

B.N. Raximov	t.f.d., professor. O'R MV AKT va AHI boshlig'i. Tahrir kengashi raisi
O.A. Mirjalolov	PhD, dotsent, AKT va AHI boshlig'ining birinchi o'rinbosari. Tahrir kengashi raisi o'rinbosari
A.X. Isxoqov	PhD., dotsent. AKT va AHI kafedra professori. Bosh muharrir
F.B. Baxramov	h.f.n., AKT va AHI KFBO' (oliy ta'limdan keying ta'lim). Bosh muharrir o'rinbosari

Tahrir hay'ati a'zolari:

X.A. Muxitdinov	i.f.n., professor. AKT va AHI ITL yetakchi ilmiy xodimi
A.M. Nazarov	t.f.d., professor. I.A. Karimov nomidagi TDTU professori
B.Z. To'rayev	DSc., professor. AKT va AHI boshlig'i o'rinbosari - Kiberxavfzilik fakulteti boshlig'i
A.A. Suleymanov	t.f.d., professor. I.A. Karimov nomidagi TDTU professori
Sh. S. Fayzibayev	t.f.d., professor. Toshkent transport universiteti kafedra mudiri
D.I. Sultanov	h.f.d., k.i.x. AKT va AHI ITL yetakchi ilmiy xodimi
X.V. Dadabayev	h.f.n., professor. O'R Milliy gvardiyasi bosh boshqarmasi boshlig'i
A.A. Beknazarov	p.f.n., professor. TGFU Aniq va gumanitar fanlar kafedrasini mudiri
U.O. Mamadaliyev	yu.f.n., dotsent. O'R MV HKT boshqarmasi boshlig'i
F.T. Shermatov	PhD., dotsent. AKT va AHI boshlig'ining o'rinbosari
A.Ya. Negrienko	t.f.n., dotsent. O'R QK Harbiy meros va zamonaviy tadqiqotlar instituti katta ilmiy xodimi
J.A. Tajiyev	PhD., dotsent. AKT va AHI ITL boshlig'i
Sh.K. Kurbanov	t.f.n., dotsent. AKT va AHI ITL katta ilmiy xodimi
X.X. Xasanbayev	PhD. O'R MV HKT boshqarmasi bo'lim boshlig'i
Y.Sh. Eshmirzayev	k.f.n. O'R IIV MOMB Maxsus tayyorgarlik o'quv markazi katta instruktori mutaxassisi
B.O. Tursunov	PhD., dotsent. TGFU ilmiy ishlar va innovatsiyalar bo'yicha prorektori
B.K. Yusupov	PhD., professor. AKT va AHI kafedra boshlig'i
Q.M. Tursunov	PhD., dotsent. AKT va AHI kafedra boshlig'i
I.I. Nishanov	PhD., dotsent. AKT va AHI kafedra boshlig'i
Sh.N. Turapov	DSc., dotsent. AKT va AHI kafedra boshlig'i
A.B. Bazarov	PhD. AKT va AHI kafedra boshlig'i
B.S. Nurmetov	PhD. AKT va AHI kafedra boshlig'i
O.R. Dexqonov	PhD., dotsent. AKT va AHI kafedra boshlig'i
D.B. Jaksimov	PhD., dotsent. AKT va AHI kafedra boshlig'i
A.T. Abdujamilov	f-m.f.n., dotsent. AKT va AHI kafedra professori
A.A. Abdigapirov	t.f.n. AKT va AHI kafedra professori
O.Sh. Abdiroziqov	PhD., dotsent. AKT va AHI kafedra katta o'qituvchisi
X.S. Pardayev	PhD, dotsent. AKT va AHI MOF katta o'qituvchisi
B.O. Muxammadov	PhD, dotsent. AKT va AHI kafedra katta o'qituvchisi
O'R. Davlatov	PhD. AKT va AHI boshlig'ining o'rinbosari - shtab boshlig'i

I. QUROLI KUCHLAR TIZIMIDA XAVFSIZLIKNI TA'MINLASH MUAMMOLARI

B.N. RAXIMOV, X.V. TURDIYEV	Xorijiy davlatlarning sun'iy yo'ldoshlar orqali qo'shinlarni boshqarish tajribalari o'rganish.....	5
З.Р. ИМИНОВ	Харбий бўлима жангавор салоҳиятини баҳолашнинг математик моделлаштириши.....	14
O.S. RAYIMJONOVA	Optoelektron o'zgartkich vositasida Mi-171E vertolyotining korpus tebranishlarini kompensatsiyalash orqali ekspluatatsiya muddatini oshirish.....	18
A.X. ИСХОКОВ, А.П. УГАЙ	Необходимость внедрения модулей управления планированием средств авиационного поражения: уроки современных конфликтов.....	23
A.X. FAYZULLAYEV, SH.O. SINDAROV	Zamonaviy radioelektron bosim berish qurilmalari va ularning uchuvchisiz uchish apparatlariga ta'siri.....	30
M.S. TOSHEMIROV	Mina maydonlarini boshqarish usullarini takomillashtirish yo'llari.....	39
З.А. ТАДЖИБАЕВ	Роль ложных узлов связи в современных боевых операциях.....	48

II. HARBIY AXBOROT TIZIMLARIDA INNOVATSION YONDASHUVLAR

B.K. YUSUPOV, B.O. MUHAMADOV	Fayl tizimi boshqaruvini tashkil etish va elektron ma'lumotlar xavfsizligini ta'minlash muammolari.....	57
B.Z. TO'RAYEV, B.N. MIRZODILOV, O.S. MIRZAMURODOV	Shaxsiy ma'lumotlarni himoyalashda matematik modellashni zarurligi (misollar yordamida).....	72
G.U. JURAYEV, Sh.S. ANVAROV	Oqimli shifrlarni kriptotahlilash usullari.....	81
I.I. NISHANOV, D.D. XAYITOV	Kompyuter tarmoqlarida trafik anomalialarini aniqlashning innovatsion yondashuvlari....	86
O.S. RAYIMJONOVA	Turli mashina va mexanizmlarning qiyalanish burchagi hamda tebranishlarini aniqlovchi optoelektron datchik.....	94
B.O. TUYCHIYEV	Troposferada muhitida to'liq tarqalishining modeli va dasturiy apparatini ishlab chiqish.....	102
R.Sh. MELIQO'ZIYEV, H.A. QODIROV	Harbiy tashkilotlardagi inventarizatsiya jarayonlarini raqamlashtirish: ilmiy yondashuvlar va statistik tahlillar.....	110
SH.T. MAHMUDOV	Muhim axborot infratuzilmasida tarmoq monitoringini avtomatlashtirishdagi mavjud muammolar.....	115
Д.Р. АБЗАЛОВ	Метод расчета информационной нагрузки на полевого узлов связи пунктов управления.....	120
A.A. АБИДОВ, O.Ш. АБДИРОЗИКОВ, Б.Н. УМАРАЛИЕВ, Ш.Р. САПАЕВ	Управление современными IT-технологиями с помощью голосовых команд.....	125

III. EKSTRIMAL VA KRIZIS VAZIYATLARDA INNOVATSION YONDASHUVLAR

B.K. YUSUPOV, B.O. MUHAMADOV	MQTT protokoli asosida IoT qurilmasida Mosquito, HiveMQ, Adafruit IO brokerlarining samaradorligini taqqoslash.....	132
I.I. NISHANOV, SH.T. MAHMUDOV	Tarmoq monitoringi avtomatizatsiyasi uchun zarur texnik yechimlar va iqtisodiy xarajatlar tahlili.....	137
Sh.O. SINDAROV, A.X. FAYZULLAYEV	Harakatlanuvchi dron tizimlarida boshqaruv signallarini uzatishning mavjud yechimlari.....	144

J.M. Mamajonov	PhD. AKT va AHI kafedra katta o'qituvchisi
P.Q. Xolmatov	p.f.n., dotsent. TGFU Aniq va gumanitar fanlar kafedrasini mudiri
S.O. Maxmudov	PhD., dotsent. AKT va AHI kafedra professori
A.A. Komilov	PhD. AKT va AHI kafedra katta o'qituvchisi
S.Ch. Muratova	PhD., dotsent. TAFU Kafedra mudiri
M.B. Aripxodjayeva	PhD., dotsent. I.A. Karimov nomidagi TDTU kafedra dotsenti

Ma'sul kotiblar:

A.A. Axunov	AKT va AHI sikl boshlig'i
N.T. Boboyev	PhD. AKT va AHI kafedra katta o'qituvchisi
Z.S. Ollaberganova	AKT va AHI MOF katta o'qituvchisi

Tahrirchilar:

Z.D. Tashtayev	dotsent. AKT va AHI uslubiy bo'lim boshlig'i
H.A. Qodirov	dotsent. AKT va AHI kafedra professori
A.Ya. Vagner	AKT va AHI kafedra dotsenti
A.N. Shafeyev	PhD. AKT va AHI kafedra katta o'qituvchisi
N.M. Xolmatov	dotsent. AKT va AHI kafedra o'qituvchisi
D.U. Allayarov	dotsent. AKT va AHI kafedra o'qituvchisi
R.I. Muxamedjanov	dotsent. AKT va AHI kafedra o'qituvchisi

Muassis:

O'zbekiston Respublikasi Mudofaa Vazirligi
Axborot-kommunikatsiya texnologiyalari
va aloqa harbiy instituti

Manzil: 100084, O'zbekiston, Toshkent viloyati,
Zangiota tumani, Quyoshli 176 h/sh.

Telefon: (95)170-17-21;

e-mail: harbiyinstitut@inbox.uz

Jurnal sayti: mvahi.uz

Ushbu ilmiy-texnik jurnal
O'zbekiston Respublikasi Oliy atestatsiya komissiyasi
Rayosatining 31.01.2023-yildagi №332/5 sonli
Qarori bilan chop etishga tavsiya etilgan
ilmiy ishlar ro'yxatiga kiritilgan

Bosishga ruxsat etildi:

Qog'oz bichimi: 60x84 1/8

Bosma tabog'i 15,5. Adadu 2 nusxa

Buyurtma raqami №82

"Harbiy institut bosmaxonasi" da chop etildi
Jurnal yilda 4 marotaba (har chorakda) chop etiladi.

ISSN 2181-2152

Jurnal O'zbekiston Respublikasi Prezidenti
Administratsiyasi huzuridagi Axborot va ommaviy
kommunikatsiyalar agentligida 2021-yil 22-aprelda
1166 raqami bilan ro'yxatga olingan.

© «AKT va AHI» 2025

M.Sh. RAYIMOV O'zbekiston Respublikasida ijtimoiy tarmoqlar orqali yuzaga kelayotgan kiberxavfsizlik tahdidlari va ularni boshqarishning intellektual yondashuvi.....	152
C.Э. ХОЛИКОВ Мухим ахборот инфратузилмасини химоя қилишда инновацион периметр хавфсизлик тизимлари.....	158
Б.С.НУРМЕТОВ, З.Ё. АХМЕДОВ Теоретические и практические аспекты использования когерентных сигналов в радиолокации.....	164
А.Я. НЕГРИЕНКО, Р.Ж. РАХМАТБАЕВ К вопросу экспериментальной оценки реальной помехоустойчивости линейных трактов цифровых систем передачи методами натурных испытаний.....	168
Н.А. КАЮМОВ Опыт применения ГИС в военном деле.....	172

IV. HARBIY TA'LIMDA ZAMONAVIY PEDTEKNOLOGIYALAR VA O'QITISHDA INNOVATSION YECHIMLAR

D.A. ABDURAXIMOVA, A.A. UBAYDULLAYEVA Harbiylarga xorijiy tillarni o'qitish jarayonida kommunikativ ko'nikmalarini rivojlantirishning ahamiyati (ingliz tili misolida).....	178
A.Sh. XUDAYAROV, X.U. YAKUBOV Harbiy pedagogik mahorat asoslari.....	184
З.Р. ИМИНОВ Ҳарбий бўлима шахсий таркибининг жангвор қобилиятини аниқлашда белгилар мажмуасини шакллантириш ва уларнинг таҳлили.....	189
U.A. ALIBAYEVA Chet tillarni o'qitish metodikasini takomillashtirish: nazariy asoslar va innovatsion yondashuvlar...	194
A.Sh. XUDAYAROV, X.U. YAKUBOV Harbiy xizmatchilarni ta'lim-tarbiya jarayonida mustaqil fikrlash va ilmiy dunyoqarashni shakllantirish.....	199
U.A. ALIBAYEVA Chet tili o'qituvchilarining metodik tayyorgarligini tashkil etishning zamonaviy tendentsiyalari.....	205

V. ILMIY AXBOROTLAR

G.U. JURAYEV, Sh.S. ANVAROV Zamonaviy oqimli shifrlash algoritmlarining taqqoslama tahlili.....	210
A.I. XURRAMOV Ekssentrik rotatsion ishqalagich yordamida ichki yonuv dvigatellari detallariga ishlov berishning kompyuter dasturi va hisobi.....	223
X.U. YAKUBOV Ukraina qurolli kuchlarida zamonaviy radioelektron kurash vositalari.....	229
I.I. SOTVOLDIYEV Amir Temur armiyasini jangovar tuzilishi.....	238
A.A. ABIDOV, B.N. UMARALIYEV, Sh.R. SAPAYEV Bugungi transformatsion harbiy to'qnashuvlarda mikrokontrollerlarning qo'llanilishi.....	247
O.O. ТАЛІПОВ Банк ва тўлов тизимларида банк карталари билан боғлиқ фирибгарлик ҳолатларини олдини олишда антифрод тизимларини қўлланилиши.....	252
D.N. XOLMURODOV Sun'iy intellekt texnologiyalarining ijtimoiy sohalarni rivojlantirishda tutgan o'rni.....	257
A.A. KARIMOV Bulutli tizimlarda multi-tenant va cross-domain sharing xavfsizlik tahlili.....	263
G.N. MEMONOVA Development of a multi-parameter groundwater monitoring device using level, temperature, and pH sensors.....	269
K.M. ТУРСУНОВ, Д.Р. ИСЛОМОВ Возрождение, становление и перспектива развития системы РЭБ.....	276
U.O. MAMADALIYEV Kiberxavfsizlikning zamonaviy klassifikatsiyasi: milliy va xalqaro modellar.....	282
S.S. USMONOV Kiberzo'ravonlikning tarixiy ildizlari va global tendentsiyalari.....	285

XORIJIY DAVLATLARNING SUN'IY YO'LDOSHLAR ORQALI QO'SHINLARNI BOSHQARISH TAJRIBALARI O'RGANISH

t.f.d. profesor B.N. RAXIMOV

O'R MV Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti

X.V. TURDIYEV

O'R QK Akademiyasi

Annotatsiya. Ushbu maqolada, yetakchi xorijiy davlatlar qurolli kuchlari tarkibidagi qo'shinlarni sun'iy yo'ldosh aloqa tizimi orqali boshqaruvini tashkil etish bo'yicha ilg'or tajribalari, ushbu boshqaruv tizimini jangovar harakatlarda tutgan o'rni va roli, uni tashkil etishda talab etiladigan vositalar ko'lamini, shuningdek, asosiy yutuq va kamchiliklari batafsil bayon etilgan. Shu bilan birga, sun'iy yo'ldosh aloqa tizimi orqali qo'shinlarni boshqarishda yetakchi xorijiy davlatlar tomonidan ahamiyat berilayotgan asosiy jihatlar detallashtirilgan holda yoritilib berilgan.

Kalit so'zlar: Sun'iy yo'ldoshli aloqa, retranslyatsiya, aloqa tizimi, jangni boshqarish, boshqaruvni niqoblash, Futur Force, konsepsiya, V-SAT (Very Small Aperture Terminal), Intelsat va Inmarsat xalqaro kompaniyalari, aloqa xavfsizligi

Аннотация. В статье подробно излагается передовой опыт ведущих зарубежных стран по организации управления войсками в вооруженных силах посредством спутниковых систем связи, место и роль этой системы управления в боевых действиях, объем ресурсов, необходимых для её организации, а также её основные достижения и недостатки. При этом подробно излагаются основные аспекты, на которые обращают внимание ведущие зарубежные страны при управлении войсками посредством спутниковых систем связи.

Ключевые слова: спутниковая связь, ретрансляция, система связи, управления боем, маскировка управления, Футур Форс, концепции, В-САТ (станция с очень малой аппаратурой), международные компании Интелсат и Инмарсат, безопасность связи.

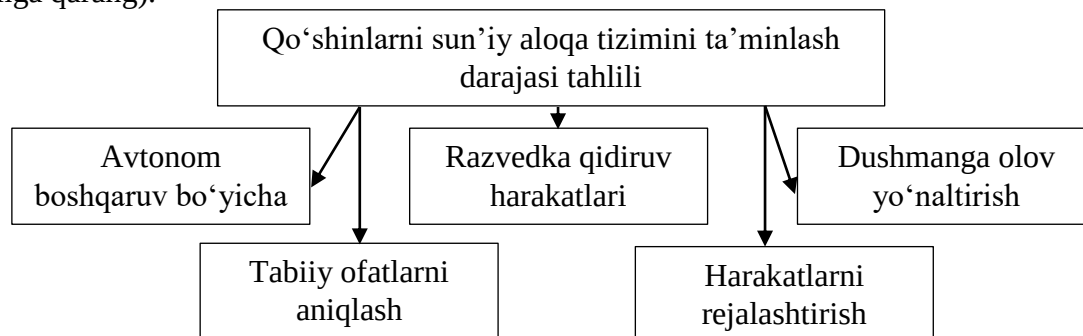
Abstract. This article describes in detail the advanced experiences of leading foreign countries in organizing the control of troops in the armed forces through satellite communication system, the place and role of this control system in combat operations, the scope of resources required for its organization, as well as its main achievements and shortcomings. At the same time, the main aspects that are being paid attention to by leading foreign countries in controlling troops through satellite communication systems are described in detail.

