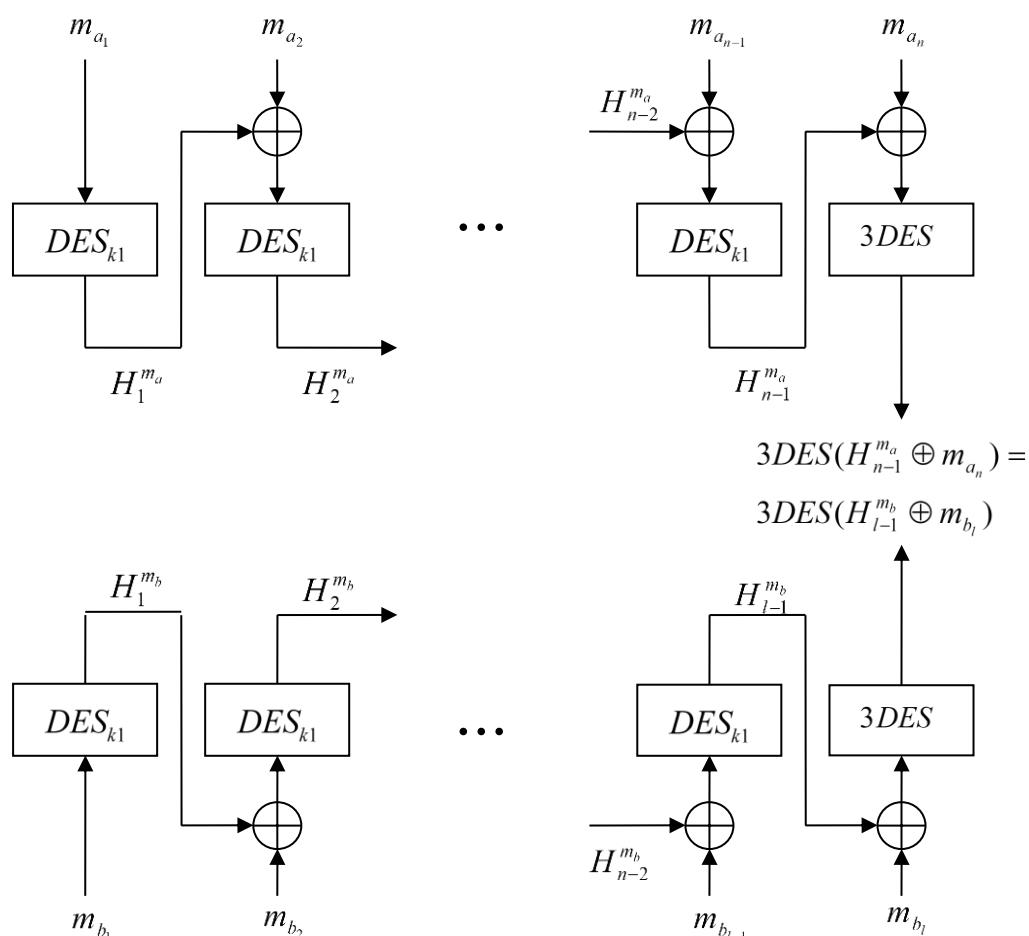
3DES нақты түрленуі белгілі болғандықтан, кіріс мәліметтері 3DES блогы үшін осы екі хабарда бірдей болуы тиіс. Бұл екі шектеуді пайдаланып, әрі қарай сипатталғандай, k_1 қалпына келтіруге болады. EuroRadio MAC келесі үрдісті қолданып, қолданбалы деңгейден хабар анықтау үшін CBC-ұқсас режимді пайдаланады:

Қолданбалы деңгеймен түрленген m берілген хабар 64-биттік блоктарға бөлінеді $m = (m_1, m_2, \dots, m_n)$. Егер m_n соңғы блок 64 бит ұзындыққа ие болмаса, ол тиісті шифрлауды қамтамасыз ету үшін нөлдермен толықтырылады (ISO-9797-ден 1 белгілі бір толтыру әдісімен [31]). m_i әр блок үшін, $i \in \{1, \dots, n-1\}$, MAC-шифрының H_i блогы кейін былай анықталады:

$$H_i = DES_{k_1}(H_{i-1} \oplus m_i)$$

m_1 бірінші блогында, $H_0 = 0$, мұндағы $H_i = 1 \oplus m_i - H_{i-1}$ және m_i үшін XOR операциясының нәтижесі. m_n үшін пайдаланылатын соңғы түрлену біздің соңғы MAC өндіретін 3DES шифрлау нәтижесі болып табылады, яғни MAC (m):

$$\text{MAC}(m) = 3DES_{k_1, k_2, k_3} (H_{n-1} \oplus m_n)$$



Сурет 3.14 – DES k_1 кілтін MAC-тың соқтығысуы арқылы қалпына келтіру

Бұл соққы сәтті болу үшін, ертеректе айтылғандай, бірдей MAC пайдаланатын екі бірегей хабар қажет. N мүмкін болатын мәндер үшін хабар / MAC екі жұбының арасында орын алатын кем дегенде бір MAC келіспеу бойынша бақылау ықтималдылығы төменде келтірілген [49]. Біз DES және 3DES үшін N-ді 264-ке тең деп аламыз. Осы соқтығыс жөнінде көрініс беретін диаграмма 3.14 суретте келтірілген.

$$P = 1 - \prod_{i=1}^{M-1} \left(1 - \frac{i}{N}\right) \approx 1 - e^{-M(M-1)/(2N)} \approx \left(1 - \frac{1}{N}\right)^{M(M-1)/2} \quad (3.9)$$

Қауіпсіздік үшін өте маңызды, теміржол көлігінде қолданылатын жүйелер үшін келісімнің 1% болу ықтималдылығы елеулі. Кері теңдеу (3.9), $P=0,01$, құқық бұзушы келісімнің жетуін бақылауы тиіс хабар/MAC жұбының саны $M = 6,1 \cdot 10^8$ құрайды.

Екеуі бірігіп бірдей MAC пайдаланатын (яғни келісім бар) m_a және m_b екі бірегей хабар және сәйкесінше әр хабарда қамтылатын блоктар саны n және l -ге

тең, MAC алгоритмінде 3DES түрлендіру үшін кіріс мәліметтері (3.14 суретті қараңыз) сондай болу қажет екендігі белгілі. Керісінше, бұл жерден $H_{n-1}^{m_a}$ және $H_{l-1}^{m_b}$ бірдей екені көрінеді: $H_{n-1}^{m_a} \oplus m_{a_n} = H_{l-1}^{m_b} \oplus m_{b_l}$ (3.10)

MAC алгоритмінің осы ерекшелігін пайдаланып, k_1 үшін артық әрекет орындауға болады, себебі құқық бұзушыға m_a және m_b мәтіндік хабарлар белгілі. Осы хабарларды қолданып, құқық бұзушы k_1 барлық мүмкін болатын кілттері үшін және $H_{n-1}^{m_a}$ және $H_{l-1}^{m_b}$ үшін әлеуетті үміткерлерді анықтай алады, яғни 5.4 теңдеуі орындалған жағдайда k_1 мүмкін болатын кілт-үміткері бар.

Бұл соққының қалай жұмыс істейтіні жөнінде нақты көрініс болу үшін екі, үш блоктық хабар үлгісін қарастырамыз.

Мысал. m_a және m_b хабарлары үшін $n = 1, \dots, 3$ болсын. (3.10) теңдеуді пайдаланып, $H_2^{m_a}$ және $H_2^{m_b}$ анықтай аламыз. Бұны базалық түрлендіруге дейін кеңейтуге болады, яғни

$$DES_{k_1}(H_1^{m_a} \oplus m_{a_2}) \oplus m_{a_3} = DES_{k_1}(H_1^{m_b} \oplus m_{b_2}) \oplus m_{b_3},$$

келесі нақты кеңейтуге әкеледі:

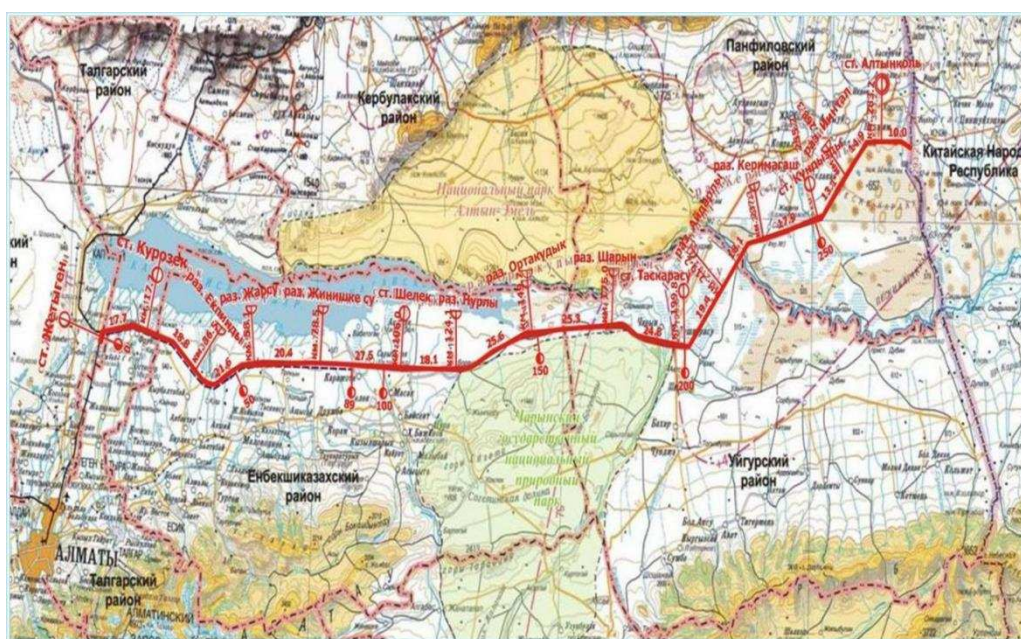
$$DES_{k_1}(DES_{k_1}(m_{a_1}) \oplus m_{a_2}) \oplus m_{a_3} = DES_{k_1}(DES_{k_1}(m_{b_1}) \oplus m_{b_2}) \oplus m_{b_3}$$

$m_{a1}, \dots, 3$ барлық блоктары секілді $m_{b1}, \dots, 3$ соққы жасаушыға белгілі, белгісіз болып қалатын жалғыз k_1 . Алайда, бұл блоктарды пайдалана отырып, біз оны қалпына келтіріп, өзіміздің жеке хабарларды әрекет етуші MAC-мекен-жайларымен қолдан жасау үшін артықшылық әдісімен соққыны қолдана аламыз.

4. МАГИСТРАЛЬДІ ЖЕЛІДЕ АҚПАРАТ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ ҮШІН РАДИОБЛОКТАУ ЖҮЙЕСІН ТӘЖІРИБЕДЕ ҚОЛДАНУ

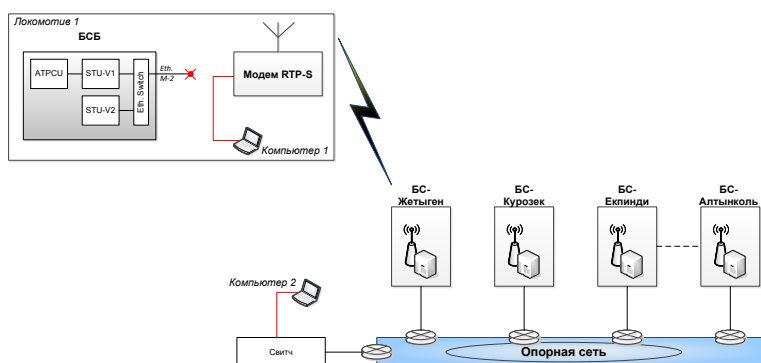
4.1 Эксперименттік сынақ нәтижелері

Радиоблоктау жүйесін тәжірибеде қолдану Алматы магистральді желі бөлімшесінің Жетіген – Алтынкөл телімінде қарастырылған (сурет 4.1) [115]. Тәжірибелік қолдану кезінде радиоблоктау орталығы мен TETRA коммутациялау орталығының байланысы, радиоблоктау орталығын [116] электрлік орталықтандыру жүйелерімен байланыстыру, локомотивтің борт құрылғысын жаңғырту, борт және стационарлық құрылғының жұмыс алгоритмдерін тексеру сұрақтары қарастырылды.



Сурет 4.1 – Тәжірибе жүргізілген телімінің картасы

Бірінші сатыда тәжірибелер 4.2 суретте ұсынылған сұлбаға сәйкес жүргізіледі.



Сурет 4.2 – Тәжірибелер жүргізу сұлбасы – 1 саты

Компьютер 1 локомотивте RTP-S радиомодемiне қосылады, компьютер 2 Жетiген бекетiнiң ЭО постында свитч арқылы TETRA тiреуiш желiсiне қосылады [116].

Екi компьютерде де тiрлi жылдамдықта ұзындығы әр тiрлi UDP топтарын жiберудi жүзеге асыратын бағдарламалық қамтамасыз ету орнатылған (компьютер 2-де «қабылдағыш» және компьютер 1-де «таратқыш»). Топтар санын арттыру немесе азайту арқылы радиоканалға жүктеменi өзгерту орындалады.

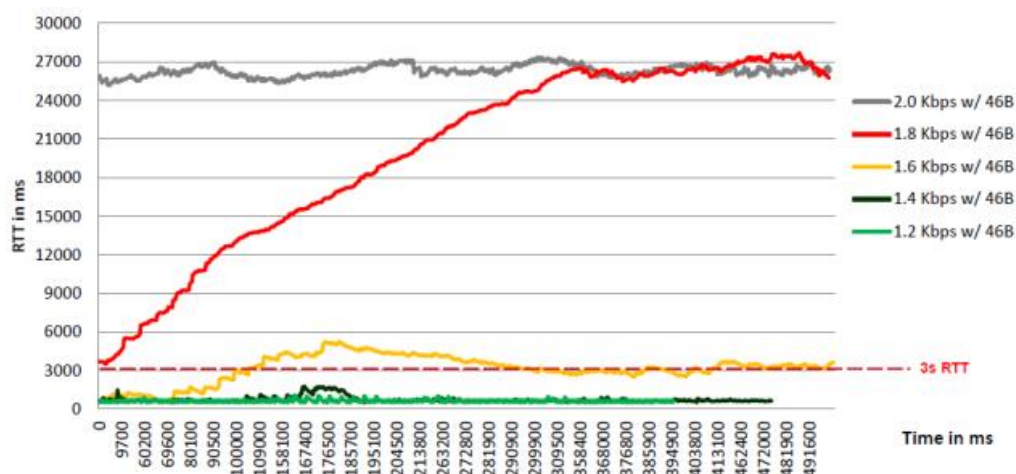
Тәжiрибе жүргiзу кезiнде 1 және 2 компьютерлерде UDP топтарын жiберудi және қабылдауды қамтамасыз ететiн мамандандырылған бағдарламалық қамтамасыз ету қосылады. Тәжiрибеге қатысатын локомотивтер қозғалмай тұрады, басқа жабдықталған локомотивтердiң ПҚИРЖ-Е бойынша қозғалысы жүзеге асырылмайды.

Тәжiрибе уақытында 4.1 кестеде келтiрiлген баптаулар пайдаланылды.

Кесте 4.1 – Алғашқы сатыны өткiзу кезiнде алынған нәтижелер

Топ өлшемі, байт	Мәліметтер тарату каналына жүктеме, кбит/с	Тест ұзақтығы, мин
46	1.2-2.0	105
64	1.2-2.4	30
76	1.2-2.4	30
86	1.2-2.8	105
106	1.2-2.8	30

Каналдың өткiзу қабiлеттiлiгi мәліметтерiн, топтардың өту уақытын, TETRA радиожелісінде топтардың жоғалуы жөнiнде мәліметтердi құрайтын өлшеу нәтижелерi 4.3 – 4.5 суреттерде ұсынылған.



Сурет 4.3 – Өлшемі 46 байт пакеттік ақпараттың өту уақыты

4.3 суретте көрініп тұрғандай, өлшемі 46 байт топтар үшін тәжiрибе мыналарды көрсеттi:

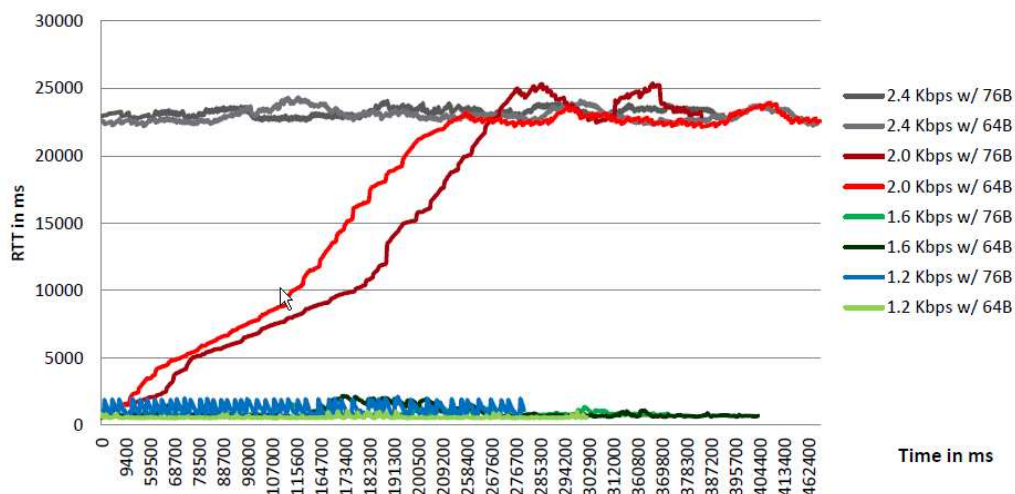
- 1,2-1,4 кбит/с жылдамдықта екi жаққа да топтар тарату уақыты (RTT) 1-

2 секундты құрайды, бұл ретте тарату уақыты барлық тест кезінде тұрақты және іс жүзінде өзгермейді;

- 1,6 кбит/с жылдамдықта екі жаққа да топты тарату уақыты 6 секундқа жетеді;

- 1,8 кбит/с жылдамдықта тарату уақыты 3 секундтан басталады да, тест уақыты кезінде 27 секундқа дейін өседі;

- 2,0 кбит/с жылдамдықта топты тарату уақыты барлық тест кезінде 26 секундты құрайды.