Ключевые слова: satellite, retransmission, communication system, battle management, control masking, Futur Force, concept, V-SAT (Very Small Aperture Terminal), International companies Intelsat and Inmarsat, communication security.

Bugungi kunda qo'shinlarni sun'iy yo'ldosh aloqa tizimi orqali boshqarish orqali jangovar vazifani muvaffaqiyatli bajarish imkoniyati oshib borayotgan bir vaqtda yetakchi xorijiy davlatlarda ham ushbu tizimni mustahkam tashkil etish, rivojlantirish va takomillashtirish bo'yicha keng ko'lamli ishlar amalga oshirilmoqda. Ayniqsa, sun'iy yo'ldosh aloqa tizimini tashkillashtiruvchi bo'linmalarni isloh qilish, ularni zamonaviy qurol, jangovar va maxsus texnikalar bilan ta'minlash, yetakchi davlatlar bilan uzviy hamkorlikni yo'lga qo'yish, operativ va taktik bo'g'indagi bo'linmalar o'rtasida ma'lumotlar almashinuvi samaradorligini oshirish hamda sun'iy yo'ldosh aloqasini qo'shinlarda tashkil etishning zamonaviy modellarini ishlab chiqishga qaratilgan bir qancha salmoqli ishlar amalga oshirilmoqda. Xususan ushbu paragrafda, operativ (taktik) bo'g'inda sun'iy yo'ldosh aloqa tizimini tashkillashtirish bo'yicha yetakchi xorijiy davlatlar AQSH, Rossiya, Xitoy va Markaziy Osiyodan Qozog'iston armiyalarining ilg'or tajribalari o'rganilgan.

Amerika Qo'shma Shtatlari (AQSH). AQSH harbiy siyosiy rahbariyatini so'nggi yillarda olib borgan siyosatidan kelib chiqib shuni aytish mumkinki operativ bo'g'indagi qo'shinlarni sun'iy

yo'ldosh orqali boshqarish bo'yicha dunyoda bugungi kunda yetakchi o'rinlarni egallaydi (1-rasmga qarang).



1-rasm. AQSH qo'shnlarni dunyoda sun'iy yo'ldosh vositalari orqali jangovar harakatlarni rejalashtirish bo'yicha yetakchilik yo'nalishlari chizmasi

Hozirgi vaqtda AQSH armiyasi operativ va strategik bo'g'inda sun'iy yo'ldosh orqali boshqaruvini yanada takomillashtirish maqsadida Futur Fors (Kelajak armiyasi) konsepsiyasi ishlab chiqilgan bo'lib ushbu konsepsiyaga asosan quyidagi tadbirlarni 2030-yilgacha amalga oshirish belgilangan:

sun'iy yo'ldosh aloqa tizimi orqali qo'shnlarni boshqaruv qamrovini 2027-yilgacha 100%ga yetkazish;

qisqa vaqt ichida har qanday hududda aloqani ta'minlashda sfera kengligini dunyo bo'ylab amalga oshirish (Afrika va Osiyo kontingentida bugungi kunda sun'iy yo'ldosh orqali boshqaruv 54% ni tashkil etadi);

strategik va operativ bo'g'indagi har qanday ma'lumotlar almashinuvi xavfsizligini to'liq ta'minlash;

nafaqat boshqaruv balkim boshqa yo'nalishlarda ham sun'iy yo'ldosh aloqa tizimini qo'llash samaradorligini takomillashtirish;

robotlashgan va smart armiyalar tuzish orqali ularni yagona avtonom boshqaruvini yaratish;

o'zgaruvchan jangovar harakatlar teatri natijalaridan kelib chiqib mavjud operativ bo'g'inda sun'iy yo'ldosh aloqasi tashkil etish modellarini qadamma-qadam takomillashtirib borish;

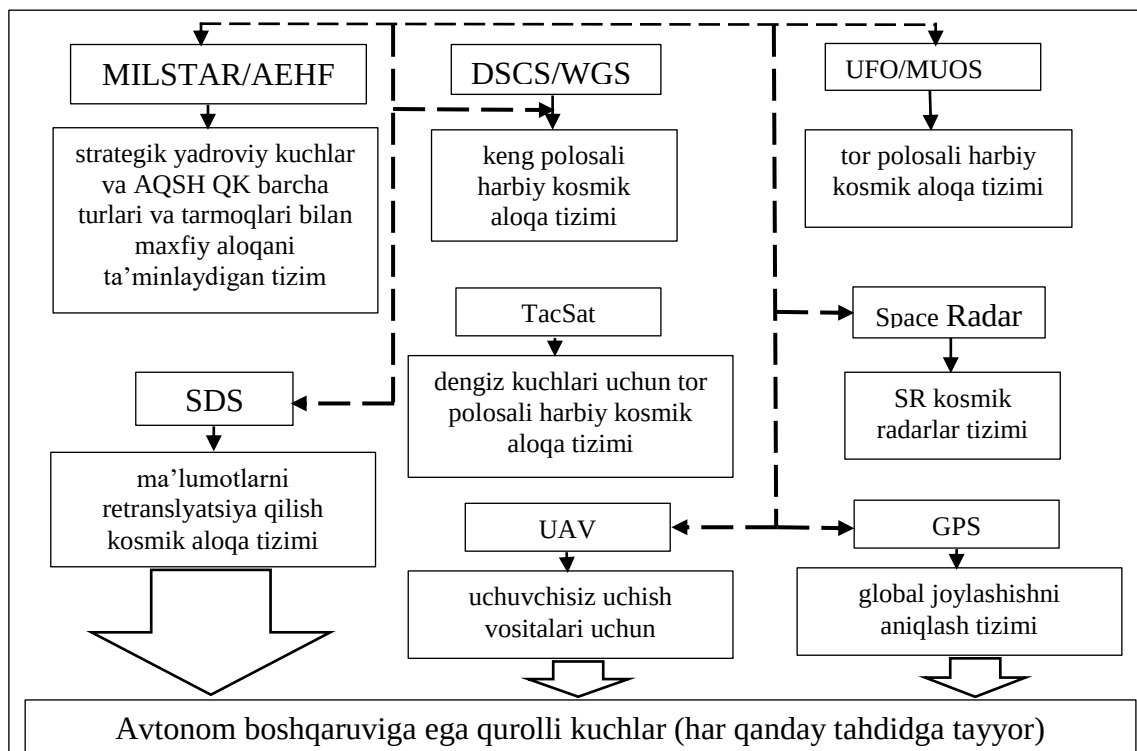
operativ bo'g'inda sun'iy yo'ldosh aloqasini tashkil etish bo'yicha mavjud shtat tuzilmalariga ega bo'linmalarni zamonaviy vositalar bilan uzluksiz ta'minlab borish;

dunyo hamjamiyatida sun'iy yo'ldosh orqali boshqariladigan qo'shnlarga qarshi kurashish yagona tizimini ishlab chiqish [1].

Bugungi kunda AQSH ilmiy tadqiqot markazlari va institutlarini xulosalariga ko'ra o'tmishdan olingan saboqlardan kelib chiqib zamonaviy sun'iy yo'ldosh aloqasini tashkil etish asosiy vazifa ekanligini ta'kidlamog'dalar. Misol tariqasida, 1991 yildagi Fors ko'rfazidagi harbiy mojaro "Cho'l bo'roni" operatsiyasi davomida AQSH qurolli kuchlari uchun "kosmik asr" ning boshlanishi bo'lgan bo'lsada yutuqlar qatorida bir necha jiddiy kamchiliklarga yo'l qo'yanlar. Natijada, o'tkaziladigan operatsiyalarni noto'g'ri rejalashtirish, bo'linmalar o'rtasida boshqaruvni yo'qotilishi kabi bir necha faktorlar yuzaga qalqib chiqish fonida sun'iy yo'ldosh aloqa tizimni zamonaviy ko'rinishlarini yaratishni o'z oldilariga maqsad qilib qo'yishgan edi (1991-1999 yy Yugoslaviya, Afg'oniston, Suriya, Shimoliy Afrika). Bu boradi bugungi kunda katta masshtabdagi ishlar olib borilib o'z samarasini ko'rsatib kelmoqda.

Yuqoridagilarni inobatga olib hozirgi vaqtda AQSH mudofaa vazirligida aloqa tizimi katta miqyosda modernizatsiya ishlari davom etmoqda. Ayniqsa, harbiy amaliyotlar o'z davlatidan boshqa hududlarda olib borilishini inobatga olgan holda harbiy va tijorat sun'iy yo'ldosh aloqa tizimidan foydalanib operativ va strategik vazifalarni bajarish nazarda tutmoqda.

Bugungi kunda, AQSH qurolli kuchlarning axborot infratuzilmasining asosini harbiy sun'iy yo'ldosh aloqa tizimlari tashkil qilib quyidagi tizimlarni o'z ichiga oladi (2-rasmga qarang) [2]:



2-rasm. AQSh harbiy sun'iy aloqa tizimining quyi tizimlari chizmasi

Yuqoridagilardan xulosa qilib aytish mumkinki, AQSH harbiy sun'iy yo'ldosh aloqa tizimlariga e'tibor yildan yilga kuchaytirib bormoqda. Misol uchun 2024-yil uchun hukumat tomonidan harbiy sun'iy yo'ldosh aloqa tizimlariga 12.8 mlrd dollar ajratilgan bo'lsa, 2025-yil uchun 24.4 mlrd dollar mablag' ajratilgan. Harbiy budjetlarning o'sishi va davom etayotgan global inqiroz sharoitida Amerika Qo'shma Shtatlari va NATO mamlakatlari hukumati va harbiy tuzilmalari tijorat kosmik kemalarining resurslaridan tobora ko'proq foydalanmoqdalar, ular maxsus sun'iy yo'ldosh aloqa tizimlaridan ancha arzon.

Harbiy ekspertlarni fikriga ko'ra, AQSH QK 2024-yil oxirigacha 122 ta harbiy sun'iy yo'ldoshlar orbitaga olib chiqqan bo'lsa, 2025-yilda ular 200 yaqin harbiy sun'iy yo'ldoshni orbitaga olib chiqishni rejalashtirmoqdalar. Bu loyihalarni amalga oshirishda asosan Northrummanation va SpaceX kompaniyalari bilan hamkorlik amalga oshirilmoqda [3].

Umumiy xulosa qilganda, AQSH QK so'nggi yillarda qo'shinlarni boshqaruvida sun'iy yo'ldosh aloqa tizimiga bo'lgan talabni kun sayin oshirib bormoqda. Rossiya-Ukraina o'rtasidagi urush tahlillaridan keng masshtabdagi xulosalar qilgan harbiy siyosiy rahbariyat tushundiki sun'iy yo'ldosh aloqa tizimi orqali qo'shinlarni boshqaruvi jangovar harakatlarda kam yo'qotishlar bilan muvaffaqiyatga erishishning asosiy vositasi bo'lib ulgurgan.

Bundan tashqari hozirgi vaqtda AQSH QK harbiy sun'iy yo'ldosh tizimi yer sharida navigatsiya orqali nishonni aniqlash, ballistik raketa uchirish, ob-havo ma'lumotlari, maxfiylashtirilgan ma'lumot almashish, uchuvchisiz samolyotlarni boshqarish, dengiz floti, aviatsiya, radioelektron kurash, maxsus jangovar vazifalarni bajarish, murakkab vaziyatda bo'linmalarni boshqarish, hamkorlikdagi qo'shni armiyalari bilan maxsus aloqani ta'minlash vazifalarini ham og'ishmay bajarib kelmoqda.

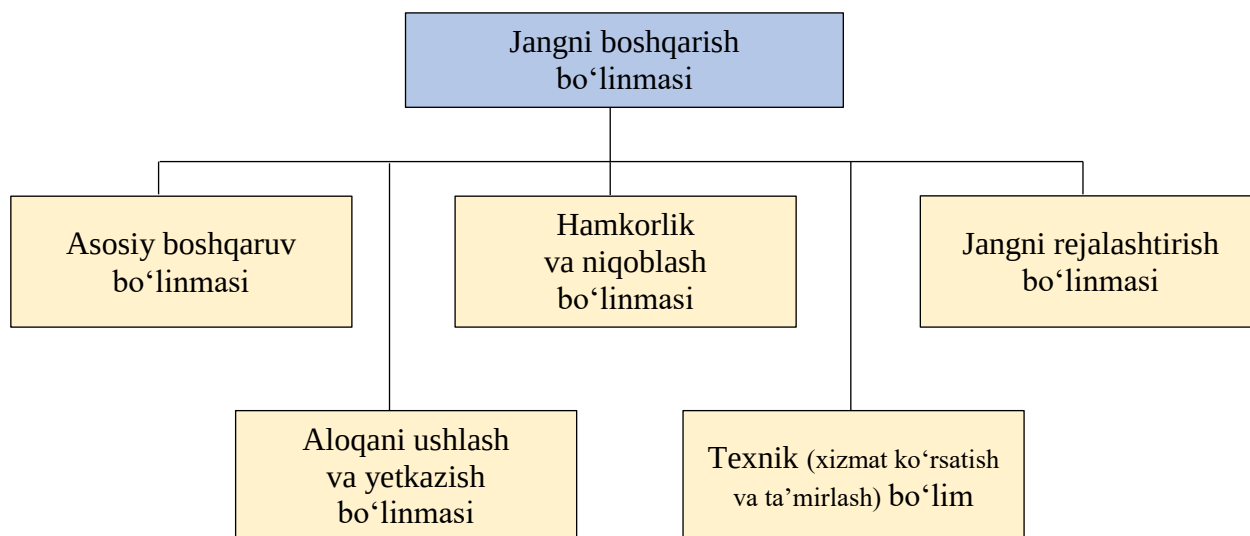
Bugungi kunda **Rossiya Federatsiyasi** qurolli kuchlari (RF QK) larida aloqa tizimini rivojlantirish orqali qurollar va qo'shinlarni boshqarish tizimiga sun'iy yo'ldosh aloqa tizimiga raqamli texnikalarni tatbiq etish va ularni takomillashtirish bo'yicha keng ko'lamli ishlar amalga oshilib kelmoqda. Barchaga ma'lumki bugungi kunda davom etayotgan Ukraina davlati bilan bo'layotgan qurolli mojaro RF QKlarini har jabhada takomillashtirishga imkon yaratdi. Ushbu urushning dastlabki bosqichida Ukraina davlati qurolli kuchlariga qarshi Rossiya QKlari sun'iy

yo'ldosh aloqa vositalari orqali qo'shinlarni boshqaruvini, jumladan, bo'linmalar o'rtasidagi uzviy aloqani ta'minlash, artilleriya va aviatsiya olovlarini dushmanga yo'naltirish, jangovar harakatlar va taktik harakat usullarini rejalashtirish, jangovar razvedka qidiruv harakatlarini olib borish, har qanday hududda bo'linmalar o'rtasida hamkorlikni tashkillashtirish vazifalari bajarildi.

Urushning dastlabki bosqichida ushbu yuqorida ko'rsatilgan tadbirlar Rossiya QKlari tomonidan muvaffaqiyatli amalga oshirildi. Biroq, urushning oltinchi oyiga kelib Ukraina QKlari tarkibiga AQSH QKlariga tegishli bugungi kunda har qanday zamonaviy talablarga javob beradigan sun'iy yo'ldosh boshqaruv tizmi biriktirildi. Natijada, Rossiya QK tomonidan har qanday rejalashtiriladigan jangovar harakatlarga javob harakatlari amalga oshirila boshlandi. Jumladan, Rossiya QK tomonidan rejalashtirilgan taktik harakat usullariga (Xarkov) qarshi Ukraina armiyasi tomonidan javob taktik harakat usuli qo'llanildi, Rus qo'shinlarini marsh olib borish yo'nalishlariga pistirmalar qo'yildi. Natijada, Rus qo'shinlari tomonidan shaxsiy tarkib va texnikalarning yo'qotish ko'lamli keskin ortib ketdi. Bundan xulosa qilgan RF harbiy siyosiy rahbariyati zudlik bilan sun'iy yo'ldosh boshqaruv tizimlarini yangicha modellarini yaratish, zamonaviy vositalar bilan ta'minlash, har bir operativ va taktik bo'g'indagi bo'linmalar tarkibiga sun'iy yo'ldosh bilan ishlovchi kichik maxsus bo'linmalarni kiritish, barcha shaxsiy tarkibni maxsus tayyorgarligini oshirishga intildilar. Bu jabhada Rossiya Federatsiyasi yetakchi ilmiy tadqiqot markazlari bugungi kunda ham keng ko'lamli ishlarni amalga oshirib kelmoqda.