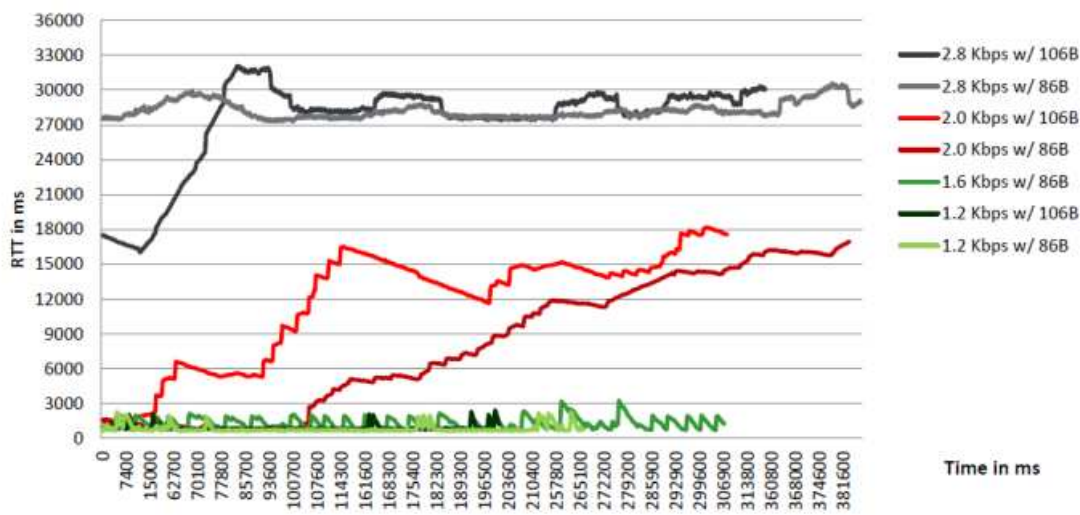
Сурет 4.4 – Өлшемі 64 және 76 байт пакеттік ақпараттың өту уақыты

4.4 суретте көрініп тұрғандай, өлшемі 64 және 76 байт топтар үшін тәжірибе мыналарды көрсетті:

- 1,2-1,6 кбит/с жылдамдықта топты тарату уақыты барлық тест кезінде 1-ден 3 секундқа дейін қалыптасады;

- 2,0 кбит/с жылдамдықта өту уақыты 25 секундқа жетеді, бұл ретте уақыт өте келе тәжірибенің басталу мезетінен өту уақыты артады;

- 2,4 кбит/с жылдамдықта топты тарату уақыты барлық тест кезінде 25 секундты құрайды.

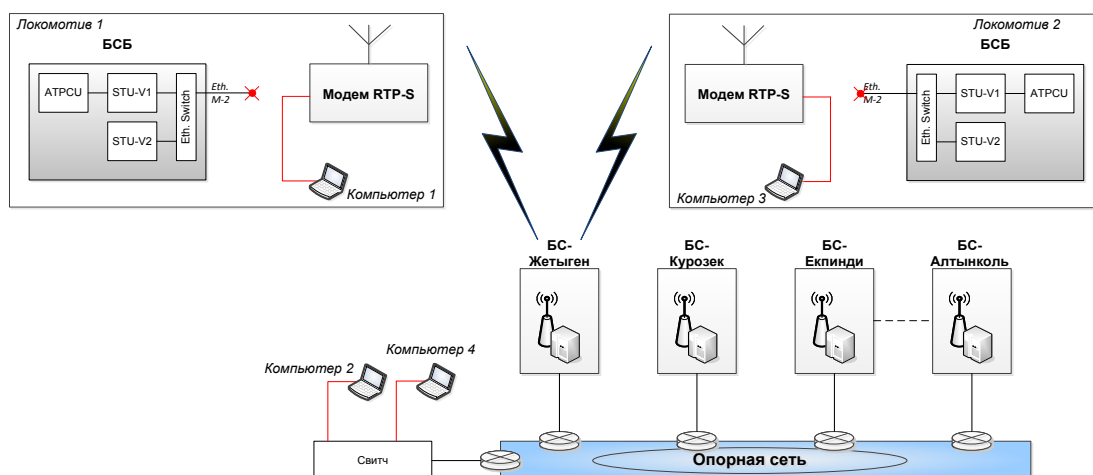


Сурет 4.5 – Өлшемі 86 және 106 байт пакеттік ақпараттың өту уақыты

4.5 суретте көрініп тұрғандай, өлшемі 86 және 106 байт топтар үшін тәжірибе мыналарды көрсетті:

- 1,2-1,6 кбит/с жылдамдықта топты тарату уақыты барлық тест кезінде 1-ден 3 секундқа дейін қалыптасады;
- 2,0 кбит/с жылдамдықта өту уақыты 18 секундқа жетеді, бұл ретте уақыт өте келе тәжірибенің басталу мезетінен өту уақыты артады;
- 2,8 кбит/с жылдамдықта топты тарату уақыты 30 секундты құрайды, бұл ретте өлшемі 106 байт топтар үшін тарату уақыты тест басында 18 секундты құрады да, кейін бірден 32 секундқа дейін өсті.

Екінші сатыда тәжірибелер 4.6 суретте ұсынылған сұлбаға сәйкес жүргізіледі.



Сурет 4.6 – Тәжірибелер жүргізу сұлбасы – 2 саты

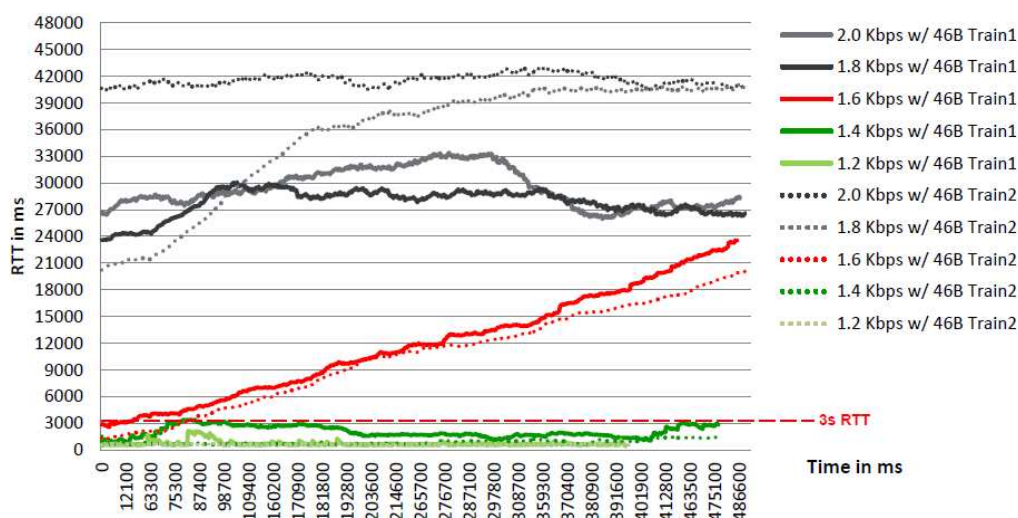
1 және 3 компьютерлер сәйкесінше 1 және 2 локомотивте RTP-S радиомодемiне қосылады, 2 және 4 компьютерлер Жетіген бекетінің ЭО постында свитч арқылы TETRA тіреуіш желісіне қосылады.

Барлық компьютерде де түрлі жылдамдықта ұзындығы әр түрлі UDP топтарын жіберуді жүзеге асыратын бағдарламалық қамтамасыз ету орнатылған (2 және 4 компьютерде «қабылдағыш», 1 және 3 компьютерде «таратқыш»). Топтар санын арттыру немесе азайту арқылы радиоканалға жүктемені өзгерту орындалады.

Топтар алмасу 1 және 2, 3 және 4 компьютерлер арасында жұп бойынша жүргізіледі.

Тәжірибе жүргізу кезінде барлық 4 компьютерде UDP топтарын жіберуді және қабылдауды қамтамасыз ететін мамандандырылған бағдарламалық қамтамасыз ету қосылады. Тәжірибеге қатысатын локомотивтер қозғалмай тұрады, басқа жабдықталған локомотивтердің ПҚИРЖ-Е бойынша қозғалысы жүзеге асырылмайды.