Yetakchi xorijiy davlatlar ekspertlarini fikriga ko'ra bugungi kunda RF Qurolli Kuchlari tarkibidagi operativ va taktik bo'g'indagi bo'linmalar tarkibiga sun'iy yo'ldosh bilan ishlash bo'yicha o'z ishini ustalaridan iborat bo'lgan maxsus harbiy xizmatchilar kiritilgan bo'lib nafaqat bo'linmalarni boshqarish shu bilan birga boshqa jangovar harakatlarni rejalashtirish hamda qarama-qarshi tomon harakatlariga va signallariga javob berish imkoniyatiga egalar.

Bugungi kunda RF qurolli kuchlari tarkibidagi operativ va taktik bo'g'indagi bo'linmalar tarkibida quyidagi tarkibdagi sun'iy yo'ldosh aloqasi boshqaruvini ta'minlovchi bo'linmalar mavjud (3-rasmga qarang) [4].



3-rasm. RF QK operativ bo'g'indagi sun'iy yo'ldosh boshqaruvini tashkillashtirish bo'linmasini TSHT chizmasi

Ushbu jangni boshqarish bo'linmasi quyidagi vazifalarni bajarish uchun mo'ljallangan:

- qisqa vaqt ichida har qanday sharoitda bo'linmalar o'rtasidagi standart aloqani tashkil etish;
- yuqori shtab va bo'linmalar o'rtasida ma'lumot almashinuvini o'z vaqtida ta'minlash;
- hamkorlikdagi va qo'llab-quvvatlovchi bo'linmalar o'rtasida ma'lumot almashinuvini ta'minlash;
- jangovar harakatlarni rejalashtirish, bo'linmalarni oldindagi jangovar harakatlarga

yo'naltirish;

- avtonom boshqaruv tizimini ta'minlash;
- aloqa xavfsizligini ta'minlash;
- boshqaruv vositalariga texnik xizmat ko'rsatish.

Ayni paytda Rossiya Federatsiyasi Mudofaa vazirligi kosmik orbital guruhi takomillashtirish va yangilanish jarayonini boshdan kechirmoqda.

Ushbu sohani yanada rivojlantirish va harbiy sun'iy yo'ldoshlarni takomillashtirishga katta e'tibor qaratmoqda. Rossiya kosmik tizimining 60% ni Qurolli Kuchlarning sun'iy yo'ldoshlari tashkil qiladi va quyidagilarni o'z ichiga oladi.

Xulosa qilib aytganda bugungi kunda har jabxada RF QK tarkibidagi birlashma, qo'shilma, qism va bo'linmalarni sun'iy yo'ldosh aloqa tizimi orqali boshqaruvini tashkil etish orqali qurolli mojaralarda muvaffaqiyatga erishmoqdalar. Shuningdek, sun'iy yo'ldosh aloqa tizimi orqali qo'shinlarni boshqarishda, boshqaruvni turg'un va faolligi, yashirinligi, o'z vaqtidaligi ta'minlanmoqda.

Bugungi kunda RF ilmiy tadqiqot institutlari qurolli kuchlarni sun'iy yo'ldosh aloqasini zamaonaviy ko'rinishlarini yaratish, yangicha usul va algoritmlarni ishlab chiqishga asosiy etiborlarini qaratib bu burada katta masshtabdagi ishlarni amalga oshirib kelmoqdalar.

Hozirgi vaqtda sun'iy yo'ldosh aloqalari Rossiya Federatsiyasi qurolli kuchlarining qo'mondonlik va boshqaruv tizimida ham keng qo'llanilmoqda. Qurolli kurash shakllari va usullarini takomillashtirish, eng yangi qurol va harbiy texnika, sun'iy yo'ldosh aloqalarini qo'llash sharoitida qo'shinlar va qurollarni boshqarish va boshqaruvni barqarorligini ta'minlashning muhim yo'nalishlaridan biri sifatida zarur bo'lgan ma'lumotlar hajmini minimal xarajatlar bilan o'z vaqtida yetkazish hisoblanadi.

Xitoy Halq ozodlik armiyasi (XXOA) tarkibida sun'iy yo'ldosh aloqa tizimini eng rivojlangan bosqichi 21-asrning boshiga kelib taqaladi. Bungacha 1982-yildan 2000-yilgacha bo'lgan davr oralig'ida XXOA siyosiy rahbariyati barcha qism va bo'linmalarni boshqaruvini portativ aloqa vositalari orqali olib borishgan bo'lsa, 2000-yilga kelib so'nggi yillardagi urushlar va qurolli mojarolar tajribalariga tayangan holda milliy sun'iy yo'ldosh aloqa tizimini harbiylashtirish harakatini rivojlanishiga o'tdilar.

Shu yilga kelib davlat va harbiy boshqaruv organlari, harbiy tuzilmalar va boshqa davlat tuzilmalarini sun'iy yo'ldosh aloqalari bilan ta'minlash uchun harbiy strategik va taktik sun'iy yo'ldosh aloqa tizimlari, shuningdek, milliy, mintaqaviy va global tijorat sun'iy yo'ldosh aloqa tizimlari (CCS) keng qo'llanila boshladi. 2001-yilda XXOA tarkibidagi qo'shinlarni sun'iy yo'ldosh aloqa tizimini zamonaviy ko'rinishlarini yaratish bo'yicha "Boshqaruv istiqboli" (UUV) konseptiyasi qabul qilingan bo'lib ushbu me'yoriy rahbariy hujjat quyidagi besh yo'nalishdagi asosiy tadbirlarni o'z ichiga olgan:

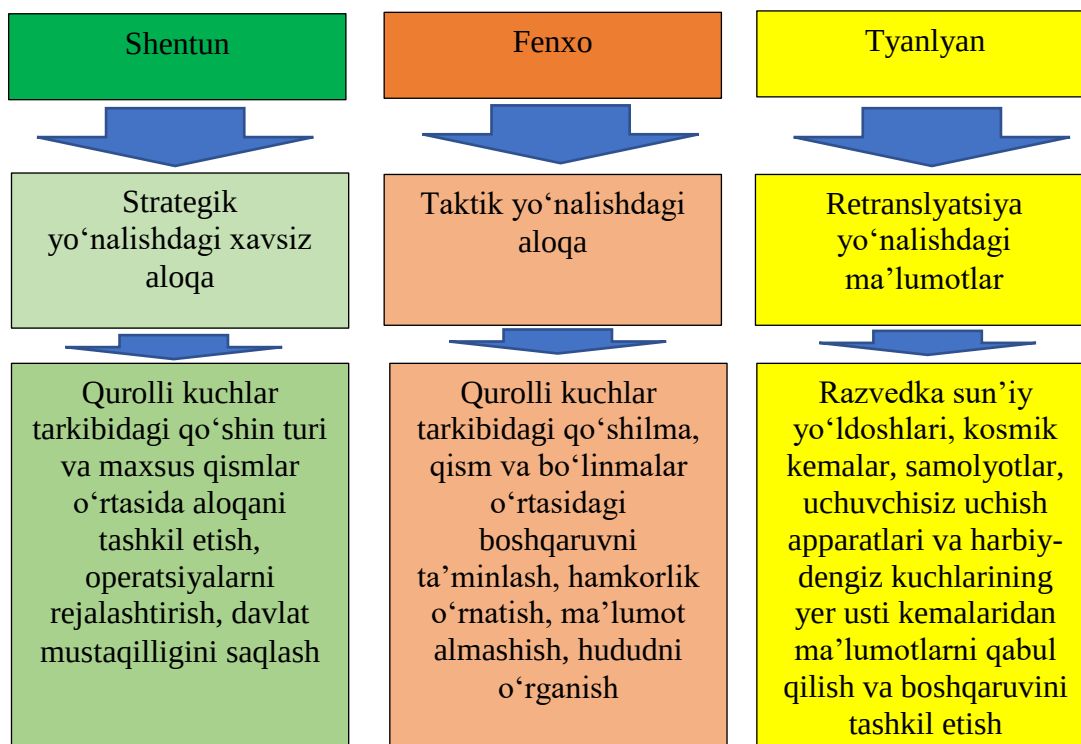
- qurolli kuchlar boshqaruvini sun'iy yo'ldosh aloqasi bilan qamrab olish;
- ma'lumotlar uzatish va qabul qilish tizimini xavfsizligini va mobilligini ta'minlash;
- jangovar harakatlarni rejalashtirish tadbirlarini avtomatlashtirish;
- qrama-qarshi tomonlarni ehtimoliy harakatlarini baholash, ularga qarshi javob tadbirlarini rejalashtirish;

barcha yo'nalishdagi qo'shin va bo'linmalar va mahaliy xokimyat idoralari bilan mustahkam hamkorlikni tashkillashtirish [5].

XXOA siyosiy rahbariyatining rejasiga ko'ra, sun'iy yo'ldosh komponenti nazorat, aloqa, razvedka ma'lumotlarini yig'ish va tarqatishning yaxlit tizimini yaratishda asosiy bo'g'in bo'lib, harbiy aloqa infratuzilmasini to'ldiradi va birlashtiradi. Bunday tizimlarni takomillashtirish Pekin tomonidan o'rta muddatli istiqbolda o'z qurolli kuchlarini modernizatsiya qilishning asosiy vazifalaridan biri sifatida qaralmoqda.

Xitoy mutaxassislari tomonidan bugungi kunda sun'iy yo'ldosh aloqa kanallari orqali aloqa tizimini tashkil qilish barcha bo'g'indagi bo'linmalar bilan amalga oshirilmoqda.

Yetakchi xorijiy davlatlar harbiy ekspertlari va nufuzli tadqiqot institutlarini ma'lumotlariga ko'ra bugungi kunda XXOA harbiy sun'iy yo'ldosh aloqa tizimini rivojlantirish dasturini asosan uchta yo'nalishda olib bormoqda (4-rasmga qarang).



4-rasm. XXR Qurolli Kuchlarning sun'iy yo'ldosh aloqa tizimi turlari chizmasi

Hozirgi vaqtda ushbu tizimlarning kosmik elementida Shentun-1 va Shentun-2 tipidagi beshta geostatsionar aloqa sun'iy yo'ldoshlari (mos ravishda bitta va ikkita), Fenxo -1 va Fenxo -2 (har birida bittadan) va Tyanlyan-1 tipidagi uchta retranslyatsiya ma'lumot sun'iy yo'ldoshlaridan foydalaniladi.

Ushbu sun'iy yo'ldosh aloqa tizimini xavsizligini ta'minlash, ma'lumotlar uzatish va qabul qilish oqimlarini maxfiylashtirish maqsadida bugungi kunda XXOA milliy ishlab chiqarilgan shifrlash uskunalaridan foydalanishga asosiy e'tiborlarini qaratmoqdalar. Bu esa boshqaruv va ma'lumot uzatish tizimini ta'minlash va kafolatlashga imkonini berganligi sababli ko'plab yetakchi xorijiy davlatlar XXOA sun'iy yo'ldosh aloqa tizimi bilan hamkorlik qilish (sotib olish, hamkorlikda ishlash)ga intilmoqdalar (Pokiston, Indoneziya, Turkiya, Markaziy osiyoning boshqa davlatlari, Shimoliy Afrika).

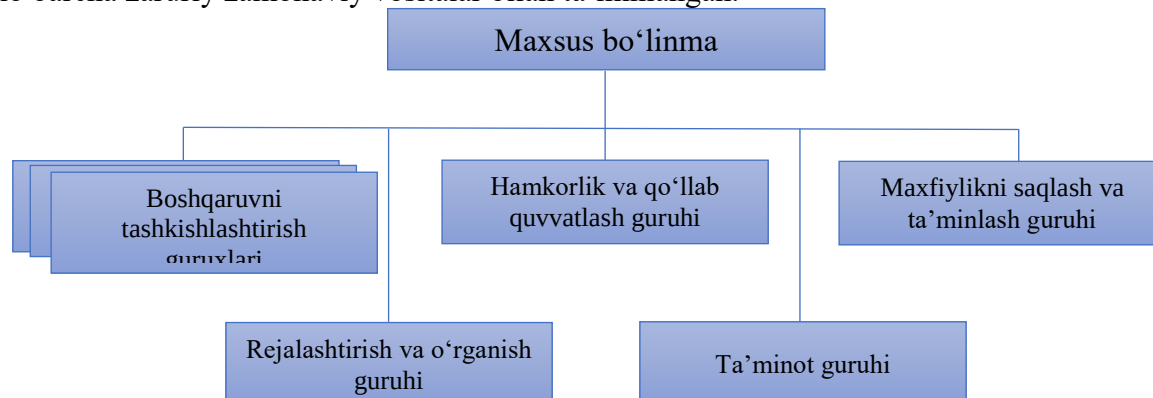
Bu borada ikki bosqichli istiqbolli loyixalar tayyorlanib hayotga tatbiq etib kelinmoqda. Jumladan,

Birinchi bosqichda (2018-yilgacha) kosmik va yer segmentlarini joylashtirish va loyihada ishtirok etuvchi mamlakatlarga aloqa xizmatlarini ko'rsatishni boshlash rejalashtirilgan;

ikkinchi bosqichda (2019-yildan) tizimning 3G, 4G va istiqbolli 5G aloqa standartlariga mos keladigan mobil aloqa xizmatlari va keng polosali ma'lumotlar uzatish, shu jumladan samolyot va poezdlarda, 2021-yildan esa ularni global miqyosda taqdim etish imkoniyatlarini kengaytirish rejalashtirilgan. Tizimning kosmik segmenti 49 ta kichik sun'iy yo'ldoshdan iborat bo'ladi.

2018-yilga kelib XXOA tarkibidagi qo'shinlarni mustahkam boshqaruvini ta'minlash, ma'lumotlar almashinuvini mobillashtirish, jangovar harakatlarni mustaqil rejalashtirish va olib borish maqsadida taktik va operativ bo'g'indagi bo'linmalar tarkiblariga sun'iy yo'ldosh aloqasini ta'minlash imkonini beruvchi kichik maxsus bo'linmalar kiritildi (5-rasmga qarang). Ushbu

bo'linmalar taktik bo'g'indagi qo'shnlarni mustaqil harakatlanish imkonini oshirish va yuqori shtab bilan hamkorlikni ushlab turish vazifalarini to'laonli bajarish imkoniyatiga ega bo'lib barcha zaruriy zamonaviy vositalar bilan ta'minlangan.



5-rasm. XXOA tarkibidagi taktik bo'g'indagi maxsus guruh TShT chizmasi

Ushbu bo'linma quyidagi ko'lamdagi vazifalarni bajarish uchun mo'ljallangan:

qisqa vaqtda har qanday hududlarda bo'linmalar o'rtasidagi aloqani tashkil etish va saqlash;
yuqori shtab bilan ma'lumotlar almashinuvini alternativ xaxiralash;
jangovar harakatlarda jang olib borayotgan bo'linmalar (harbiy xizmatchi) bilan barcha turdagi ma'lumotlar almashinuvini ta'minlash;

qarama-qarshi tomonlarni harakatlarini kuzatish va ularga munosib zarbalar berishni rejalashtirish;

hududni o'rganish va tegishli hisob-kitoblarni aniqlash;

avtomatlashgan boshqaruv tizimini tashkillashtirish va ushlab turish;

boshqaruvni turg'un va faolligini va yashirinligini ta'minlash;

jangovar harakatlarda bo'linmalarni bo'lg'usi harakatlarini rejalashtirish.

Bugungi kunda, sun'iy yo'ldosh aloqasi imkoniyatlarini kengaytirish uchun Xitoy hukumati tashkilotlari Intelsat va Inmarsat xalqaro operatsion kompaniyalaridan sun'iy yo'ldosh resurslarini ham ijaraga oladi.

2013-yildan boshlab esa davlat va harbiy boshqaruv tarmoqlarini tashkil qilish uchun SSS ning yer osti elementida diametri 0,15-2,5 m bo'lgan antennalarga ega V-SAT (Very Small Aperture Terminal) tipidagi kichik sun'iy yo'ldosh terminallari qo'llanilib kelinmoqda.

Ular Internetda ishlash, videokonferensiya, ma'lumotlarni uzatish, video tasvirlar va IP telefoniya kabi keng ko'lamli aloqa xizmatlarini taqdim etadilar. V-SAT terminallari okrug, armiya, diviziya (brigada) va polk qo'mondonligi darajalarida o'rnatiladi. Bundan tashqari, Shentong-1 va Fenghuo-1 kabi birinchi avlod harbiy sun'iy yo'ldoshlari orqali statsionar aloqa uchun diametri 3-4 m bo'lgan antennali katta o'lchamli terminallardan foydalanish davom etmoqda [6].

XXOA operativ bo'g'indagi qo'shnlarni boshqaruvini mustahkamlash va zamonaviy milliy maxsulotlar turini ko'paytirish borasida hozirda katta masshtabdagi ishlar olib bormoqda. Shuningdek, sun'iy yo'ldosh aloqasini tashkil etishning zamonaviy modellari va usullari bo'yicha ham tadqiqot va izlanishlar olib bormoqda.

Xulosa qilib aytganda XXOA o'z qo'shnlarni sun'iy yo'ldosh aloqa tizimi orqali boshqaruvini tashkillashtirishiga asosiy e'tiborlarini qaratmoqdalar. Shuningdek, har qanday bo'linmalarni mustaqil boshqaruv tizimini joriy etish orqali jangovar harakatlarda muvaffaqiyatga erishishga intilmoqdalar. Bu masalada ularning yetakchi tadqiqot institutlari va tadqiqotchilari tomonidan istiqbolli ishlar amalga oshirilmoqda. XXOA siyosiy rahbariyatini fikriga ko'ra 2027-yilga kelib qurolli kuchlar tarkibidagi barcha harbiy xizmatchilar sun'iy yo'ldosh aloqasi orqali boshqaruviga to'liq qamrab olinishi rejalashtirilgan.

Qozog'iston Respublikasi (QR) qurolli kuchlarida sun'iy yo'ldosh aloqa tizimi orqali boshqaruvini tashkil etish bo'yicha dastlabki qadamlar 2011-yilga borib taqaladi. 2011-Rossiya kompaniyalari bilan hamkorlikda birinchi sun'iy yo'ldosh KazSat – 2 Boyqo'ng'ir kosmodromidan orbitaga uchirildi (Milliy mahsulot sifatida).

KazSat - 2 kosmik kemasining xizmat ko'rsatish maydoni Qozog'iston Respublikasining butun hududini, Markaziy Osiyo mamlakatlari hududini va Rossiyaning Markaziy qismini tengsizligi bilan o'z ichiga qamrab oladi.

Ushbu sun'iy yo'ldoshni orbitaga uchirishdan asosiy maqsad dastlab - Qozog'iston Respublikasida axborot ta'minoti bilan bog'liq barcha muammolarni hal qilish belgilangan bo'lsa, 2017-yilga kelib bu maqsadlar tarkibiga qurolli kuchlarni sun'iy yo'ldosh aloqasini ta'minlash ham kiritilgan.

QR siyosiy rahbariyati so'nggi qirq yillikdagi urushlar va qurolli mojarolar tahlillariga tayangan holda 2014-yilga kelib sun'iy yo'ldosh aloqa tizimini tashkillashtirish va rivojlantirish bo'yicha keng masshtabdagi choralarni qo'llamoqdalar. Jumladan, "Raqamli Qozog'iston" davlat dasturining "raqamli Ipak yo'li" tashabbusi ortidan butun QR tarkibidagi (chekka hududlarni ham inobatga olgan holda) aholi va qurolli kuchlar tarkibidagi kuch tuzilmalarini 2030-yilgacha sun'iy yo'ldosh aloqa tizimi bilan qamrab olishni maqsad qilganlar [7].

Shuningdek, 2018-yilda Mustaqil Davlatlar Hamdo'stligi davlatlari tasarrufidagi suniy yo'ldosh aloqa tizimiga qo'shilish bo'yicha memorandum imzolangan bo'lsa, 2019-yilda Rossiya, 2021-yilda Xitoy Xalq Respublikasining yetakchi kompaniyalari bilan ko'p maqsadli shartnomalar imzolandi.

2022-yilning may oyida QR qurolli kuchlarini sun'iy yo'ldosh orqali boshqaruvini tashkillashtirish bo'yicha asosiy rahbariy xujjat bo'lgan "Qozog'iston osmoni" ishlab chiqildi va unda 70 dan ortiq tadbirlar belgilandi. Ushbu hujjatga asosan qurolli kuchlarni sun'iy yo'ldosh orqali boshqaruvini tashkillashtirish bo'yicha istiqbolli tendensiyalar belgilandi.

Bugungi kunda QR qurolli kuchlarini sun'iy yo'ldosh orqali boshqaruvini tashkillashtirish bo'yicha katta masshtabdagi loyihalar ilgari surilmoqda va davlat budjetidan mablag'lar ajratilib kelinmoqda.

Ushbu dasturga asosan sun'iy yo'ldosh aloqa tizimini tarkibiy ko'rinishlari quyidagi 1-jadvaldagi ko'rinishga ega bo'ladi.

1-jadval

QR sun'iy yo'ldosh aloqasini tashkillashtirish jadvali

Sputnik nomlanishi	Holati	Ishga tushirilgan kuni
KazSat-2	ishlamogda	2011
KazSat-3	ishlamogda	2014
KazSat-2R	rejada	2018-2025
KazEOSat-1,2	ishlamogda	2014
KazSTSAt-1,2	rejada	2025
Al-pharabi-2	rejada	2022-2027
KazEOSat-3,4	rejada	2023-2027
Milliy ko'rinish	rejada	2024-2030

Bugungi kunda QR qurolli kuchlari tarkibidagi qo'shnlarni sun'iy yo'ldosh orqali boshqaruvini tashkil etish bo'yicha quyidagi yo'nalishlarda istiqbolli islohatlar olib borilmoqda:

2027-yilgacha qurolli kuchlar tarkibiga sun'iy yo'ldosh boshqaruvi qamrovini jadalashtirish; zamonaviy milliy sun'iy yo'ldosh kemalarini orbitaga uchirish va ulardan qo'shnlarni boshqaruvida foydalanish;

qurolli kuchlar tarkibida sun'iy yo'ldosh aloqasini ta'minlash imkoniyatiga ega bo'linmalarni joriy etish;

sun'iy yo'ldosh aloqa tizimini tashkillashtirish bo'yicha zamonaviy model va usullarni ishlab chiqish;

qo'shinlar o'rtasida ma'lumot uzatilishini shifrlash.

Xulosa qilib aytganda Qozog'iston respublikasi harbiy siyosiy rahbariyati so'nggi yillardagi qurolli to'qnashuvlar natijasidan kelib chiqib sun'iy yo'ldosh aloqa tizimi orqali qo'shinlarni boshqarishni butun qurolli kuchlar miqiyosida qamrab olishni, sun'iy yo'ldosh aloqa tizimida ishlash imkoniyatiga ega bo'linmalarni tashkiliy shtat tuzilishlariga kiritish hamda zamonaviy vositalar bilan ta'minlash, shuningdek, yangicha boshqaruv usul va modellarini isloh qilishga asosiy e'tiborlarini qaratmoqdalar hamda bu borada katta hajmdagi ishlarni bajarib ulgurishgan.

Yuqorida rivojlangan davlatlarni sun'iy yo'ldosh aloqa tizimi orqali qo'shinlarni boshqarish tajribalarini tahlil qilib buning natijasida quyidagicha **xulosalar qilish mumkin**:

yetakchi xorijiy davlatlar hozirgi tahlilali zamonda o'zlarini qurolli kuchlari tarkibida ixcham, yuqori harakatchanlikka ega bo'linmalarni joriy etish ularni zamonaviy qurol, jangovar va maxsus texnikalar bilan butlash bilan birga ularni zamonaviy, xavfsiz, barcha aloqani tashkillashtirish talablariga javob beradigan sun'iy yo'ldosh orqali qo'shinlarni boshqarish bo'yicha bosqichma-bosqich isloh qilish ishlarini amalga oshirib kelayotganligini guvohi bo'ldik;

shu bilan birga qurolli kuchlari tarkibidagi qo'shinlarni tashkiliy shtat tuzilishlariga sun'iy yo'ldosh aloqa tizimi bilan ishlash imkoniyatiga ega bo'lgan maxsus bo'linmalarni joriy etishga intilmoqda.

Bundan tashqari sun'iy yo'ldosh aloqa tizimi orqali qo'shinlarni boshqaruvini tashkillashtirish bo'yicha zamonaviy model va moslashuvchan usullarni ishlab chiqarish orqali bo'linmalar o'rtasida turg'un va barqaror aloqani tashkillashtirish, ma'lumotlar almashinuvini yaxshilash, jangni to'g'ri rejalashtirish va olib borish orqali o'z oldiga qo'yilgan vazifalarni bajrisha harakat qilmoqdalar.

Bundan kelib chiqib quyidagilarni **taklif etish mumkin**:

birinchidan, yetakchi xorijiy davlatlari armiyalari tarkibida sun'iy yo'ldosh aloqa tizimini tashkil etish tajribalarini doimiy o'rganib borish va tegishli xulosalar qilish;

ikkinchidan, dunyodagi yetakchi xorijiy davlatlar kompaniyalari va tashkilotlari bilan qo'shinlarni sun'iy yo'ldosh aloqa tizimini tashkil etish bo'yicha uzviy hamkorlikni yo'lga qo'yish;

uchinchidan, O'zbekiston Respublikasi mudofaa vazirligi tizimidagi qo'shinlarni sun'iy yo'ldosh aloqa tizimi orqali boshqaruvini tashkil etish bo'yicha keng ko'lamli ishlarni tashkil etish hamda milliy modelini yaratish;

to'rtinchidan, sun'iy yo'ldosh aloqa tizimi bilan ishlovchi maxsus bo'linmalar tashkiliy shtat tarkiblariga integratsiya qilish, shuningdek, kerakli mutaxassislarini tayyorlash.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

[1] Sklarsky, T.A. Developing the Future Soldier System/Army Research.-January-February 1993.-P.35-36.

[2] Hallion, R.P. Desert Storm 1991. The Most Shattering Air Campaign in History. Osprey Publishing.

[3] Izbosarov, A.F. Harbiy aloqani tashkil qilish tamoyillari/ Darslik II-qism. Asqarov U.J., To'rayev B.T., Voxidov M.B., Yaxyoyev A.A., Nazarov A.A. O'zbekiston Respublikasi Mudofaa vazirligi nashri, 2021. - 97 b.

[4] Goksel, E. (2022). "Satellite Communication and Its Role in Modern Warfare: Ukraine's Use of Starlink". International Security Studies Journal.

[5] Последствия модернизации НОАК. www.indefenseforum.com/ru/ 2023/08.

[6] Доброходов, В. Системы военной спутниковой связи Китая. Зарубежное военное обозрение. Доброходов В. 2016 г. №2, С.-65-66.

[7] Unescap.Org/sites/default/files/Kazakhstan_6.

ҲАРБІЙ БЎЛИНМА ЖАНГАВОР САЛОҲИЯТИНИ БАҲОЛАШНИНГ МАТЕМАТИК МОДЕЛЛАШТИРИШИ

З.Р. ИМИНОВ

Ўзбекистон Республикаси Мудофаа вазирлиги

Аннотация. Ушбу мақолада ҳарбий бўлинмалар жанговор салоҳиятини аниқлаш ва баҳолашда қўлланиладиган математик моделлар таҳлил қилинган. Ҳарбий хизматчиларнинг индивидуал салоҳияти асосида бўлинманинг умумий жанговор салоҳиятини аниқлаш усул ва алгоритмлари таклиф этилган. Бунда аскарларнинг жисмоний, руҳий ва тайёргарлик даражалари ҳисобга олинган ҳолда жанговор салоҳиятни баҳолашнинг аниқ ва илмий ёндашувлари асосланган.

Калит сузлар: жанговор салоҳият, ҳарбий бўлинма, математик моделлаш, баҳолаш алгоритми, аскар салоҳияти, ўртача қиймат, жанговор тайёргарлик, баҳолаш мезони, салоҳият йиғиндиси, ҳарбий таҳлил, баҳолаш усули, ҳисоблаш модели, самарадорлик.

Аннотация. В данной статье рассматриваются математические модели, применяемые для определения и оценки боевого потенциала военных подразделений. Предложены методы и алгоритмы, позволяющие рассчитать совокупный боевой потенциал подразделения на основе индивидуальных показателей военнослужащих, включая их физическую, психологическую и профессиональную подготовленность.

Ключевые слова: боевой потенциал, воинское подразделение, математическое моделирование, алгоритм оценки, потенциал солдата, среднее значение, боевая подготовка, критерии оценки, сумма потенциалов, военный анализ, метод оценки, расчетная модель, эффективность.

Abstract. This article explores mathematical models used to determine and evaluate the combat potential of military units. It proposes methods and algorithms to calculate a unit's total combat capacity based on the individual capabilities of servicemen, taking into account their physical condition, psychological stability, and combat readiness.

Keywords: combat potential, military unit, mathematical modeling, assessment algorithm, soldier potential, average value, combat readiness, evaluation criteria, sum of potentials, military analysis, evaluation method, computational model, efficiency.

Ҳарбий жанговор салоҳиятини аниқлаш масалалари таҳлили ва уларни ечиш усул ва алгоритмлари ҳамда олинган натижаларни қуролли кучлар тизими барча жаҳонларига тадбиқи ҳозирги куннинг ўта долзарб муаммоларидан бири ҳисобланади. Жумладан, қуролли кучлар тизимида маълумотларни интеллектуал таҳлил қилиш масалаларини ечишда Ҳарбий салоҳиятини характерловчи белгилар ва белгилар мажмуаси аро яширин боғлиқликларни ҳамда қонуниятларни аниқлашда ўлчам, фазо муаммоларига дуч келинади. Аскар жанговор салоҳиятини аниқлашнинг асосий босқичларидан бири бўлиб, бўлинмалаштириш масаласини ечишни мазмунан белгилаб берувчи мезонларни танлашга бориб тақалади[1].

Масаланинг қўйилиши. Фараз қилайлик, Аскарларнинг жанговор салоҳиятини белгиловчи, экспертлар томонидан аниқланган бошланғич маълумотлар асосида шакллантирилган Ҳарбийлар бўлинмалари қуйидаги кўринишда берилган бўлсин:

$$X_1 = \begin{bmatrix} x_{11}^1 & x_{11}^2 & \dots & x_{11}^N \\ x_{12}^1 & x_{12}^2 & \dots & x_{12}^N \\ \vdots & \vdots & \ddots & \vdots \\ x_{1m_1}^1 & x_{1m_1}^2 & \dots & x_{1m_1}^N \end{bmatrix} \dots X_r = \begin{bmatrix} x_{r1}^1 & x_{r1}^2 & \dots & x_{r1}^N \\ x_{r2}^1 & x_{r2}^2 & \dots & x_{r2}^N \\ \vdots & \vdots & \ddots & \vdots \\ x_{rm_r}^1 & x_{rm_r}^2 & \dots & x_{rm_r}^N \end{bmatrix}. \quad (1)$$

Буни умумий кўринишда қуйидагича ифодалаш мумкин:

$$K_p = \begin{bmatrix} x_{p1}^1 & x_{p1}^2 & \dots & x_{p1}^N \\ x_{p2}^1 & x_{p2}^2 & \dots & x_{p2}^N \\ \vdots & \vdots & \vdots & \vdots \\ x_{pm_p}^1 & x_{pm_p}^2 & \dots & x_{pm_p}^N \end{bmatrix} \quad (2)$$

Бу ерда $p = \overline{1, r}$; ҳамда жанговор бўлинмалар $X = \bigcup_{p=1}^r X_p$ кўринишда ифодаланиб, улар ўзаро кесишмайдиган бўлинмалардан иборат бўлсин, яъни $X_p \cap X_q = \emptyset, (p \neq q, p = \overline{1, r}; q = \overline{1, r};)$ шартлар берилган.

Худди шунингдек, Ҳарбий x_{pi} - нинг компоненталари x_{pi}^j - номинал сонлардан иборат бўлиб, у қуйидагича ўқилади: p - бўлинмага тегишли i - аскарнинг j - белгиси. Бу ерда $p = \overline{1, r}; i = \overline{1, m_p}; j = \overline{1, N}$; ҳамда r -берилган бўлинмаларнинг умумий сони, m_p - p -бўлинмадаги Ҳарбийларнинг умумий сони ва N - белгиларнинг умумий сонини билдиради.

1-масала. Қаралаётган Ҳарбий бўлинма аскарларини характерловчи белгиларнинг фойдаланишга яроқлилик даражалари аниқлансин[2].

2-масала. Қаралаётган Ҳарбий бўлинма аскарларини характерловчи белгилар узлуксиз микдорий кўринишдан 0 ёки 1 кўринишга ўтказилсин.

3-масала. X_p Ҳарбий бўлинма аскарларини бўлинмалаштириш масаласини ечиш, яъни бўлинмаларга ажратилган аскарнинг ўз бўлинмасини мукамал шаклланишига қўшган ҳиссасини аниқлаш талаб этилади.

Қўйилган амалий масалаларни ечиш босқичлари: 1-босқич. Юқорида келтирилган X_p бўлинмага тегишли ҳар бир аскарни характерловчи белгилар фойдаланишга яроқлиги даражасини аниқлаш ҳар бир бўлинма учун алоҳида қуйидагича кетма-кетликда амалга оширилади:

а) қуйидаги белгилашлар киритайлик: $\bar{x}_p = (\bar{x}_p^1, \bar{x}_p^2, \dots, \bar{x}_p^N)$ вектор, X_p бўлинмаларнинг ўрта вакил Ҳарбийлари, $p = \overline{1, r}$. Унинг компоненталари қуйидаги формула орқали ҳисоблансин:

$$\bar{x}_p^j = \frac{1}{m_p} \sum_{i=1}^{m_p} x_{pi}^j, p = \overline{1, 3}, j = \overline{1, 27}, i = \overline{1, m_p}; \quad (3)$$

б) белгилар кесимида ўртача квадратик оғиш(четланиш) $D(\bar{x}_p^j)$ қуйидаги формула орқали ҳисоблансин:

$$D(\bar{x}_p^j) = \sqrt{\frac{1}{m_p} \sum_{i=1}^{m_p} (\bar{x}_p^j - x_{pi}^j)^2}, p = \overline{1, 3}, j = \overline{1, 27}, i = \overline{1, m_p}. \quad (4)$$

Қуйидаги тенгсизлик бажарилсин ва унинг кўрсаткичлари бўлинма аскарларига нисбатан фоиз кўринишида ҳисоблансин:

$$|\bar{x}_p^j - x_{pi}^j| \leq D(\bar{x}_p^j), p = \overline{1, r}, j = \overline{1, N}, i = \overline{1, m_p}. \quad (5)$$

Ҳарбийларнинг салоҳиятини аниқловчи белгиларнинг бошланғич маълумотларнинг узлуксиз микдорий кўринишдан параметрлари 0 ва 1 лардан иборат бўлган вектор кўринишга алмаштириш жараёни амалга оширилади[3].