Каналдың өткізу қабілеттілігі мәліметтерін, топтардың өту уақытын, TETRA радиожелісінде топтардың жоғалуы жөнінде мәліметтерді құрайтын өлшеу нәтижелері 4.7 суретте ұсынылған



Сурет 4.7 – Өлшемі 46 байт пакеттің өту уақыты

4.7 суретте көрініп тұрғандай, өлшемі 46 байт топтар үшін тәжірибе мыналарды көрсетті:

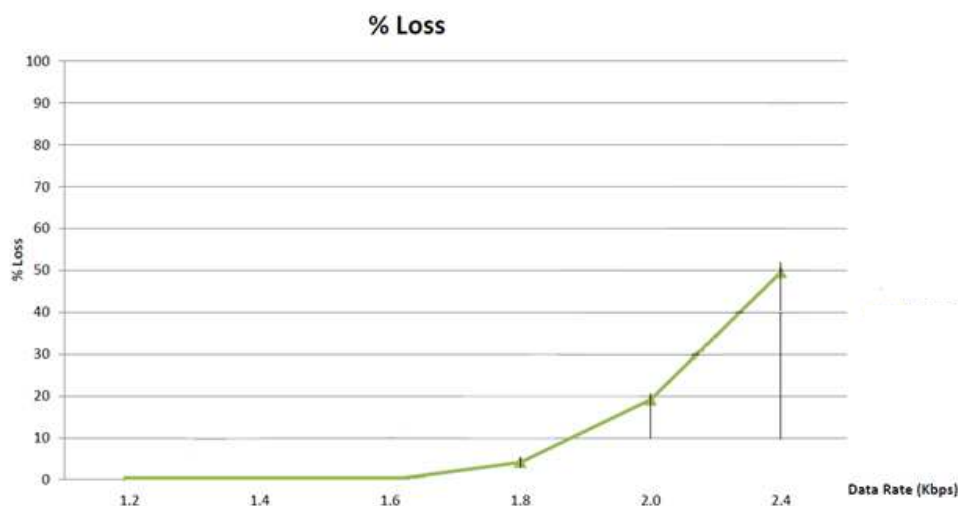
- 1,2-1,4 кбит/с жылдамдықта топты тарату уақыты екі локомотивте де орнатылған модемдер үшін барлық тест кезінде 1-ден 3 секундқа дейін қалыптасады;

- 1,6 кбит/с жылдамдықта уақыт 21 секундқа жетеді, бұл ретте уақыт өте келе тәжірибенің басталу мезетінен өту уақыты артады. Бұл заңдылық локомотивтерде орнатылған екі модемге де тән;

- 1,8 кбит/с жылдамдықта топты тарату уақыты бірінші локомотивте 30 секундқа, екінші локомотивте – 40 секундқа жетті;

- 2,0 кбит/с жылдамдықта топты тарату уақыты бірінші локомотивте 33 секундқа, екінші локомотивте – 42 секундқа жетті.

Радиожеліде топтардың жоғалу пайызы 4.8 суретте ұсынылған.



Сурет 4.8 – Радиожеліде пакетердің жоғалу пайызы

4.8 суретте көрініп тұрғандай, тарату жылдамдығы мен топтарды жеткізу

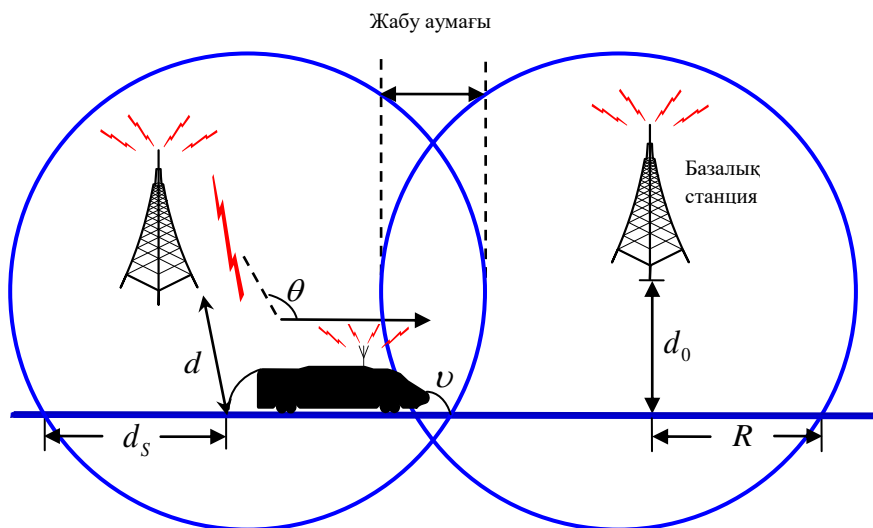
уақытының артуымен олардың жоғалу пайызы да өседі (2,4 кбит/с жылдамдықта 50%-ға дейін) [117].

Осылайша, сандық радиобайланыс жүйесіне қойылатын талаптарға сәйкес қажетті өткізу қабілеттілігі 4,8 кбит/с кем болмауы тиіс, бір жаққа топтар тарату уақыты 0,5 сек, екі жаққа да сәйкесінше 1 сек. артық болмауы қажет.

Жүргізілген тәжірибелер топтың кез келген өлшемінде TETRA стандартының сандық радиобайланыс жүйесінде жүктеме артқан кезде топтардың өту уақыты жоғарылайтындығын көрсетеді. 1,4 кбит/с дейін тарату жылдамдығы үшін жүйе топтардың өту уақыты талаптарын қанағаттандырады. 1,6-2,0 кбит/с жүктемеден бастап топтардың өту уақыты қолайсыз үлкен болады да, 30-40 секундқа жетеді, бұл қойылатын талаптарға сай келмейді. Бұнымен бір уақытта жоғалған топтар пайызы өседі (50%-ға дейін), бұл ретте бірнеше қатар топтың жоғалуы байқалады.

4.2 Теміржол транкингтік байланысы үшін базалық бекетті жабу моделін құру

Транкингтік байланыс үшін базалық бекетті жабудың әзірленген моделі 4.9 суретте келтірілген. Базалық бекеттер бір бірінен $2R$ қашықтыққа қойылу арқылы темір жол бойында орналасқан, бұл бір базалық бекетке қызмет көрсету қашықтығын құрайды. Пойыз рельс бойымен v тұрақты жылдамдықта қозғалады.



Сурет 4.9 – Теміржол транкингтік байланысы үшін базалық бекетті жабу моделі

Пойыз d_s жағдайында болған кезде, $0 \leq d_s \leq 2R$ үшін ағымдағы ұяшық, базалық бекет пен пойыз арасындағы қашықтық құрайды: $d = \sqrt{d_0^2 + (d_s - R)^2}$, мұндағы d_0 – базалық бекет пен теміржол желісі арасындағы қашықтық. Базалық бекет пен теміржол антеннасы арасындағы биіктік айырмашылығын орындамау жөнінде болжамды басшылыққа ала отырып, тура көріну жолының еркін кеңістікте өтуі кезінде жоғалулар былай анықталады [6, б. 58]:

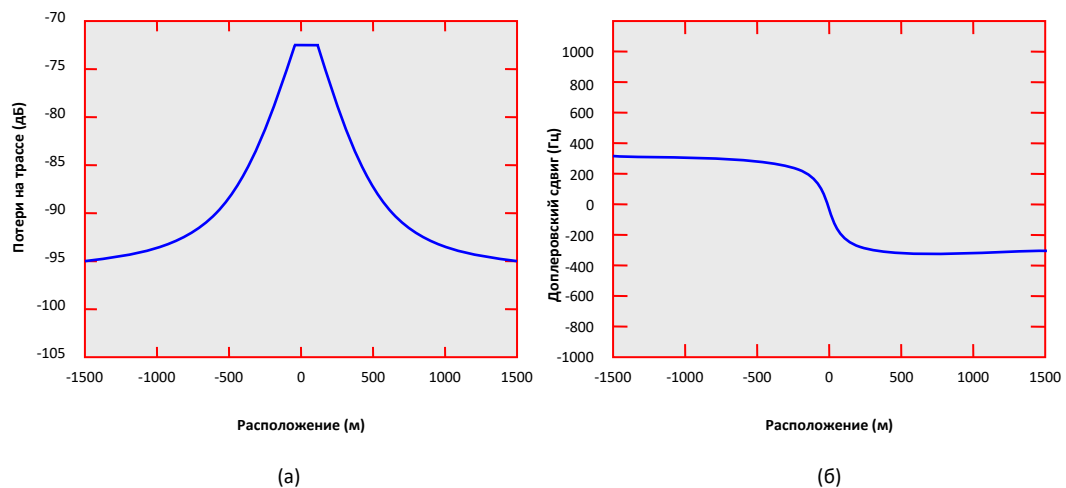
$$L = 20 \log_{10} \left[\frac{4\pi df}{c} \right], \quad (4.1)$$

мұндағы f және c – сәйкесінше сәулелену жиілігі және жарық жылдамдығы.

(4.1)-де L жолдағы жоғалулар d қашықтығы мен f жиілігіне байланысты екені көрініп тұр.

Тәжірибе жүргізу үшін базалық бекет 0 нүктесінде орналасқан, R ұяшық радиусы 1500 м-ге тең, ал v пойыздың қозғалыс жылдамдығы 100 км/сағатқа тең.