Юқорида келтирилган X_p бўлинмага тегишли ҳар бир Ҳарбийни характерловчи ноль ёки бир қийматли белгилар қийматларини вектор кўринишдаги қийматга ўтказиш жараёни ҳар бир бўлинмадаги ҳар бир ҳарбийнинг характерловчи белгилар барча бўлинма ва барча белгилар кесимида қуйидаги белгилашларни киритиш орқали амалга оширилади:

а) $\bar{x}_p = (\bar{x}_p^1, \bar{x}_p^2, \dots, \bar{x}_p^N)$ вектор, X_p бўлинмаларнинг ўртача вакил Ҳарбийлари, $p = \overline{1, r}$.
Унинг компоненталари қуйидаги формула орқали ҳисоблансин:

$$\bar{x}_p^j = \frac{1}{m_p} \sum_{i=1}^{m_p} x_{pi}^j, p = \overline{1, r}, j = \overline{1, N}, i = \overline{1, m_p}; \quad (6)$$

б) векторлар $a_p = (a_p^1, a_p^2, \dots, a_p^N)$ ва $b_p = (b_p^1, b_p^2, \dots, b_p^N)$, қуйидаги кўринишда белгилайлик ва унинг компоненталари ушбу формула орқали ҳисоблансин:

$$a_p^j = \frac{1}{m_p} \sum_{i=1}^{m_p} (\bar{x}_p^j - x_{pi}^j)^2, p = \overline{1, r}, j = \overline{1, N}. \quad (7)$$

$$b_{pi}^j = (\bar{x}_p^j - x_{pi}^j)^2, p = \overline{1, r}, j = \overline{1, N}. \quad (8)$$

Бу босқич якунида берилган 3 та бўлинма Ҳарбийларини характерловчи белги қийматларини 0 ва 1 вектор кўринишдаги қийматга алмаштирилади[4].

X_p бўлинма ҳарбийларининг бўлинмалаштириш масаласини ечиш, яъни бўлинмалардаги ҳар бир ҳарбийни ўз бўлинмасига ёки ўзидан бошқа бўлинмага тегишлилиги аниқланади.

Бунда X_p бўлинмага тегишли бўлган ҳар бир ҳарбий ўз бўлинмасидаги ҳамда бошқа бўлинмалардаги Ҳарбийлар билан бирма - бир қиёслашни, информатив белгилар фазосида Ҳарбийлараро яқинлик функцияси $\rho_i(x_{p1}, x_{p2})$ ни қуйидагича амалга оширилади:

$$\rho_i(x_{p1}, x_{p2}) = \begin{cases} 1 & \text{агар } (x_{p1}^i - x_{p2}^i) = 0, i = \overline{1, N}, \\ 0 & \text{акс ҳолда.} \end{cases} \quad (9)$$

Биринчи шарт иккита ҳарбийлар орасидаги ўхшашлик даражасини билдирса, иккинчи шарт эса уларнинг бир-бирдан фарқли эканлигини билдиради.

Қиёсий баҳолаш йиғиндиси қуйидаги формула орқали амалга оширилади:

$$\Gamma_j(x_{pj}, x_{pk}) = \sum_{k=1}^{m_p} \sum_{i=1}^N \rho_i(x_{pj}, x_{pk}), j = \overline{1, m_p}; k = \overline{1, m_p}; j \neq k; \quad (10)$$

Қиёсий баҳолаш ҳар бир бўлинма бўйича ҳисобланиб, олинган йиғиндиларнинг ўртача қийматларидан энг каттаси ҳарбийнинг шу бўлинма шаклланишига қўшган ҳиссасини билдиради.

Юқорида қўйилган масалаларни ечиш орқали қуйидаги натижаларга эришилди:

- биринчи масалага кўра, биз қараётган ўқув танлама бўлинмалари ҳарбийларини характерловчи белгиларнинг фойдаланишга яроқлиги қай даражада эканлигини аниқланди;

- иккинчи масалага кўра, биз қараётган ҳарбий маълумотларда бўлинмалардаги Ҳарбийларни характерловчи белгилар узлуксиз миқдорий кўринишдан 0 ёки 1 кўринишга ўтказиш жараёни амалга оширилди;

- учинчи масалани ечиш асносида бўлинмаларга ажратилган ҳарбийларнинг ўз бўлинмасига ёки бошқа бўлинмага тегишлилигини аниқлаш жараёни қадамма-қадам амалга оширилиб, ҳар бир қадамда ўз бўлинмасини шаклланишига қўшган ҳиссаси баҳоланди.

Айрим ҳолатларда ҳарбий хизматчиларнинг жанговар қобилиятларини характерловчи белгилар қуйидаги кўринишда берилади: 5(аъло), 4(яхши), 3(қониқарли), 2(қониқарсиз). Ҳарбийларнинг жанговар қобилиятларини юқорида ифодаланган (8), (9) формулалар асосида ҳисоблаш мумкин. Бунинг учун дастлаб (8) асосида белгилар миқдорий кўринишдан 0 ёки 1 кўринишга ўтказиш жараёни амалга оширилади ва сўнгра (9) формуладан фойдаланиб жанговар қобилият ҳисобланади[5].

Ҳарбий хизматчининг жанговар қобилияти аниқлашда бир-бири билан боғлиқ бўлган сифат кўрсаткичларни умумлаштирилади ва қуйидагича аниқланади:

Жисмоний ҳолати. Ҳарбий хизматчининг жисмоний ҳолати унинг соғломлик (саломатлик ҳолати) ва жисмоний тайёргарлик даражаси билан аниқланади.

Маънавий-ахлоқий ҳолати. Ҳарбий хизматчиларнинг маънавий-ахлоқий ҳолати унинг ахлоқий-руҳий ҳолати ва маънавий-маърифий тайёргарлик даражаси билан аниқланади.

Жанговар тайёргарлик ҳолати. ҳарбий хизматчининг жанговар тайёргарлик даражаси унинг жанговар тайёргарлик дастурига кўра белгиланган фанлар бўйича олинган натижалари асосида аниқланади.

Хулоса

Ушбу мақолада ҳарбий бўлинмаларнинг жанговар салоҳиятини аниқлаш ва баҳолаш бўйича математик моделлар ва алгоритмлар таҳлил қилинди. Ҳарбий хизматчиларнинг шахсий салоҳиятларини ўртача қиймат асосида ҳисоблаш орқали бўлинманинг умумий жанговар салоҳияти аниқланиши таъкидланди. Моделлар ва баҳолаш усуллари ҳарбий бўлинмаларнинг самарадорлигини оширишда муҳим аҳамиятга эга эканлиги кўрсатилди. Шу билан бирга, баҳолаш тизимларининг такомиллаштирилиши ҳарбий хизматчиларнинг жисмоний ва руҳий ҳолатларини инобатга олган ҳолда жанговар тайёргарликни аниқ ва самарали баҳолаш имконини беради. Мақола ҳарбий бошқарув жараёнларида илмий ва амалий ёндашувларни жорий этишга ҳисса қўшади.

ФҲЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ:

[1] Mirshohid Aslanov. Reassessing Uzbekistan's military power: a case of underestimated strength // Defense.info (analiz maqola). — 2025.—Highlights reserve forces, budget, logistics for military readiness.

[2] President of the Republic of Uzbekistan. Issues of strengthening the country's defense capability discussed // Official press release. — 2025.—Feb 3 meeting on increasing combat readiness and personnel morale.

[3] Arslon APC introduction and troop modernization // Institute for Strategic and Regional Studies under the President of the Republic of Uzbekistan. — 2025.—Discusses modern equipment and doubling combat power.

[4] Reassessing Uzbekistan's military power... (Rossiya talqinida) // Daryo.uz rus versiyasi. — 2025.—Analysis in Russian of military potential.

[5] Armed Forces of the Republic of Uzbekistan (Wikipedia, includes Russian-language details) — 2025.—Covers structure, manpower, conscription

[6] Vulnerability Assessment Laboratory // Wikipedia. — Describes US Army's vulnerability analysis methods including combat systems.

[7] Center for Army Analysis // Wikipedia. — US Army organization for evaluating combat capability and force effectiveness.

[8] Joint Deployable Analysis Team // Wikipedia. — Covers US military joint analysis exercises to improve combat identification.

**OPTOELEKTRON O'ZGARTKICH VOSITASIDA
MI-171E VERTOLYOTINIG KORPUS TEBRANISHLARINI KOMPENSATSIYALASH
ORQALI EKSPLOATATSIYA MUDDATINI OSHIRISH**

PhD, professor O.S. RAYIMJONOVA

Farg'ona davlat texnika universiteti

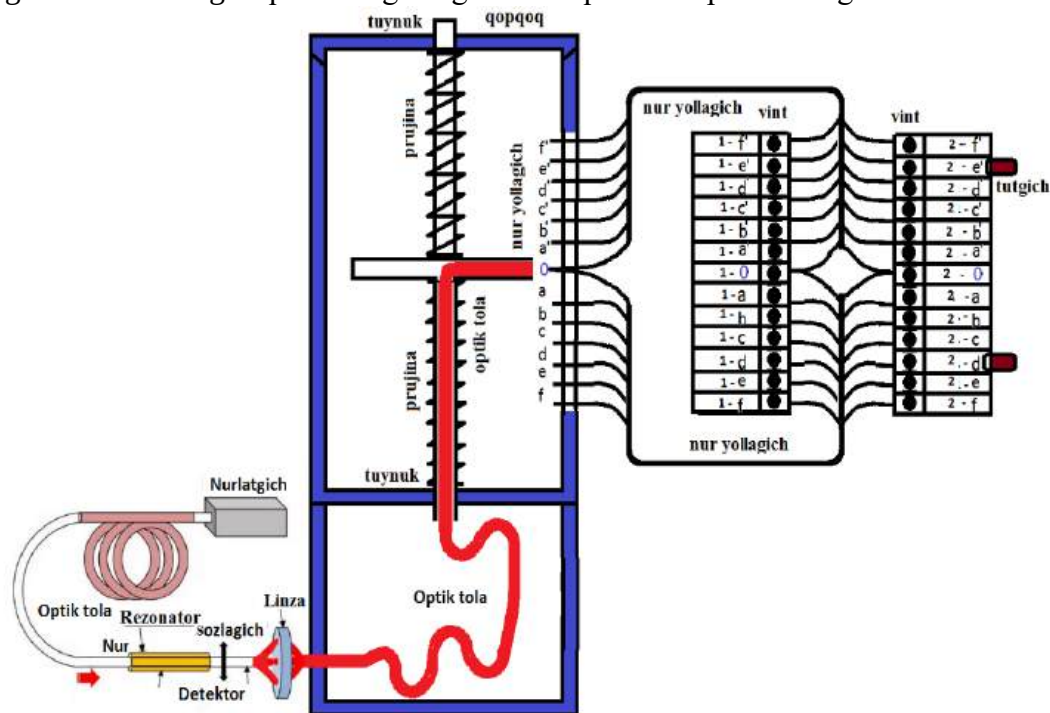
Annotatsiya. Ushbu maqolada Mi-171E rusumli vertolyotning ishlash muddatini uzaytirish va ishonchliligini oshirish maqsadida vertolyot korpusidagi tebranishlarni nazorat qilish va muvozanatlash uchun "Chiziqli ko'chishlarni optoelektron o'zgartkichi" patenti asosida ishlab chiqilgan qurilmani taqdim etadi. Tadqiqotning maqsadi tebranishlarni aniq o'lchash va faol kompensatsiya qilish orqali bort tizimlarining aniqligi va xizmat davomiyligini oshirishdir. Taklif etilayotgan qurilma yordamida tebranish ta'siridagi umumiy noaniqlik darajasi 10,2 % ga bo'lganligini inobatga olgan holda, tebranish ta'sirini aniqlik darajasi 89.795% teng bo'lishi, tizimning tebranishlarni juda yuqori darajada aniqlay olishi va samarali kompensatsiya qilishini tasdiqlaydi. Ya'ni, qurilma vertolyotning rul boshqaruvi va boshqa muhim jihatlari tebranishning salbiy ta'sirini sezilarli darajada kamaytirish imkoniyatini beradi. Bu texnologiya Mi-171E vertolyotlarining samaradorligini oshirish va texnik umrini uzaytirish uchun muhim ahamiyatga ega.

Kalit so'zlar: Mi-171E vertolyoti, vibratsiya kompensatsiyasi, optoelektron o'zgartkich, ish muddatini uzaytirish, vertolyot korpusi, chiziqli siljishlar, faol kompensatsiya, aniqlik, bort tizimlari, texnik xizmat.

KIRISH. Mi-171E mashhur Mi-8/17 vertolyot oilasining modernizatsiya qilingan versiyasi bo'lib, turli maqsadlarda keng qo'llaniladi. U asosan yuk tashish, yo'lovchi transporti, tibbiy evakuatsiya va qidiruv-qutqaruv operatsiyalari uchun mo'ljallangan. Qurolli versiyalarida raketalar, pulemyotlar va zambaraklar bilan jihozlanishi mumkin. Kuchli dvigatellari yuqori yuk ko'tarish qobiliyati va turli iqlim sharoitlarida, jumladan tog'li hududlarda ham samarali ishlash imkonini beradi. Harbiy vertolyotlarning parvozi, ayniqsa, eskiroq modellardagilari, kuchli tebranishlar bilan bog'liq. Bu holat ekipajga noqulaylik tug'diribgina qolmay, vertolyot korpusining tuzilmaviy yaxlitligiga, shuningdek, bortdagi barcha muhim tizimlar, jumladan navigatsiya, aloqa, boshqaruv va nishonga olish qurilmalarining faoliyatiga salbiy ta'sir ko'rsatadi. Doimiy tebranishlar mexanizmlarning yemirilishini tezlashtiradi, elektron komponentlarning nosozlik xavfini oshiradi. Mi-171E rusumli vertolyotlar konstruktiv xususiyatlari tufayli ma'lum tebranishlarga ega. Ularning uzoq muddatli ekspluatatsiyasi uchun korpus tebranishlarini samarali boshqarish va kompensatsiyalash muhimdir. Ushbu maqola O'zbekiston Respublikasining "Chiziqli ko'chishlarni optoelektron o'zgartkichi" (UZ IAP 05858) patenti asosida vertolyot korpusidagi tebranishlarni aniq o'lchash va ularning salbiy oqibatlarini minimallashtirishga qaratilgan ishlanmani yoritadi. Tadqiqotning asosiy maqsadi vertolyot korpusining umumiy barqarorligini oshirish orqali uning xizmat muddatini uzaytirish hamda bort tizimlarining samaradorligini ta'minlashdir.

MATERIALLAR VA USULLAR. Harbiy vertolyotlarning parvozi paytida tebranishlar asosiy va dum rotorlari, dvigatellar va transmissiya tizimlarining ishlashi, shuningdek, aerodinamik omillardan kelib chiqadi. Bu tebranishlar korpusga uzatilib, keng chastota diapazonida va turli amplitudalarda sodir bo'ladi. Natijada, korpusning tuzilmaviy buzilishi, bortdagi uskunalarning yemirilishi, sensorlarning aniqligi pasayishi va umumiy ishonchlilikning kamayishi kuzatiladi. Qurilma orqali patentda tasvirlangan optoelektron o'zgartirgichni korpus qismiga integratsiya qilish orqali vibratsiyalarni yuqori aniqlikda aniqlash va ular asosida faol/yarim-faol kompensatsiya tizimlarini boshqarish hisoblanadi.

Qurilma optik tolali sensorlar prinsipiga asoslangan. Uning ichidagi harakatlanuvchi naychasimon vtulka va flanes orqali o'tgan svetovod orqali yorug'lik o'tadi. Vibratsiya ta'sirida vtulka siljiganda, svetovodning flanesdagi teshikka nisbatan joylashuvi o'zgaradi, bu esa chiqaruvchi svetovodlarga tushadigan yorug'lik miqdorini o'zgartiradi. Bu yorug'lik o'zgarishi fotoqabul qilgichlar tomonidan elektr signalga aylantiriladi. Bu signallar ko'prik sxemalari, kuchaytirgichlar va analog-raqamli o'zgartirgichlar orqali mikroprotsessorga uzatiladi.