4.10 (а) суретте жолдағы жоғалу әсерінен қашықтық пен жиіліктің әсері көрсетілген. Суретте көрініп тұрғандай, жолдағы жоғалулар пойыздың орналасқан жеріне байланысты жылдам өзгереді. Пойыз ұяшық шетіне қарай жүрген кезде жолдағы жоғалулар көп болады да, каналдың сәйкес күйі нашарлайды. Керісінше, пойыз ұяшық ортасына қарай жүрген кезде жолдағы жоғалулар азайып, каналдың сәйкес күйі жақсара бастайды. Осылайша, канал күйінің мерзімді түрде өзгеруі уақыт бойынша қуатты басқару тарату өнімділігіне үлкен әсер ететін факторға алып келеді.



Сурет 4.10 – 450 МГц жиілікте орналасқан жерге байланысты жолдағы жоғалулар мен доплерлік жылжу

Жоғары мобильділік үлкен доплерлік ығысуды және таралуды туғызады. Берілген телімде тура көрінетін жол трактасында энергияның көпсәулелі таралу энергиясына қатынасы қатысты түрде жоғары, ал көпсәулелі таралуды кідірту қатысты түрде аз. 4.10 суретте көрсетілгендей, пойыз рельс бойымен қозғалған кезде f_p доплерлік ығысуды былай есептеуге болады

$$f_p = f_d \times \cos \theta, \quad (4.2)$$

мұндағы

$f_d = \frac{v}{c} \cdot f$ - максималды доплерлік жиілік;

θ - пойыздың тура бағыты мен базалық бекеттен пойызға дейінгі жүру сызығы арасындағы бұрыш. 4.10 суреттегі геометрия жөнінде ақпарат негізінде, біз ие боламыз: $\cos \theta = \frac{R-d_s}{d}$, $0 \leq d_s \leq 2R$.

Осылайша, базалық бекет рельстен қашық орналасқан кезде, яғни $d_0 \gg R$, f_p қатысты түрде төмен болады, себебі θ шамамен 90° . Алайда бұл (4.1) теңдеуге сәйкес жолда үлкен жоғалуға алып келеді. Осылайша, базалық бекетті тағайындауды оңтайландыру кезінде жолдағы жоғалу мен доплерлік ығысу арасында келісім болады [118].

4.10 (б) суретте 450 МГц тасымалдаушы жиілік үшін рельс бойымен доплерлік ығысу көрсетілген:

- f_p пойыз ұяшық арқылы қозғалған кезде максималды оң мәннен максималды теріс мәнге дейін уақыт бойынша өзгереді;
- қозғалыс үрдісінде доплерлік жылжу орын алады;
- f_p өте аз болса да, пойыз базалық бекет арқылы қозғалған кезде, ол жылдам доплерлік көшумен кездеседі;
- f_p пойыз 4.10 суретте көрсетілгендей көрші ұяшықтар арасында жабу аумағына жылжыған кезде максималды теріс мәннен максималды оң мәнге ауысатын болады.

Сымсыз транкингтік байланыс үшін тәжірибеде қолдану алдында доплерлік ығысу мен жылдам доплерлік ауысу мәселелерін шешу қажет. Маңызды доплерлік ығысу синхрондаудың қиындауына және биттер бойынша қателіктердің пайда болу жиілігіне әкелуі мүмкін. Доплерлік ығысу үлкен болғанымен, оның өзгеруі өте аз екендігін айта кеткен жөн, яғни пойыздың жылдамдығы мен орналасқан жері жөнінде нақты ақпарат болған кезде оны дәл бағалап, оңай орнын толықтыруға болады. Сонымен бірге ұяшық ортасындағы жылдам доплерлік ауысу каналды бағалау және доплерлік ығысу үрдісін айтарлықтай қиындатады.

ҚОРЫТЫНДЫ

Диссертацияда жүргізілген зерттеулер негізінде қойылған міндеттер шешіліп, келесі жаңа ғылыми және практикалық нәтижелер алынды:

1. «ҚТЖ» ҰҚ» АҚ инфрақұрылымына қарасты ТАТ құралдарының жалпы жағдайын талдау негізінде қауіпті күйге жақын деп қорытындыланды. Пойыздар қозғалысының қауіпсіздігін және басқаруды тікелей қамтамасыз ететін ТАТ негізгі құрылғыларының 70%-дан астамы ұзақ қызмет ету мерзімімен қолданылады. Егер жақын арада ББОБ қазіргі жүйелерімен жабдықталған теміржол телімдерін қайта құру және жаңғырту шаралары жасалмаса, онда 2025 жылға таман бұл цифр 80%-дан асып кетуі әбден ықтималдығы дәлелденді.

2. «ҚТЖ» ҰҚ» АҚ темір жол желісіндегі қолда бар инфрақұрылымды ескіргенін негіздей отырып, ең жақсы көрсеткіштерін қамтамасыз ететін радиоарна негізінде Қазақстандық пойыздар қозғалысын басқарудың KTCS ұлттық жүйесінің архетиктурасы алғаш рет әзірленді. Белгілі қорғаныс құралдарын қолдану негізінде қауіпсіздікке байланысты келесі сипаттамаларға қол жеткізіледі: хабарламалардың түпнұсқалығы, тұтастығы, уақтылығы және дәйектілігі. TETRA стандартты сандық технологиялық радиобайланыс жүйесінде ақпараттық қауіпсіздік және ақпаратты қорғау мәселелері шешілді. Ұсынылған алгоритмдердің тиімділігі TETRA жүйелік жүйелік хаттамасының архитектуралық моделінде көрсетілген.

3. KTCS жүйесіндегі ақпаратты қауіпсіз таратудың көп деңгейлі моделіне талдау жасалды. KTCS элементтері арасында ақпарат алмасу келтірілген. GSM-R және TETRA желісінің архитектуралары талданып, TETRA-ға KTCS-тен ақпарат берілуіне әсер ететін факторлар анықталды. Радиоарна арқылы деректерді беру кезінде аутентификация және кілттерді құру тізбегі және MAC криптографиялық талдауы ұсынылған.

4. Радиоблоктау жүйесін тәжірибеде қолдануды Алматы магистральді желі бөлімшесінің Жетіген – Алтынкөл телімінде эксперименттік сынақ нәтижесінде TETRA стандартының сандық радиобайланыс жүйесінде жүктеме артқан кезде ақпараттың өту уақыты жоғарылайтындығын көрсетеді. 1,4 кбит/с дейін тарату жылдамдығы үшін жүйе ақпараттың өту уақыты талаптарын қанағаттандырады. 1,6-2,0 кбит/с жүктемеден бастап ақпараттың өту уақыты қолайсыз үлкен болады да, 30-40 секундқа жетеді, бұл қойылатын талаптарға сай келмейді. Бұнымен бір уақытта жоғалған ақпараттар пайызы өседі (50%-ға дейін), бұл ретте бірнеше қатар ақпараттың жоғалуы анықталды.

5. Сымсыз транкингік байланыс үшін тәжірибеде қолдану алдында доплерлік ығысу мен жылдам доплерлік ауысу мәселелерін шешу қажеттілігін негізге ала отырып, транкингік байланысы үшін базалық бекетті жабу моделі әзірленді.

6. Темір жол транкингік байланысы үшін базалық станцияны жабу моделі әзірленді. Тәжірибе арқылы радио желісіндегі пакеттердің жоғалу пайызы, жолдағы шығындар және 450 МГц жиіліктегі орналасқан жеріне байланысты доплердің ығысуы шектелді.