1-rasm. Optoelektron o'zgartirgich qurilmasining konstruksiyasi

Qurilmaning ilmiy-texnik yechimi quyidagilarni o'z ichiga oladi: aniq o'lchov – optoelektron o'zgartirgich nishonlash tizimining muhim nuqtalariga (masalan, girostabilizatsiyalangan platformaga) joylashtirilib, uning vertolyot korpusiga nisbatan yoki o'zining ichki qoldiq vibratsiyalarini aniq o'lchaydi; real vaqtda qayta ishlash – o'zgartirgichdan olingan ma'lumotlar yuqori tezlikda mikroprotsessor tomonidan qayta ishlanadi, bunda vibratsiyaning amplitudasi, chastotasi va yo'nalishi aniqlanadi; faol/yarim-faol kompensatsiya – qayta ishlangan ma'lumotlar asosida faol (piezoelektrik aktyuatorlar) yoki yarim-faol (magnitoreologik dempferlar) kompensatsiya tizimlari boshqariladi. Bu tizimlar korpus holati tizimiga aniqlangan vibratsiyaga qarama-qarshi yo'nalishda kuch yoki siljish qo'llash orqali uning barqarorligini ta'minlaydi; ogohlantirish va monitoring – agar vibratsiya darajasi ruxsat etilgan chegaralardan ohsa, mikroprotsessor optik va tovush signalizatsiyasini ishga tushiradi. Operatorga tezkor qaror qabul qilishga yordam beradi. Patent tavsifiga asoslanib, qurilmadagi yorug'likning intensivligini siljishga bog'liqligini aks ettiruvchi soddalashtirilgan matematik modelni yaratish mumkin.

Faraz qilaylik:

- L_0 - nurlanish manбайдan chiqayotgan yorug'likning umumiy intensivligi.
- x - naychasimon vtulkaning chiziqli siljishi (vibratsiya ta'sirida).
- A - svetovodning flanesdagi teshigining radiusi.
- k - svetovoddan chiqayotgan nurning difraksiyasini yoki tarqalishini hisobga oluvchi koeffitsient.
- $I_1(x)$ va $I_2(x)$ - ikkita qabul qilgichga tushadigan yorug'lik intensivliklari.

Patentda ikki guruh chiqaruvchi tolali svetovodlarning kirish toreslari joylashgan plastina va ikkita nurlanish qabul qilgichi o'rnatilgan qo'shimcha plastina ko'rsatilgan. Bu differensial o'lchov sxemasi ekanligini anglatadi. Agar svetovodning markazi siljishga proporsional ravishda o'zgarsa,

ikki qabul qilgichga tushadigan yorug'lik intensivliklari quyidagicha ifodalanishi mumkin (chiziqli yaqinlashishda):

$$I_1(x) = I_{ref} + C \cdot x; \quad I_2(x) = I_{ref} - C \cdot x; \quad (1)$$

Bu yerda I_{ref} – siljish mavjud bo'lmagandagi ($x=0$) o'rtacha yorug'lik intensivligi. C – qurilmaning sezgirlik koeffitsienti, bu 20ptic tizimning geometriyasi va yorug'lik tarqalishiga bog'liq.

Qabul qilgichlar ko'priksimon sxemalarga ulangan. Bunday sxemalarda chiqish signali ikki kirish signalining farqiga proporsional bo'ladi, bu esa tashqi shovqinlarning ta'sirini kamaytiradi.

Farqli signal:

$$U_{diff} = K \cdot (I_1(x) - I_2(x)); \quad U_{diff} = K \cdot ((I_{ref} + C \cdot x) - (I_{ref} - C \cdot x)); \quad (2)$$

$$U_{diff} = K \cdot (2C \cdot x); \quad U_{diff} = (2KC) \cdot x \quad (3)$$

Bu yerda K - qabul qilgichlar va ko'priksimon sxemasining umumiy konversiya koeffitsienti (V/luks). Demak, chiqishdagi elektr signali (U_{diff}) siljish x ga chiziqli bog'liq bo'ladi. Mikroprotessor ushbu U_{diff} qiymatini analog-raqamli o'zgartirgichlar orqali qabul qilib, siljish x ni hisoblaydi:

$$x = U_{diff} / (2KC) \quad (4)$$

Vibratsiyaning chastotasini aniqlash: Mikroprotessor $x(t)$ signalning vaqtga bog'liq o'zgarishini tahlil qilib, uning maksimal va minimal qiymatlarini (amplituda) va vaqt birligidagi tebranishlar sonini (chastota) aniqlaydi. Fure transformatsiyasi (FFT) algoritmi yordamida vibratsiyaning chastota spektrini olish mumkin.

Noaniqlikni baholash va hisoblash usuli: Tizimning tebranish ta'siridagi umumiy noaniqligini baholashda quyidagi asosiy komponentlar inobatga olinadi:

- **Bazaviy noaniqlik (U_{base}):** Bu yangi tizimning bazaviy noaniqligidir. U sensorlarning o'ziga xos aniqligi, kalibrlash xatolari va boshqa ideal sharoitdagi xatoliklarni o'z ichiga oladi. Faraz qilaylik, $U_{base}=10\%$.

- **Texnik eskirishdan kelib chiqadigan noaniqlik (U_{aging}):** Buni parvoz soatlariga (T_{flight}) bog'liq chiziqli funksiya sifatida ifodalash mumkin, bunda eskirish koeffitsienti (K_{aging}) qo'llaniladi. Faraz qilaylik, har 1000 parvoz soati uchun degradatsiya noaniqlikka 0.5% qo'shimcha xatolik qo'shadi:

$$U_{aging} = K_{aging} \cdot \left(\frac{K_{flight}}{1000 \text{ soat}} \right); \quad (5)$$

Bu yerda, $K_{aging}=0.5\%$ (gipotetik eskirish koeffitsienti).

- **Harorat o'zgarishidan kelib chiqadigan noaniqlik (U_{temp}):** Buni tizimning normal ishlash haroratidan (ΔT) chetlanishiga bog'liq chiziqli funksiya sifatida ifodalashimiz mumkin, bunda harorat koeffitsienti (K_{temp}) qo'llaniladi. Faraz qilaylik, har 10°C harorat o'zgarishi 0.2% qo'shimcha xatolik keltirib chiqaradi: $U_{temp} = K_{temp} \cdot \left(\frac{|\Delta T|}{10^\circ\text{C}} \right)$ Bu yerda, $K_{temp}=0.2\%$ (gipotetik harorat koeffitsienti) va $|\Delta T|$ – o'rtacha ekspluatatsiya haroratidan mutlaq chetlanish.

- **Umumiy noaniqlik (U_{total})** quyidagi formulasi orqali hisoblanadi:

$$U_{total} = \sqrt{U_{base}^2 + U_{aging}^2 + U_{temp}^2} = \sqrt{(10\%)^2 + (2\%)^2 + (0.4)^2} = \sqrt{100 + 4 + 0.16} \approx 10.205\%$$

- **tebranish ta'sirini aniqlik darajasi:**

$$100\% - U_{base} = 100\% - 10.205\% = 89.795\%$$

NATIJALAR. Ushbu ishlanmaning amalga oshirilishi Mi-171E vertolyotlarining umumiy texnik holati va foydalanish muddatini yaxshilashga olib keladi. Optoelektron o'zgartkich orqali korpus tebranishlarning aniq o'lchanishi va faol kompensatsiyasi uning tuzilmaviy barqarorligini oshiradi. Yuqorida keltirilgan hisoblash usuli yordamida, texnik eskirish (masalan, 4000 soat parvoz uchun $U_{aging}=2\%$) va harorat o'zgarishi (masalan, 20°C harorat chetlanishi uchun $U_{temp}=0.4\%$) kabi omillar hisobga olinganda ham, tebranish ta'sirini aniqlik darajasi bazaviy aniqlik ($100\% - U_{base}=10\% = 90\%$ aniqlik) bilan birgalikda, umumiy hisobda 89.795% ga teng bo'lishi tizimning yuqori aniqligini tasdiqlaydi. Bu ko'rsatkich, umumiynoaniqlik

bo'lganligini inobatga olgan holda ($100\% - 10.205\% = 89.795\%$), tizimning tebranishlarni juda yuqori darajada aniqlay olishi va samarali kompensatsiya qilishini tasdiqlaydi. Ya'ni, taklif etilayotgan qurilma vertolyotning rul boshqaruvi va boshqa muhim jihatlariga tebranishning salbiy ta'sirini sezilarli darajada kamaytirish imkoniyatini beradi.

Bundan tashqari, tebranish yuklanishlarining kamayishi bortdagi barcha muhim tizimlar, jumladan dvigatellar, avionika va nishonga olish tizimlarining eskirishini sekinlashtiradi. Bu esa ularning ishonchliligini va ekspluatatsiya muddatini uzaytiradi. Texnik xizmat ko'rsatish xarajatlari qisqarib, vertolyotning jangovar tayyorgarligi yuksaladi. Ishonchlilikning oshishi, ayniqsa eski rusumdagi vertolyotlar uchun, ularning yana ko'p yillar davomida samarali xizmat qilishini ta'minlaydi.

MUHOKAMA. Mi-171E kabi vertolyotlar uchun korpus tebranishlarini nazorat qilish muhim, chunki bu ularning ekspluatatsiya muddati va jangovar samaradorligini oshiradi. Mavjud passiv izolyatsiya usullari yuqori chastotali tebranishlarni to'liq bartaraf eta olmasdan, bortdagi nozik uskunalarning eskirishiga olib keladi. Taklif etilayotgan optoelektron o'zgartkich bu muammoga kompleks va faol yechim taqdim etadi. U tebranishni bevosita o'lchash va real vaqtda kompensatsiya qilish orqali vertolyot korpusining barqarorligini oshiradi. Bu yondashuv nishonga olish tizimlarining ishlashini yaxshilab, korpus tuzilmaviy yaxlitligini saqlaydi va avionika kabi muhim agregatlarning ishonchliligini oshiradi.

Noaniqlikni hisoblash usuli tizimning real sharoitdagi aniqligini chuqurroq tushunishga yordam beradi. Bu modellar tizimni optimallashtirish, xizmat muddatini aniqroq prognoz qilish va profilaktik xizmatni rejalashtirish uchun muhim. Eskirish va harorat koeffitsientlari bo'yicha aniq eksperimental ma'lumotlar tizimning ish qobiliyatini ta'minlashda hal qiluvchi ahamiyatga ega. Bu texnologiyaning joriy etilishi eskiruvchi vertolyot parki uchun iqtisodiy jihatdan maqsadga muvofiqdir. Mahalliy patent asosidagi bu ishlanma milliy mudofaa salohiyatini oshirishda muhim qadam bo'lib, kelajakda boshqa havo kemalariga ham tatbiq etilishi mumkin.

XULOSA. Ushbu ishlanma Mi-171E rusumli vertolyotlardagi korpus vibratsiyalarining salbiy ta'sirini "Chiziqli ko'chishlarni optoelektron o'zgartirgichi" patenti asosida ishlab chiqilgan innovatsion qurilma yordamida hal etishga qaratilgan. Qurilma vertolyot korpusining chiziqli siljishlarini yuqori aniqlikda o'lchaydi va bu ma'lumotlarni faol yoki yarim-faol kompensatsiya tizimlarini boshqarish uchun ishlatadi. Taklif etilayotgan qurilma tebranish ta'sirini aniqlik darajasi 89.75% teng bo'lishi tizimning tebranishlarni juda yuqori darajada aniqlay olishi va samarali kompensatsiya qilishini tasdiqlaydi.

Bunda texnik eskirish va harorat o'zgarishi kabi omillar ham hisobga olingan. Bu esa vertolyotning umumiy ishonchliligini, bort tizimlarining xizmat muddatini sezilarli darajada oshiradi va texnik xizmat ko'rsatish xarajatlarini kamaytiradi. Ishlanma Mi-171E vertolyotlarining ekspluatatsiya samaradorligini oshirish, ularning texnik umrini uzaytirish va O'zbekiston Respublikasining mudofaa salohiyatini mustahkamlashda muhim ro'l o'ynaydi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

[1] Azimov, R. K., Shipulin, G. Y., Xolmatov, U. S., Rayimjonova, O. S., Ismailov, X. A., & Abdullaev, T. M. (N.d.). UZ IAP 05858 raqimli ixtiro patenti. O'zbekiston Respublikasi Intellektual mulk agentligi.

- [2] Rayimjonova, O. S., et al. (2020). LR Dalibekov Photo Converter for Research of Characteristics Laser IR Radiation. *International Journal of Advanced Research in Science, Engineering and Technology*, 7(2), pp.12788-12791.
- [3] Shipulin, Yu. G., Raimimonova, O. S., Ergashev, O. M., & Usmanov, Zh. K. (2021). Method for Ensuring Continuous Functioning of Multichannel Systems Control and Recording of Water Composition in Seismic Wells. *International Journal of Advanced Research in Science, Engineering and Technology*, 8(2), pp.16575-16581.
- [4] Kadirov, O. Kh., Shipulin, Yu. G., & Kakhkharov, A. A. (2019). The Multipurpose converter for control of Parameters of Gaseous Environments. *International Journal of Advanced Research in Science, Engineering and Technology*, 6(5), pp.9155-9160.
- [5] Shevtsov, E. A., & Belkin, M. E. (1992). Optik tolali uzatish tizimlarining fotodetektorlari. *Radio va aloqa*.
- [6] Toshpulatov, S. M., Dadabaev, M. M., & Alimdjanov, D. B. (2021). Analysis of the gsm communication channel in security systems. *ACADEMICIA: An International Multidisciplinary Research Journal*, 11(3), pp.681-685.
- [7] Ignatov, A. N. (2006). Optoelektron qurilmalar va qurilmalar: Proc. nafaqa. Eko-trendlar.
- [8] Umarovich, I. U., et al. (2020). Methods of reducing the probability of signal loss on optical fiber communication lines. *Наука, техника и образование*, (6(70)), с.27-31.
- [9] Raimjonova, O.S., et al. (2020). Overview of the experimental reasarche of open optical system for monitoring of deviations of the buildings with concrete products. *Scientific Bulletin of Namangan State University*, 2(6), pp.374-378.
- [10] Turgunov, B., et al. (2021). Researching Of The Degradation Process Of Laser Diodes Used In Optical Transport Networks. In 2021 International Conference on Information Science and Communications Technologies (ICISCT) pp. 1-4. IEEE.
- [11] Искандаров, У. У., & Эгамбердиев, М. М. (2018). Аспекты и проблемы создания и содержания "Умного дома". *Перспективные информационные технологии (ПИТ 2018)*, с. 444-447.
- [12] Toshpulatov, S. M. (2021). Analysis of fiber-optic sensors for diagnostics and monitoring of electrical equipment. *ACADEMICIA: An International Multidisciplinary Research Journal*, 11(3), pp.858-863.

НЕОБХОДИМОСТЬ ВНЕДРЕНИЯ МОДУЛЕЙ УПРАВЛЕНИЯ ПЛАНИРОВАНИЕМ СРЕДСТВ АВИАЦИОННОГО ПОРАЖЕНИЯ: УРОКИ СОВРЕМЕННЫХ КОНФЛИКТОВ

**PhD, доцент А.Х. ИСХОКОВ,
А.П. УГАЙ**

Военный институт информационно-коммуникационных технологии и связи МО РУ

Аннотация. Современные вооружённые конфликты в мире показали необходимость использования высокоточных и малозаметных средств поражения, позволяющих эффективно достигать целей, без входа в зону действия противовоздушной обороны. Одним из ключевых элементов такой стратегии становятся авиационные бомбы оснащенные модулем управления планированием (МУП). Кроме того, наряду с высокой эффективностью применения высокоточных средств поражения, всё большее значение приобретает экономическая эффективность вооружений. В данной статье рассматривается актуальность внедрения дальнобойного авиационного вооружения, а также анализируются преимущества таких средств поражения в современных условиях ведения боевых действий. Необходимость внедрения МУП обосновывается как экономически целесообразная альтернатива крылатым ракетам и традиционным методам поражения. Проведены математические расчёты, раскрывающие тактико-технические возможности авиационных бомб оснащенных МУП и доказывающие снижение затрат на вооружение при сохранении высокой боевой эффективности.

Ключевые слова: авиационные бомбы оснащенные модулем управления планированием, высокоточное оружие, дальнобойность, противовоздушная оборона, современная война, военные конфликты, экономика вооружений, снижение затрат, эффективность применения.

Annotatsiya. Dunyo bo'yicha zamonaviy qurolli mojarolar yuqori aniqlikdagi va kam ko'rinadigan zarba berish vositalaridan foydalanish zarurligini ko'rsatdi. Bunday vositalar havo hujumidan mudofaa (HHM) tizimlari ta'sir doirasiga kirmagan holda belgilangan nishonlarni samarali yo'q qilish imkonini beradi. Ushbu strategiyaning muhim elementlaridan biri bu — yo'nalishli traektoriya asosida harakatlanuvchi boshqaruv moduliga ega aviabombalardir (YTBA). Bundan tashqari, yuqori aniqlikdagi zarba berish vositalarining samaradorligi bilan bir qatorda, qurol-yarog'ning iqtisodiy samaradorligi ham tobora dolzarb ahamiyat kasb etmoqda. Mazkur maqolada uzoq masofali aviatsiya qurollarini joriy etishning dolzarbligi ko'rib chiqiladi, shuningdek, bunday zarba vositalarining zamonaviy jangovar harakatlar sharoitidagi afzalliklari tahlil qilinadi. Boshqaruv moduli bilan jihozlangan aviabombalarni joriy etish qanotli raketalar va an'anaviy zarba vositalariga iqtisodiy jihatdan maqbul alternativ sifatida asoslab beriladi. Shuningdek, YTBA imkoniyatlarini ochib beruvchi taktik-texnik hisob-kitoblarni keltirilib, yuqori jangovar samaradorlikni saqlagan holda qurol-yarog' xarajatlarini sezilarli darajada kamaytirish isboti taqdim etiladi.