ПАЙДАЛАНҒАН ӘДЕБИЕТТЕР ТІЗІМІ

- 1 Послание Президента Республики Казахстан Н. Назарбаева народу Казахстана. 10 января 2018 года. «Новые возможности развития в условиях четвертой промышленной революции». <https://www.akorda.kz/ru>. 23.11.2018
- 2 Государственная программа «Цифровой Казахстан». Программа утверждена постановлением Правительства Республики Казахстан № 827 от 12.12.2017 года. <https://online.zakon.kz/>. 23.11.2018.
- 3 Инвестиционная программа акционерного общества «Национальная компания «Қазақстан темір жолы» на 2014 год. Утверждена Комитетом транспорта и путей сообщения Министерства транспорта и коммуникаций Республики Казахстан от 27 сентября 2013 года № 43. – С. 1-2.
- 4 Государственная программа развития и интеграции инфраструктуры транспортной системы Республики Казахстан до 2020 года. Утверждена указом Президента Республики Казахстан от 13 января 2014 года № 725. (с изменениями и дополнениями, внесенными Указом Президента РК от 26 мая 2015 года № 30). – С. 5-7.
- 5 Бакышева А. Дороги независимости: 2,5 тысячи километров за 25 лет! <https://railnews.kz/>. 3.12.2018
- 6 Сансызбай К.М., Куандыков А.А. Метод взаимодействия по радиоканалу, обеспечивающий информационную безопасность движения поездов // Программа XLIV Международной научно-практической конференции КазАТК им. М. Тынышпаева «Инновационные технологии на транспорте: образование, наука, практика», – Алматы: 2020. – С. 56-59.
- 7 Бахтиярова Е.А., Сансызбай К.М. Сравнительный анализ микропроцессорной централизации стрелок и сигналов // Вестник Евразийского национального университета имени Л.Н. Гумилева Серия «Технические науки и технологии». – Астана, 2018, – №2 (123). – С. 30-36.
- 8 Программа развития железнодорожного транспорта Казахстана на долгосрочную перспективу. <http://miid.gov.kz/ru/>. 8.12.2018.
- 9 Куандыков А.А., Сансызбай Қ.М. Темір жол автоматика және телемеханика жүйелерінде ақпараттық қауіпсіздікті қорғау әдістері // Қазақстан Британ техникалық университетінің хабаршысы. – Алматы, 2019. – № 16. – Б. 353-359.
- 10 Ададуров С.Е., Диасамидзе С.В., Корниенко А.А., Сидак А.А. Международная кибербезопасность на железнодорожном транспорте: методологические подходы и нормативная методическая база // Вестник ВНИИЖТ. – Москва, 2015. – № 6. – С. 9-15.
- 11 СТ РК 1824-2008 Система железнодорожной автоматики и телемеханики. Термины и определения. – 2 с.
- 12 ГОСТ Р 53431-2009 Автоматика и телемеханика железнодорожная. Термины и определения. <http://docs.cntd.ru>. 17.02.2019.

- 13 Теєга Г., Власенко С. Системы автоматики и телемеханики на железных дорогах мира: учебное пособие для вузов ж.д. транспорта / под ред. Теєга Г., Власенко С. – М.: Интекст, 2010. – С. 7-13.
- 14 Маркетинговое исследование рынка систем железнодорожной автоматики / Уральский федеральный университет им. Первого Президента России Б.Н. Ельцина. – Екатеринбург, 2014. – С. 8-12.
- 15 Стратегия инновационно-технологического развития группы компаний акционерного общества «Национальная компания «Қазақстан темір жолы» на период 2013 – 2018 годы. – Астана, 2013. – С. 10-20.
- 16 Техническая политика департамента автоматики и телемеханики и телекоммуникации на период с 2017 по 2022г.г. АО «Национальная компания «Қазақстан темір жолы». – Астана, 2017. – С. 5-12.
- 17 АГО-5 Отчет о технических средствах сигнализации и связи по структурным подразделениям и дочерним организациям АО «НК «ҚТЖ» по состоянию на 1 января 2018 года.
- 18 Концепции модернизации и производства систем железнодорожной автоматики и телемеханики. – Астана, 2018. – С. 16-31.
- 19 СП 235.1326000.2015 Железнодорожная автоматика и телемеханика. Правила проектирования. <http://docs.cntd.ru/>. 22.04.2019.
- 20 Кравцов Ю.А. Системы железнодорожной автоматики и телемеханики. – М.: Транспорт, 1996. – 400 с.
- 21 Бахтиярова Е.А., Сансызбай К.М., Чигамбаев Т.О. Обоснование целесообразности модернизации систем железнодорожной автоматики и телемеханики // Научно-технический журнал «Новости науки Казахстана». – Алматы, 2020. – № 3. – С. 132-144.
- 22 Бахтиярова Е.А., Сансызбай К.М. «Анализ в случае неосуществления модернизации существующих систем ЖАТ в Республике Казахстан» // Материалы всероссийской научно-технической конференции с международным участием. – Омск, 2019. – С. 97-104
- 23 Winter P., ed., Compendium on ERTMS. Eurailpress, first ed., 2009. ISBN 978-3-7771-0396-9.
- 24 Ruesche S.F., Steuer J., Jobmann K. The European Switch. A Packet-Switched Approach to a Train Control System // IEEE Vehicular Technology Magazine. – 2008. – Vol. 3(3). – P. 37-46.
- 25 Куандыков А.А., Сансызбай Қ.М. Әлемдік масштабтағы теміржол автоматика және телемеханика жүйелерінің даму тенденциялары мен принциптері // «Көліктегі инновациялық технологиялар: білім ғылым тәжірибе» атты ХLI Халықаралық ғылыми-практикалық конференцияның материалдары. – Алматы, 2017. – Б. 11-16.
- 26 Kastell K., Bug S., Nazarov A., Jakoby R. Improvements in Railway Communication via GSM-R // in Proceedings of the 63rd IEEE Vehicular Technology Conference (VTC 2006-Spring). – IEEE, 2006. – P. 3026–3030,
- 27 Lockyear M.J. Changig track: Moving-block railway signaling // IEE Reviews. – 1996. Vol. 42, № 1. – P. 21-25

28 Transit Capacity and Quality of Service Manual, Part 5: Rail Transit Capacity. Chapter 2. Train control and signaling // Moving-Block Systems. 2nd Edition. Transportation research board. Washington D.C. 2003.

29 Gallamore R.E. Tests of RTS train traffic control system // Railway Gazette International. - 2000. – P. 359-362.

30 Giuliari A., Pellegrini M., Savio S. Moving Block and Traffic Management in Railway Applications. // The EC Project COMBINE. – CompRail, 2000. – Vol.139. – P.261-275.

31 Eichenberger P. Increase in throughput using ETCS system // Signal und Draht. – 2007. – № 3. – P. 6-13.

32 Тега Г., Власенко С. Системы автоматики и телемеханики на железных дорогах мира: учебное пособие для вузов ж.д. транспорта / под ред. Тега Г., Власенко С. – М.: Интекст, 2010. – С.261 – 274.

33 Geisder A., Schwah M. ETCS уровня 2 с альтернативными системами радиосвязи // Железные дороги мира (ЖДМ). – Москва, 2013. – № 10. – С.57-63.

34 European Council, Council Directive 96/48/EC of 23 July 1996 on the interoperability of the trans-European high-speed rail system // Official Journal of the European Communities. – 1996. – № L 235. – P. 6-24.

35 European Commission, Commission Decision 2001/260/EC of 21 March 2001 on the basic parameters of the command-control and signalling subsystem of the trans-European high-speed rail system referred to as 'ERTMS characteristics' in Annex II(3) to Directive 96/48/EC // Official Journal of the European Union. – 2001. – № L 93. – P. 53-56.

36 Carpinelli V., Missoumi A., Brutin E., Filippini C., ERTMS Atlas 2012. International Union of Railways (UIC), third ed., 2012. ISBN 978-2-7461-2078-5.

37 Brutin E. ERTMS: Global dimensions, global challenges // European Railway Review. – 2012. – Vol. 18(3). – P. 36–38.

38 EN 50126 Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS).

39 EN 50128 Railway applications – Communication, signalling and processing systems - Software for railway control and protection systems.

40 EN 50129 Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signaling.

41 IEC 61508 Functional safety of electrical, electronic, programmable electronic safety-related systems.

42 Sansyzbay K.M., Kuandykov A.A. The development of the national microprocessor system «KTCS» // Proceedings of international scientific-practical conference «Auezov readings-15: Third modernization of Kazakhstan – New concepts and modern solutions», dedicated to 120 years of Mukhtar Omirkhanovich Auezov. – Shymkent, 2017. – P. 276-279.

43 EN 50155 Railway applications – Electronic equipment used on rolling stock.

44 Строительства микропроцессорной системы интервального регулирования движением поездов на участке Кандыагаш – Никельтау. Пояснительная записка 281-ЦУКС/1011-ПЗ. – Алматы, 2011. – С. 17-40.

45 410905-00-00-00-00 ТР. Система интервального регулирования движения поездов KTCS для участка Кандыагаш – Никельтау. – Астана, 2013. С. 16-21.

46 18082013.ТР.С Система интервального регулирования движения поездов KTCS. Техническое решения. – Астана, 2013. – С. 12-25.

47 ГОСТ 33890-2016 «Система счета осей. Требования безопасности и метода контроля» <https://www.egfntd.kz/>. 15.06.2019.

48 Система точечной передачи данных на основе реперных датчиков (балис). Инструкция по монтажу, регулировке и вводу в эксплуатацию. – Астана, 2011.

49 Технические решение на построение системы СЦБ и связи по проекту «Строительство системы интервального регулирования движением поездов на участке Кандыагаш-Никельтау» в соответствии с техническими требования к Казахстанской системе управления движением поездов (KTCS) АО «НК «КТЖ» на базе технологий, продуктов и систем компаний «Alstom Transport», ЗАО «НПЦ «Промэлектроника», ЗАО «Информтехника и Промсвязь». – Астана, 2015. – С.12-27.

50 Сансызбай Қ.М., Спабекова М.Ж. Түркістан – Шиелі теліміне поездар қозғалысын интервалды реттеу жүйелерін жетілдіру жолын талдау // ҚР президенті Н.Ә.Назарбаевтың «Нұрлы жол – Путь в будущее» жолдауына арналған «Көлік ғылымы және инновация» Халықаралық ғылыми-практикалық конференциясының материалдары. – Алматы, 2015. – Б. 177-181.