Kalit so'zlar: boshqaruv moduliga ega aviabombalar, yuqori aniqlikdagi qurol, uzoq masofali ta'sir, havo hujumidan mudofaa, zamonaviy urush, harbiy mojarolar, qurol-yarog' iqtisodiyoti, xarajatlarni kamaytirish, qo'llash samaradorligi.

Abstract. Modern armed conflicts around the world have demonstrated the critical need for the use of high-precision and low-observable strike systems that can effectively achieve objectives without entering areas covered by enemy air defenses. One of the key components of this strategy is the use of aerial bombs equipped with a Glide Control Module (GCM). In addition to their operational efficiency, the economic effectiveness of such precision-guided weapons is gaining increasing importance. This article examines the relevance of deploying long-range aviation

weaponry and analyzes the advantages of such strike systems in the context of modern warfare. The necessity of implementing GCMs is substantiated as a cost-effective alternative to cruise missiles and conventional strike methods. Mathematical calculations are presented to demonstrate the tactical and technical capabilities of aerial bombs equipped with GCMs, proving that they reduce overall armament costs while maintaining high combat effectiveness.

Key words: Aerial bombs with Glide Control Module (GCM), precision-guided munitions, long-range capabilities, air defense, modern warfare, air defense systems, military conflicts, weapons economics, cost reduction, operational effectiveness.

В мире, отмечается возрастающая роль высокоточного оружия. Успешное поражение ключевых объектов инфраструктуры противника требует применения средств, обеспечивающих не только точность, но и безопасность для авиации, действующей в условиях развитой системы ПВО. Авиационные средства поражения на принципах дистанционного и интеллектуального наведения приобретают всё большую значимость, особенно в условиях насыщенной системы противовоздушной обороны (ПВО) противника. Применение высокоточного авиационного вооружения позволяет достигать стратегических целей без непосредственного входа в зону поражения ПВО.

Разработка вооружений в XXI веке всё больше ориентирована на достижение максимального эффекта при минимальных ресурсных затратах. Концепция «стоимость–эффективность» становится ключевой в процессе модернизации вооружённых сил [1]. В условиях ограниченного бюджета, решение задач уничтожения противника на дальних дистанциях требует не только высокой точности, но и оптимального распределения ресурсов.

В ходе конфликта в Сирии активно использовались как управляемые, так и неуправляемые боеприпасы. Однако именно высокоточные средства, такие как ПАБ и ракеты класса "воздух-земля", позволили авиации коалиции эффективно наносить удары по инфраструктуре с минимальными сопутствующими потерями [2].

Также авиационные бомбы с управляемыми модулями планирования и коррекции (УМПК) эффективно показали себя и в ходе Украинского конфликта, позволяя пилотируемой авиации наносить удары, не заходя в зону действия средств ПВО противника [3]. Например, УПАБ-1500Б, позволял поражать цели на удалении до 50-70 км от линии фронта [4].

Авиабомбы с модулями управления планированием (АМУП) обладают следующими преимуществами:

безопасность носителя - авиация может работать вне зоны действия ПВО, снижая риск потери экипажей;

высокая точность - современные планирующие авиационные бомбы оснащаются спутниковой и инерциальной навигацией, что позволяет достигать кругового вероятного отклонения (КВО) менее 10 м;

сниженные затраты - в отличие от ракет, стоимость ПАБ значительно ниже, при сохранении аналогичного эффекта;

гибкость применения - планирующие боеприпасы могут использоваться с широкого спектра самолётов, включая фронтовую авиацию.

С учётом изменения характера конфликта - от фронтальных атак к маневренной войне дронов, дальнобойных артсистем и высокоточных ударов, можно сделать вывод, что Вооруженные силы, не обладающие соответствующими средствами поражения, теряют инициативу на поле боя. [5].

Проведем исследования тактико-технических характеристик модулей управления планирующими авиабомбами:

Определим математическую зависимость дальности планирования авиационной бомбы от её веса (массы), площади крыла, скорости и высоты сброса, мы рассмотрим модель планирующего объекта в поле силы тяжести и аэродинамического сопротивления.

Определим переменные:

m - масса объекта, кг

S - площадь крыла, м²

V_0 - начальная горизонтальная скорость сброса, м/с

H - высота сброса, м

ρ - плотность воздуха, кг/м³ (на уровне 0–10 км ≈ 1.225 –0.413)

C_L - коэффициент подъемной силы

C_D - коэффициент лобового сопротивления

g - ускорение свободного падения, 9.81 м/с²

Определим аэродинамическое качество E (отношение подъемной силы к сопротивлению):

$$E = \frac{C_L}{C_D} \quad (1)$$

Это отношение показывает, на сколько метров по горизонтали может пролететь объект на каждый метр снижения.

При планирующем полёте дальность (горизонтальная проекция пути) определяется как:

$$D = H * \frac{C_L}{C_D} = H * E \quad (2)$$

Однако для объекта, сбрасываемого с определённой скоростью V_0 , дальность планирования также зависит от этой скорости.

Если объект имеет начальную горизонтальную скорость V_0 , и при этом поддерживает угол планирования с аэродинамическим качеством E , тогда время планирования:

$$t = \frac{H}{V_Z} \quad (3)$$

Где вертикальная скорость:

$$V_Z = \frac{V_0}{E} \quad (4)$$

Следовательно:

$$t = \frac{H * E}{V_0} \quad (5)$$

Тогда дальность:

$$D = V_0 t = V_0 \frac{H * E}{V_0} = H * E \quad (6)$$

Таким образом, при установившемся планирующем полёте дальность зависит только от высоты и аэродинамического качества, и не зависит от массы напрямую.

Подъёмная сила:

$$L = \frac{1}{2} \rho V^2 C_L S \quad (7)$$

В режиме равномерного планирования подъёмная сила уравнивает вес в проекции:

$$L = G * \cos(\theta) \quad (8)$$

Влияние массы проявляется через необходимость увеличения скорости для поддержания равновесия:

$$V = \sqrt{\frac{2mg}{\rho S C_L}} \quad (9)$$

Если учитывать аэродинамическое качество как функцию скорости и массы, можно выразить дальность как:

$$D = H * \frac{C_L(V,m)}{C_D(V,m)} \quad (10)$$

А при малых углах и постоянных коэффициентах:

$$D = H * \frac{C_L}{C_D} = H * E \quad (11)$$

С учетом встречного ветра. Ветер уменьшает эффективную горизонтальную скорость авиационного средства поражения (АСП) с МУП:

$$V_{эф} = V_0 \cos(\theta) - V_{\omega} \quad (12)$$

Если принять угол планирования $\theta \approx \tan^{-1}(1/K)$, тогда:

$$\cos(\theta) = \frac{K}{\sqrt{1+K^2}} \quad (13)$$

В итоге:

$$V_{эф} = V_0 * \frac{K}{\sqrt{1+K^2}} - V_{\omega} \quad (14)$$

Вычисляем время планирования:

$$t = \frac{H}{V_v} \quad (15)$$

Где H – высота, V_v – вертикальная скорость планирования

Получаем итоговую дальность:

$$D_{итог} = V_{эф} * t = \left(V_0 * \frac{K}{\sqrt{1+K^2}} - V_{\omega} \right) * \frac{H * K}{V_0} \quad (16)$$

Возьмем к примеру следующие исходные данные:

$K = 6$, $H = 10000$, $V_0 = 900$ км/ч $V_{\omega} = 10$ м/с

Тогда:

$$R = (0.986 - 0.04) * 10000 * 6 \approx 0.946 * 60000 \approx 56760 \text{ м} \approx 56.8 \text{ км}$$

Получим следующий расчет по диапазонам высоты и скорости применения АСП приближенным к техническим возможностям авиационной техники:

Таблица – 1

Таблица зависимости дальности поражения АСП с массой 500 кг с МУП от высоты и скорости сброса.

Высота (м)	Скорость (км/ч)	Дальность (км)
1000	720	5
3000	720	16
6000	900	33
10000	900	56
12000	1080	71

Графическая зависимость математических расчётов дальности поражения при минимальной и максимальной скорости сброса приведена на Рис.1.

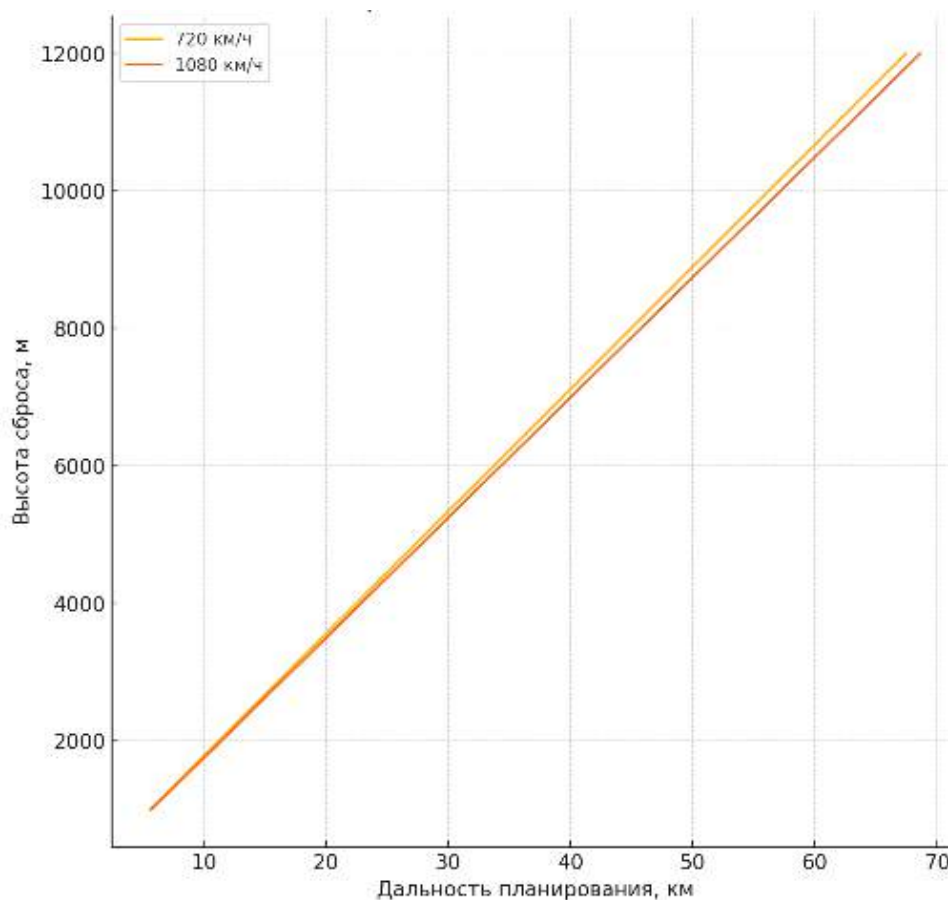


Рис. 1. График зависимости дальности планирования от высоты сброса для скоростей 720 км/ч и 1080 км/ч

Внедрение МУП АСП особенно актуально для Вооруженных сил, стремящихся развивать асимметричные средства сдерживания. Такие боеприпасы могут эффективно использоваться и в условиях ограниченных ресурсов - в отличие от дорогостоящих ракетных комплексов.

Современная концепция ведения боевых действий смещается от огневого подавления к высокоточному поражению точечных целей. Это особенно важно в условиях, когда каждая потеря авиационной техники может иметь стратегические последствия. Планирующие боеприпасы позволяют наносить упреждающие удары без входа в зону поражения противника [6]. Наличие в арсенале модулей управления планированием АСП предоставляет Вооруженным силам возможность асимметричного ответа на угрозу, снижая затраты при сохранении боевой эффективности.

Проведем математическую оценки эффективности. Для этого введем коэффициент Е (эффективность на единицу стоимости):

$$E = \frac{P \cdot D}{\$} \quad (17)$$

где:

P – вероятность поражения цели,

D – допустимая дальность (в км),

\$ – стоимость одного боеприпаса (в у.е.).

Пример:

Для АСП с МУП:

$P = 0.9$; $D = 70$; $C = 25\ 000$

$$E_{\text{МУП}} = \frac{0,9 \cdot 70}{25000} \approx 0,00252 \quad (18)$$

Для «Калибра»:

$P = 0.95$; $D = 1500$; $\$ = \text{более } 1\ 000\ 000$

$$E_K = \frac{0,95 \cdot 1500}{1000\ 000} \approx 0,001425 \quad (19)$$

Таким образом эффективность на доллар у АСП оснащенного МУП более чем в 2 раза выше, несмотря на меньшую дальность. Это делает авиационное средство поражения с МУП оптимальным решением для тактических и оперативных задач в условиях ограниченных ресурсов [7]. Кроме того, у таких высокоточных средств поражения как «Калибр» и ему подобные нет экспортных паспортов (страна производитель не экспортирует данные виды вооружения), а в случае экспорта оставляет за собой возможность контролировать их применение.

В ходе СВО в 2023–2024 гг. Россия массово использовала модернизированные ПАБ для подавления украинской ПВО и разрушения ключевых логистических объектов. По данным опубликованным в средствах массовой информации, с марта по декабрь 2023 года было применено более 2000 ПАБ, что позволило существенно снизить применение дорогостоящих ракетных комплексов «Калибр» [5].

Переход на массовое применение АСП с МУП потребует минимальных затрат [8], в частности основные расходы будут ограничены созданием МУП и системы управления. При этом модернизация имеющихся авиационных средств поражения экономически целесообразное решение, не требующее новых производств [9].

Вывод: на фоне интенсивного развития различных систем ПВО и растущих требований к точности и эффективности авиационных ударов, необходимость внедрения систем высокоточного дальнобойного авиационного поражения с применением МУП становится неоспоримой. Это подтверждается как эмпирическим опытом современных конфликтов, так и стратегической логикой развития военных доктрин. АСП с МУП становятся неотъемлемым элементом современной концепции высокоточной войны. Их внедрение в вооружённые силы является необходимым условием поддержания паритета и повышения боевого потенциала Вооружённых сил. В условиях возрастающей роли ПВО, беспилотных средств разведки и систем РЭБ, АСП с МУП предоставляют стратегическую гибкость и высокую эффективность при минимальных рисках. АСП с МУП представляют собой не только технологически эффективное, но и экономически оправданное решение задач высокоточного поражения. В условиях бюджетных ограничений, модернизация имеющихся на вооружении авиационных средств поражения за счет установки на них МУП обеспечивает оптимальный баланс между стоимостью, точностью и безопасностью применения. Создание и массовое внедрение таких модулей позволит существенно повысить боеспособность национальных вооружённых сил. Наряду с этим, модернизация АСП позволит оперативно уничтожать, любого агрессора вторгшегося на территорию страны на любом операционном направлении на дистанции превышающей радиус действия авиации более чем на 70 км, не подвергая авиацию опасности уничтожения средствами ПВО противника (в том числе современными переносными зенитно-ракетными комплексами). Оперативность будет достигаться за счет того, что время для нанесения удара будет пропорционально сумме полётного времени авиационного носителя и времени необходимого на принятие решения.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

- [1] Corporation. Air-to-Ground Precision Strike Capabilities: A Comparative Analysis. – 2022.
- [2] Кузнецов Н. Высокоточные авиаудары в Сирии. – 2019. URL: <https://vpk-news.ru/articles/52896>.
- [3] Raximov B.N. To'raev B.Z. Ugay A.P. Rayimov M.SH. Qo'shnlarni boshqarishning gibrud tizimi - prussiya modeli hamda markazlashgan tarmoq kontseptsiyasining evolyutsion rivojlanish natijalari// O'zbekiston Respublikasi Mudofaa vazirligi Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti "Professional armiya boshqaruvini rivojlanishida innovatsiyalar va raqamlashtirishning o'rni" mavzusidagi VII Xalqaro Ilmiy-Amaliy Konferensiya Maqolalar To'plami (2025-yil 11-aprel). – V 313 – 321.
- [4] Белоусов В. Революция в российском ВВС: ПАБ как ответ HIMARS. – Военное обозрение, 2023. URL: <https://topwar.ru/212345-revoljucija-v-rossijskih-vvs-pab-kak-otvet-himars.html>.
- [5] Скоморохов Р. Боль и нищета российской артиллерии. – Военное обозрение, 2022. URL: <https://topwar.ru/206569-bol-i-nischeta-rossijskoj-artillerii.html>.
- [6] Скоморохов Р. Украина против России: артиллерия. Интернет журнал: Военное обозрение. – 2023. URL: <https://topwar.ru/208210-ukraina-protiv-rossii-artillerija.html>.
- [7] Кузнецов Н. Применение корректируемых боеприпасов в Сирии // ВПК. – 2019. – URL: <https://vpk-news.ru/articles/52896>
- [8] Белоусов В. Революция в российском ВВС: ПАБ как ответ HIMARS // Военное обозрение. – 2023. – URL: <https://topwar.ru/212345-revoljucija-v-rossijskih-vvs-pab-kak-otvet-himars.html>.
- [9] Министерство обороны РФ. Ежегодный отчёт об исполнении бюджета и программе вооружения, 2023.