51 Сансызбай Қ.М., Куандыков А.А. Еліміздің темір жол желілерінде ұлттық «Kazakhstan Train Control Systems» жүйесін енгізу арқылы пойыздар қозғалысының ақпараттық қауіпсіздігін қамтамасыз ету // «Интеллектуалдық ақпараттық және коммуникациялық технологиялар – «Қазақстан-2050» стратегиясы аясында үшінші индустриалды революцияны жүзеге асырудың құралы»: V Халықаралық ғылыми практикалық конференция баяндамалар жинағы. – Астана, 2018. – Б. 460-463.

52 Локомотивный бортовой терминал стандарта. TETRA. Технические требования. – Астана, 2012. – С. 3-8.

53 Степанова И.В. Проектирование систем радиотелефонной связи стандарта TETRA // Т-Сomm: Телекоммуникации и транспорт. – Москва, 2017. – Том 11, №1. – С. 10-16.

54 Шаманов В.И. Системы интервального регулирования движения поездов с цифровыми радиоканалами // Автоматика на транспорте. – Санкт-Петербург, 2018. – № 2, том 4. – С. 223-240.

55 Технические решение по реализации системы KTCS интервального регулирования движением поездов на участке Кандыагаш-Никельтау в соответствии с техническими требования к Казахстанской системе управления движением поездов (KTCS) АО «НК «КТЖ» на базе технологий, продуктов и

систем компаний RDCS, Frauscher, Promelektronika, Hima, Men, Sysgo. – Алматы, 2012. – С. 12-15.

56 RBC-RBC Safe Communication Interface Subset-098 v1.0.0.

57 Попов П.А., Королев И.Н. Системы управления движением по радиоканалу // Автоматика, связь, информатика (АСИ). – Москва, 2011. – №7. С. 26-27.

58 Попов П.А., Ададуров А.С. Общие принципы работы системы ITARUS-АТС // Автоматика, связь, информатика (АСИ). – Москва, 2010. – №7. С. 9-10

59 Венцевич Л.Е. Локомотивные устройства обеспечения безопасности движения поездов и расшифровка информационных данных их работы. – М.: Маршрут, 2006. – 328 с.

60 Устройство КЛУБ-У. Руководство по эксплуатации 36991-00-00 РЭ. – 260 с.

61 Лисенков В.М., Бестемьянов П.Ф., Леушин В.Б Системы управления движением поездов на перегонах. – Москва, 2009. С. 34 – 36.

62 Noh S.H., Kim T.J. A comprehensive analysis of map matching algorithms for ITS // Hongik Journal of Science and Technology. – 1998. – Vol. 9. – P.303-313.

63 Jae-seok YANG, Seung-pil KANG The map matching alghorithm of GPS data with relatively long polling time intervals // Journal of the Eastern Asia Society for Transportation Studies. – 2005. – Vol. 6. P. 2561 – 2573.

64 Попов П.А. Федоров А.Ю. Ададуров А.С. Система спутниковой навигации на пожарных поездах // Автоматика, связь, информатика (АСИ). – Москва, 2011. – №7. – С. 26-27.

65 Carpinelli V., Missoumi A., Brutin E., Filippini C. ERTMS ATLAS 2012 // International Union of Railways (UIC). – Paris, 2012. – 258p.

66 Попов П.А. Стохастическое моделирование движения поездов в задачах интервального регулирования // Наука и транспорт. – Москва, 2013. – № 2. – С.18-19.

67 Веретягин А.А. Теория обработки сигналов и автоматического управления в радиоэлектронных системах. – Спб.: Министерство обороны, 1992. – 718 с.

68 Тильк И.Г. Новые устройства автоматики и телемеханики железнодорожного транспорта. – Екатеринбург: УрГУПС, 2010. – 168 с.

69 EN 50159 Railway applications – Communication, signalling and processing systems – Safety-related communication in transmission systems.

70 EN 50159-2 Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling.

71 Зорин В.И., Алабушев И.И., Титов В.П. Локомотивные устройства обеспечения безопасности движения. ЦПИИТЭИ. Серия «Сигнализация и связь» - М.: 2004. – С. 39-60.

72 Гью Б. Система передачи данных с защитой от опасных отказов // Alsthom Review. – 1987. – № 7. – С. 51-62.

73 Вернер М. Основы кодирования. - М.: Техносфера. 2004. – 288 с.

- 74 Фомин А.Ф. Вованов Ю.В., Помехоустойчивость систем железнодорожной радиосвязи. – М.: Транспорт, 1987. – 295 с.
- 75 Харкевич А.А. Борьба с помехами. – М.: Наука, 1965. – 276 с.
- 76 Бернард С. Цифровая связь. Теоретические основы и практическое применение / под ред. С. Бернард. – Изд. 2-е, пер с англ. – М: Издательский дом «Вильямс», 2004. – 1104 с.
- 77 Захаров А.В. «Особенности построения модемов в цифровых системах технологической радиосвязи стандарта TETRA на железнодорожном транспорте».- М.: Труды ВНИИАС 2005. – выпуск 2. С. 36-38.
- 78 Розенберг Е.Н., Шубинский И.Б. Аналитические методы доказательства функциональной безопасности систем железнодорожной автоматики и связи // Безопасность движения поездов: Тезисы докладов четвертой научно-практической конференции. – М.: 2003. – С.11-22.
- 79 Сердюков П.Н., Бельчиков А.В., Дронов А.Е. и др. Защищенные радиосистемы цифровой передачи информации. – М.: АСТ, 2006. – 403 с.
- 80 Зорин В.И., Алабушев И.И., Новиков В.Г.. Применение измерителей расстояния в устройствах обеспечения безопасности движения поездов // Автоматика, связь, информатика. – Москва, 2007. – № 10. С. 25-26.
- 81 Маргарян С.А. Радиосети для систем управления поездами // Автоматика, связь, информатика (АСИ). – Москва, 2014. – №4. – С.19-23.
- 82 Тильк И.Г. АЛС с использованием радиоканала // Автоматика, связь, информатика (АСИ). – 2010. – № 7. – С. 7-8.
- 83 Bakhtiyarova E.A., Kemel'bekov B.Zh., Bekmagambetova Zh.M., Lipskaya M.A., Chigambaev T.O., Orazymbetova A.K., Ospanova N.A., Mekebaeva A.K., Khan V.A., Mamilov B.E. Quality of speech reproduction using stochastic digital systems of information transfer with its statistical compaction // Russian Physics Journal. – 2017. – Vol. 60, № 1. – P. 190-195.
- 84 André Lisker, Kersten Kanis. Inbetriebnahme des DSTW Annaberg-Buchholz Süd. SIGNAL+DRANT | Ausgabe 04/2018.
- 85 Смагин Ю.С., Ефремов А.Ю. Первая цифровая система централизации в Германии // Железные дороги мира. – Москва, 2018. – № 8. – С. 63-67.
- 86 Власенко С.В., Лунев С.А., Соколов М.М. Централизованная и децентрализованная архитектура постов управления станциями // Автоматика, связь и информатика. – Москва, 2019. – № 3. – С. 22-25.
- 87 Hansen L., Booth P., Lautenschlager W. ETCS/GSM-R Quality of Service - Operational Analysis // Tech. Rep. EEIG: 04E117, EEIG ERTMS Users Group, October 2005.
- 88 Stanley P., ed., ETCS for Engineers. Germany: Eurailpress, first ed., 2011. ISBN 978-3-7771-0416-4.
- 89 Yuan J., Hansen I.A., Optimizing capacity utilization of stations by estimating knock-on train delays // Transportation Research Part B: Methodological – 2007. – Vol. 41(2). – P. 202-217.
- 90 Taylor D., Lofmark N., McKavanagh M., Survey on operational communications (study for the evolution of the railway communications system) //

Final report for the European Railway Agency 37760-496v04, Analysys Mason, February 2014. <http://www.era.europa.eu/>. 22.04.2020.

91 Barbu G. SATLOC – система управления движением поездов на базе спутниковой навигации для малодеятельных линий // Железные дороги мира (ЖДМ). – Москва, 2014. – №6 – С. 63-67.

92 GSM-R Interfaces Class 1 Requirements Subset-093 v2.3.0.

93 Jacobsen P. ETCS уровня 3 и сеть TETRA на монорельсовой дороге в Вуппертале // Железные дороги мира (ЖДМ). – Москва, 2014. – №7 – С.54-56.

94 Мыльников П.Д. Обеспечение информационной безопасности в спецификациях ERTMS. Управление ключами и защита данных // Интеллектуальные системы на транспорте: материалы IV междунар. науч.-практич. конф. «Интеллект Транс-2014». – СПб.: ПГУПС, 2014. – С. 498–500.

95 ERTMS/ETCS. Subset-114. KMC-ETCS Entity Off-line KM FIS. Vol. 1.0.0.

96 ERTMS/ETCS. Subset-038. Off-line Key Management FIS. Vol. 3.0.0.

97 ERTMS / ETCS. Subset-037. Euroradio FIS. Vol. 3.0.0.

98 Коржик В.И., Просихин В.П., Яковлев В.А., Коржик В.И. Основы криптографии. – СПб.: СПбГУТ, 2014. – 276 с.

99 Осяев А.Т., Никифоров В.А., Осяев А.Т. О системе обслуживания локомотивов за рубежом // Вестник ВНИИЖТ. – Москва, 2012. – № 5. – С. 56-62.

100 ETSI. EN 300 392-7 v3.3.1 (2012-07): Terrestrial trunked radio (TETRA); voice plus data; part 7: Security, 2012.

101 Dolev D., Yao A.C. On the security of public key protocols. Information Theory // IEEE Transactions. – 1983. – Vol.29(2):198208.

102 Sesia S., Toufik I., Baker M., LTE – The UMTS Long Term Evolution From Theory to Practice. John Wiley & Sons, 2011. ISBN 978-0-470-66025-6.

103 Holma H., Toskala A., LTE for UMTS - OFDMA and SC-FDMA Based Radio Access. John Wiley & Sons, first ed., 2009. ISBN 978-0-470-99401-6.

104 Фергюсон Н., Шнайер Б. Практическая криптография / Пер. с англ. – М.: Издательский дом Вильямс, 2005. – 424 с.

105 ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

106 Euroradio FIS Subset-037 v2.3.0 <http://www.era.europa.eu/>. 25.04.2020.

107 BSI, “BS ISO/IEC 9797-1:2011 – Information technology. Security techniques. Message authentication codes (MACs). Mechanisms using a block cipher,” 2011. <https://bsol.bsigroup.com/>. 27.04.2020.

108 Mitchell C.J., Key recovery attack on ANSI retail MAC // Electronics Letters. – 2003. – Vol. 39, № 4. P. 361-362.

109 Preneel B., van Oorschot P.C, Key recovery attack on ANSI X9. 19 retail MAC // Electronics Letters. – 1996. – Vol. 32, № 17. – P. 1568–1569.

110 Pépin F., Vigliotti M.G. Risk Assessment of the 3Des in ERTMS. Cham: Springer International Publishing. – 2016. – P. 79-92.

- 111 Franekova M., Rastocny K., Janota A., Chrtiansky P. Safety Analysis of Cryptography Mechanisms used in GSM for Railway // International Journal of Engineering. – 2011. – Vol.11, № 1. – P. 207-212.
- 112 Smart N.P., Cryptography Made Simple. Cham: Springer International Publishing, 2016. <https://doi.org/>. 2.05.2020.
- 113 Lopez I., Aguado M., Cyber security analysis of the European train control system // IEEE Communications Magazine. – 2015. – Vol. 53, № 10. – P. 110-116.
- 114 Karstensen L. GSM A5/1 rainbow tables in Oslo, Norway, 2015. <https://lassekarstensen.wordpress.com/>. 2.05.2020.
- 115 Концепции модернизации и производства систем железнодорожной автоматики и телемеханики. – Астана, 2018. – С. 88-90.
- 116 Технический анализ нагрузочных испытаний системы радиосвязи стандарта TETRA. – Алматы, 2016. – С. 15-16.
- 117 Sansyzbay K.M., Kuandykov A.A., Bakhtiyarova Ye.A., Vlasenko S.V., Mamyrbaev O.Zh. Radio communication channel interaction method, maintaining train performance information security // Journal of Theoretical and Applied Information Technology. – Islamabad, 2020. – Vol.98. № 06. – P. 957-969.
- 118 Бахтиярова Е.А., Дуйсебекова К.С., Чигамбаев Т.О., Сансызбай К.М. Практическое применение системы радиоблокировки для обеспечения информационной безопасности на магистральной сети // Промышленный транспорт Казахстана. – Алматы, 2020. – №1. – С. 111-117.

ҚОСЫМША А

Енгізу актісі

«ҚАЗАҚСТАН ТЕМІР ЖОЛЫ» ҰЛТТЫҚ КОМПАНИЯСЫ»
АКЦИОНЕРЛІК ҚОҒАМЫНЫҢ «АВТОМАТТАНДЫРУ
ЖӘНЕ ЦИФРЛАНДЫРУ ДИРЕКЦИЯСЫ»
ФИЛИАЛЫ



ФИЛИАЛ АКЦИОНЕРНОГО ОБЩЕСТВА
«НАЦИОНАЛЬНАЯ КОМПАНИЯ «КАЗАХСТАН ТЕМІР
ЖОЛЫ» - «ДИРЕКЦИЯ АВТОМАТИЗАЦИИ И
ЦИФРОВИЗАЦИИ»

010000, Нур-Султан қ-сы, Д. Қонаев к-сі, 6
Тел. +7(7172)60-61-00
E-mail: Nakisheva_Sh@Railways.kz
<http://www.railways.kz>

010000, г. Нур-Султан, ул. Д.Қонаев, 6
Тел. +7(7172)60-61-00
E-mail: Nakisheva_Sh@Railways.kz
<http://www.railways.kz>

6 D.Kunaev Str., Nur-Sultan 010000
Tel. +7(7172)60-61-00
E-mail: Nakisheva_Sh@Railways.kz
<http://www.railways.kz>

"КТЖ" ҰК" АҚ "АЦД"	
Шығыс №	бет
« » 20 ж.	
АО "НК "КТЖ" - "ЦДАН"	
Исходящий №	лист
« 17 » 09	20 20 г.

АКТ

о внедрении результатов докторской диссертационной работы Сансызбай Қанибек Мұратбекұлы

на тему: «Обеспечение информационной безопасности для систем железнодорожной автоматики и телемеханики»

Результаты исследований диссертационной работы применяются в опытно-конструкторских работах и научно-технических проектах АО «НК «КТЖ» по следующим направлениям:

- внедрение элементов предлагаемой архитектуры национальной системы управления движения поездов;
- разработка программы обновления устройств железнодорожной автоматики и телемеханики на основе представленного анализа и рекомендаций;
- расчеты по снижению уровня эксплуатационных затрат и улучшению показателей пропускной способности на участках железнодорожной магистральной сети.

При этом, практической ценностью исследования, выполняемого докторантом Сансызбай Қ.М. является проведение сравнительного анализа железных дорог мира по принятым нормам безопасности для передачи данных в системах управления движением поездов. А так же разработка рекомендаций для АО «НК «КТЖ» по внедрению современных цифровых технологий в системах централизации, с возможной перспективой их дальнейшей модернизации и глобализации в железнодорожные комплексы, центры. Кроме того, расчеты экономической эффективности использования современных устройств СЦБ были использованы при подготовке технико-экономического обоснования для реконструкции инфраструктуры основных транзитных коридоров. Ряд предложенных решений одобрены техническим советом АО «НК «КТЖ» в рамках принятия результатов хозяйственного договора «Концепция модернизации и производства систем железнодорожной автоматики и телемеханики», выполненного докторантом в качестве руководителя проекта по заказу АО «Транстелеком» для АО «НК «КТЖ» в период с декабря 2017 г. по ноябрь 2018 г. (№248/02 от 14.12.2017).

Исполнительный директор
по производству филиала АО «НК «КТЖ» -
«Дирекция автоматизации и цифровизации», д.т.н.

С.Омаров

Главный менеджер департамента
по развитию и внедрению железнодорожной
автоматики, телемеханики и телекоммуникаций

М.Батырханов

Менеджер функционального направления
по развитию и внедрению железнодорожной
автоматики и телемеханики

К.Орабоев

ҚОСЫМША Б
Енгізу анықтамасы



HYUKSHIN Engineering Co., Ltd

Passion for Innovation since 1955 <http://www.hyukshin.co.kr>

**Certificate of implementation on the results of scientific developments of
Kanibek Sansyzbay, doctoral student of the International University of
Information Technologies on the theme: «Ensuring information security for
railway automation and telemechanics systems».**

For the purpose of improvement of applied decisions on use of system of a digital radio communication of standard «TETRA» with functions of transfer of the operative information between subsystems of multilevel control system and maintenance of safety of movement of trains, results of practical application of the given system, on a site of a railway network of Republic Kazakhstan, namely Zhetygen - Altynkol have been used.

The obtained results on data loss and transmission delay depending on the set transmission speed and packet size allowed to develop an optimal model of polygon coverage by base stations aimed at reducing the risks of data packet loss and its subsequent adaptation to local conditions.

In addition, the conclusions from the analysis of the possibility of using the TETRA network in train traffic control systems at speeds of up to 500 km/h, as well as conclusions on the level of safety and security of data transmission via these networks were used in practice.

Head : Kynjung Han Vice - President: Gyu-Nam CHOI
Document No : Hyukshin - 190510(2020.06.16)
Address : 19, Seoae-ro 3-gil, Jung-gu, Seoul, South Korea, 04623
Office Tel : 82 - 2-2272 - 6531 / Fax : 82 - 2- 2272 - 3011

203-81-01742

HYUKSHIN ENGINEERING CO.,LTD

CEO Youngshin KIM

19, Seoae-ro 3-gil, Jung-gu, Seoul
04623, Rep. of KOREA