ZAMONAVIY RADIOELEKTRON BOSIM BERISH QURILMALARI VA ULARNING UCHUVCHISIZ UCHISH APPARATLARIGA TA'SIRI

A.X. FAYZULLAYEV, SH.O' SINDAROV

O'R MV Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti

Annotatsiya. Ushbu maqolada uchuvchisiz uchish apparatlarining (UUA) simsiz aloqa tarmoqlariga qarshi qo'llanilayotgan zamonaviy radioelektron bosim berish vositalari (REBBV)ning afzalliklari va kamchiliklari, ularning asosiy xususiyatlari, 2.4 GHz va 5.8 GHz diapazonida ishlovchi UUALarning simsiz aloqaga bog'liqligi hamda REB vositalarining ushbu diapazonlarga yo'naltirilgan tahdidlari, doimiy, reaktiv va sun'iy intellektning DRL (ing. Deep Reinforcement Learning – chuqur mustahkamlovchi o'qitish) texnologiyasi asosida ishlovchi aqlli REBBV tasnifi va ularning texnik-parametrik ilmiy nuqtai nazardan tahlil qilinadi. Ilg'or xalqaro tizimlar — CEASAR, Krasukha-4, CHL-906, Drone Dome va SPS-6160 kabi komplekslar ko'rib chiqiladi.

Kalit so'zlar: uchuvchisiz uchish apparatlari (UUA), radioelektron bosim (REB), doimiy bosim, reaktiv bosim, aqlli bosim, chuqur mustahkamlovchi o'rganish (DRL), ko'pagentli bosim, spektr monitoringi.

Abstract. This article analyzes the advantages and disadvantages of contemporary Radio-Electronic Countermeasure (REC) systems employed against Unmanned Aerial Vehicles (UAVs) within wireless communications networks. It examines their key characteristics, the dependence of UAVs operating in the 2.4 GHz and 5.8 GHz bands on wireless links, and the directed threats posed by REC systems to these bands. A technical-parametric scientific review is conducted on the classification of intelligent RECs based on constant, reactive, and Deep Reinforcement Learning (DRL) technologies. Advanced international systems—CEASAR, Krasukha-4, CHL-906, Drone Dome, and SPS-6160—are also considered.

Keywords: unmanned aerial vehicles (UAV), radio-electronic countermeasure (REC), constant jamming, reactive jamming, intelligent jamming, deep reinforcement learning (DRL), multi-agent jamming, spectrum monitoring.

Zamonaviy uchuvchisiz uchish apparatlari (UUA) turli sohalarda, jumladan, harbiy razvedka, favqulodda holatlarda qutqaruv, sanoat monitoringi va logistika operatsiyalarida keng qo'llanilmoqda. Ularning asosiy ustunliklaridan biri — simsiz aloqa tarmoqlari orqali real vaqt rejimida ma'lumot uzatish va qabul qilish imkoniyatidir. Biroq, so'nggi yillarda radioelektron bosim vositalari tomonidan ushbu aloqa kanallariga nisbatan bo'layotgan tahdidlar UUALarning ishonchliligini jiddiy xavf ostiga qo'yimoqda.

Radioelektron bosim vositalari — bu elektromagnit spektrda sun'iy shovqin yoki maqsadli signal aralashuvi orqali foydali signalni yo'q qilishga qaratilgan texnik vositalar bo'lib, ular aloqa tizimining sinxronizatsiyasini buzish, paketlarni yo'qotish yoki butun uzatish kanalini ishdan chiqarish kabi salbiy oqibatlariga olib keladi. Ayniqsa, 2.4 GHz va 5.8 GHz chastota diapazonlarida ishlovchi UUALar Wi-Fi, GPS va telemetriya signallari orqali aloqa o'rnatadi. Radioelektron bosim berish vositalari ushbu diapazonlarni aniqlab, yuqori quvvatli yoki selektiv shovqin yuborish orqali UUALarning signalini izdan chiqaradi.

Bunday sharoitda dron tomonidan yuborilayotgan axborot markaziy boshqaruv tizimi tomonidan qabul qilinmaydi, navigatsiya ishdan chiqadi, sinxron ishlash buziladi va kechikishlar ortadi. Ayniqsa, real vaqtli boshqaruv talab qilinadigan vaziyatlarda (masalan, dronlarga asoslangan havo razvedkasi yoki qidiruv-qutqaruv amaliyotlari) radioelektron bosim berish vositalarining kichik aralashuvi ham jiddiy xavf tug'dirishi mumkin. Doimiy yoki reaktiv tarzda ishlaydigan radioelektron bosim berish vositalari, uzatilayotgan signalni aniqlab, darhol bosim berish orqali UUA ni aloqa zonasidan uzib qo'yadi va missiyani muvaffaqiyatsiz holga keltiradi.

Yuqoridagi muammolarni bartaraf etish maqsadida UUAlar uchun moslashuvchan, o'z holatini real vaqtda tahlil qila oladigan va dushmanning radioelektron bosim bersih vositalariga tezda javob bera oladigan aqlli aloqa strategiyalarini ishlab chiqish zarurati ortib bormoqda [1].

Zamonaviy radioelektron bosim (REB)ning texnik va ilmiy jihatdan eng xavfli jihatlaridan biri — bu uning uzatilayotgan signalga moslasha olish qobiliyatidir. Ya'ni radioelektron bosim berish vositasi foydalanuvchi signalining chastotasi, kuchi, uzatish vaqti yoki takroriyiligiga qarab bosim strategiyasini avtomatik ravishda tanlaydi (1-rasm). Aynan shu moslashuvchanlik tufayli mobil, real vaqtli va chastotaga sezgir qurilmalar radioelektron bosimdan eng ko'p zarar ko'radigan tizimlar qatoriga kiradi.



1-rasm. UUALarga qarshi zamonaviy portativ radioelektron bosim berish vositalari

Bugungi kunda UUAlar Wi-Fi, GPS, LTE hamda maxsus radiokanallar orqali markaziy boshqaruv punktlari bilan doimiy aloqa o'rnatadi. Agar radioelektron bosim berish vositalari ushbu uzatma parametrlarini tahlil qila olsa, u holda signalga oddiy shovqin berish emas, balki targetli (nishonga yo'naltirilgan) aralashuv hosil qilinadi [2]. Bu holat chastotani sakrab o'zgartiruvchi, kognitiv kanal tanlash yoki muqobil yo'llar orqali himoyalangan UUAlar uchun ham tahdid hisoblanadi.

Radioelektron bosim berish vositalari o'zining ishlash strategiyasiga ko'ra quyidagi turlarga bo'linadi:

- **Doimiy radioelektron bosim vositalari** — bu oldindan belgilangan chastotalarda uzluksiz shovqin yuboradigan eng oddiy bosim berish vositasidir. Masalan, "JBlock-12" modeli 2.4 GHz va 5.0 GHz kabi UUAlar ishlatadigan chastotalarda ishlaydi va 10–15 W quvvat bilan 500 metrgacha bo'lgan masofada signalni butunlay yo'qotadi. Bu turdagi vositalar kichik UUALarning GPS yoki Wi-Fi kanalini uzib qo'yishda ishlatiladi.

- **Reaktiv radioelektron bosim vositalari** — bu signal faolligini doimiy kuzatib boradi va faqat faol uzatish aniqlangach bosim yuboradi. Masalan, "RJX-8" modeli signalni sezganidan so'ng atigi 0.3 soniyada faollashadi va aniq chastotaga nishonli bosim beradi. UUA tizimlarida aynan telemetriya signallarini uzatish vaqtida bunday vositalar signalga turg'unlik yetkazadi, bu esa uchish algoritmining izdan chiqishiga sabab bo'ladi.

- **Aqlli radioelektron bosim vositalari** — eng xavfli va murakkab vositalar bo'lib, ular sun'iy intellekt, xususan, DRL (ing. Deep Reinforcement Learning – chuqur mustahkamlovchi o'qitish) asosida faoliyat yuritadi. Bu turdagi REBBV foydalanuvchi signalining tuzilishi, uzatish oralig'i, kuchi va chastota ketma-ketligiga qarab o'rganadi va shunga mos bosim strategiyasini ishlab chiqadi. Masalan, "SmartBlock-AI" deb nomlanuvchi qurilma DQN (Deep Q-Network) asosida o'qitilgan bo'lib, UUAlar harakat trayektoriyasi, uzatish davri va aloqa zichligiga qarab eng nozik joyda bosim yuboradi [3].

1-jadval.

Radioelektron bosim vositalari turlari va ularning asosiy xususiyatlari

Turi	Tavsif	Model nomi	Chastota diapazoni	Quvvat	Faollik	Ishlash strategiyasi
Doimiy bosim vositalari	Oldindan belgilangan chastotalarda uzluksiz shovqin yuboradi; signalni uzlatuvchi kanalni uzib qo'yadi.	JBlock-12	2.4 GHz, 5.0 GHz	10–15 Vt	Doimiy	Uzluksiz tarmoqni qoplash orqali kanalni to'sib qo'yadi
Reaktiv bosim vositalari	Signal faolligini kuzatadi va faqat uzatish aniqlangach nishonga yo'naltirilgan bosim yuboradi.	RJX-8	Dinamik	5–10 Vt	~0.3 soniya	Signal aniqlangach bosim beradi
Aqlli (DRL asosida) bosim vositalari	Sun'iy intellekt yordamida signal tuzilishi, kuchi, chastota ketma-ketligi va uzatish vaqti bo'yicha o'rganadi va moslashadi.	SmartBlock-AI	1–6 GHz	5–20 Vt	O'rganish ga bog'liq	eng nozik joy va vaqt oralig'ida bosim yuboradi

Dron aloqa tizimlariga qarshi qo'llanilayotgan radioelektron bosim vositalarining murakkabligi va moslashuvchanligi sababli oddiy statik himoya choralari o'z samaradorligini yo'qotmoqda. Bu esa UUALar uchun o'z-o'zini o'rgatuvchi, moslanuvchan va real vaqtli bosimga qarshi himoya algoritmlarini ishlab chiqish zaruriyatini yuzaga keltiradi.

Zamonaviy radioelektron bosim berish vositalari nafaqat UUAning fizika darajasidagi radiosignaliga, balki aloqa protokollari, kodlash tizimi, sinxronizatsiya algoritmlari va retranslyatsiya jarayonlariga ham ta'sir ko'rsatadi. Bu ularning xavfini oddiy radioelektron bosimdan ko'ra ancha murakkab, ko'p qatlamli va aniqlash qiyin bo'lgan holatga olib keladi. Ayniqsa, real vaqt rejimida ishlaydigan UUALar uchun bunday aralashuvlar parvoz barqarorligi, buyruq almashinuvi va vazifani bajarish samaradorligini xavf ostiga qo'yadi.

Zamonaviy radioelektron bosim berish vositalarining eng xavfli tomoni — bu ularning signalga adaptiv javob bera olishidir. Aqlli radioelektron bosim vositalari, ayniqsa DRL asosida ishlovchi modellar, UUA uzatmalarining chastotasi, kodlash formati, va vaqtli naqshlarini tahlil qilib, unga qarshi moslashtirilgan bosim strategiyasini ishlab chiqadi. Masalan, Deep Q-Learning (DQL) asosida ishlovchi radioelektron bosim vositalari uzatilayotgan signalni o'rganib, aynan signal eng muhim bo'lgan bosqichlarda bosim yuborishni o'rganadi [4].

Endilikda radioelektron bosim vositalari oddiy chastota bo'yicha bosim berishdan tashqari, paket tuzilmasi, sinxronizatsiya fazasi va protokol darajasidagi ma'lumotlar oqimini ham tahlil qilib, strategik nuqtalarda nishonga olish orqali aloqani samarali buzmoqda. UUALar tomonidan yuborilayotgan paketlar uzunligi, signal oralig'lari va retranslyatsiya algoritmlariga moslashgan holda, radioelektron bosim vositalari foydalanuvchi signalini izdan chiqarish uchun maksimal foydali fursatni kutadi.

Shuningdek, ilg'or radioelektron bosim vositalari modellari ko'pfazali va ko'pkanalli ishlash rejimini qo'llab-quvvatlaydi. Masalan, "RFBLOCK-X20" qurilmasi bir vaqtning o'zida 0.9 GHz, 2.4 GHz va 5.8 GHz diapazonlarda faoliyat yurita oladi. Bu qurilma 20 Vt quvvatda, 360° sektoral qamrov bilan, 50 millisekund ichida reaktiv faollikka o'tadi. U o'zida DQN asosida o'qitilgan DRL modulini saqlagan bo'lib, UUA signalining ehtimollik xaritasini real vaqt rejimida tuzadi va eng nozik joyda aralashuvni amalga oshiradi.

Ushbu turdagi aqlli radioelektron bosim berish vositalarining UUALar uchun eng og'ir tahdidi — bu ular tomonidan signal uzatishning eng muhim nuqtalarini aniqlab, faqat o'sha paytlarda bosim yuborishidir. Masalan, aloqa sessiyasining boshlanishi, sinxronizatsiya fazasi yoki yuqori zichlikdagi uzatish lahzalarida amalga oshiriladigan qisqa, lekin kuchli bosim foydali signalni izdan chiqaradi. Bunday strategiya nafaqat energiyani tejaydi, balki foydalanuvchi tomonidan radioelektron bosim vositalarini aniqlash imkoniyatini keskin kamaytiradi. Shuning uchun dron aloqa tizimlarida bunday tahdidlarga qarshi kurashish uchun tezkor adaptatsiyaga ega, o'z holatidan

o'rganadigan, real vaqtli qaror qabul qiluvchi bosimga qarshi kurashish (ing. anti-jamming) algoritmlari zarurdir. Bu holatda aynan Deep Q-Learning (DQL) asosidagi yondashuv eng mos variantlardan biri hisoblanadi.

Radioelektron bosim vositalarining yana bir jiddiy tahdid manbai — bu ularning UUA aloqa tizimlarida ishlatiladigan protokollar va signal boshqaruv strukturasi uchun ichki mantig'iga aralasha olishi bilan bog'liq. Ilgari radioelektron bosim asosan signalning chastotasi yoki quvvatiga qaratilgan bo'lsa, bugungi kunda zamonaviy radioelektron bosim vositalari, ayniqsa DRL asosidagi aqlli tizimlar, signalning yuqori darajadagi (ing. higher-layer) tarkibini ham tahlil qilmoqda. Ular aloqa protokoli bo'yicha uzatmalar oqimini tahlil qilib, aynan uzatishdagi muhim qismlarni — boshqaruv paketlari, sinxronizatsiya belgilari yoki ACK paketlarini nishonga olish orqali butun uzatishni izdan chiqaradi.

Ushbu strategiya UUALar tomonidan TCP/IP, UDP yoki maxsus real vaqtli protokollar ishlatilganda yanada xavfli bo'ladi. Masalan, dron tomonidan yuborilgan ACK (ing. Acknowledgement - tanishtiruv) signaliga bosim berilsa, asosiy ma'lumotlar to'g'ri yetkazilgan bo'lsa ham, uzatuvchi tomonidan bu signal "olmadim" deb qabul qilinadi va butun sessiya uziladi.

DRL asosidagi radioelektron bosim vositalari agentlari bu kabi zaif nuqtalarni aniqlash uchun o'z tajribasiga asoslanadi. Ular turli signal oqimlarini kuzatib, ketma-ketlikdagi eng zaif bo'g'inlarni tahlil qiladi. O'rganilgan tajriba asosida bosim beruvchi qurilma "qaysi vaqtda va qaysi nuqtaga bosim yuborish eng samarali bo'lishi"ni aniqlab oladi. Bu usul doimiy shovqindan ko'ra kamroq energiya sarflaydi, lekin maksimal funksional buzilish hosil qiladi.

Bundan tashqari, DRL agenti UUA signalining spektral xaritasini (ing. spectrum map) tuzadi. Bu xarita orqali real vaqt rejimida qaysi chastotalar faol, qaysi kanallar tarmoq uzatishida eng muhim rol o'ynayotganini aniqlaydi. So'ngra dushman agenti nishonga yo'naltirilgan spektr hujumi (ing. targeted spectrum attack) strategiyasini qo'llab, aynan o'sha muhim chastotaga bosim yuboradi. Bunday yondashuv UUA signalining muhim qismini bosib, aloqani izdan chiqaradi [5].

Hozirgi paytda bunday radioelektron bosim vositalari ko'p-agentli shaklda ham faoliyat yurita boshlagan. Ya'ni, har bir radioelektron bosim vositalari o'z qarorini mustaqil qabul qilishdan ko'ra, kooperatsion tarzda (ing. multi-agent learning) ishlaydi. Bunday tizimlarda bir nechta radioelektron bosim vositalari bir-birini to'ldirib, UUALar to'dasi, ya'ni markazlashmagan kognitiv tarmoqlarga qarshi koordinatsiyalangan bosim strategiyasini amalga oshiradi. Bu esa aloqa tizimini nafaqat lokal, balki tarmoq darajasida ishdan chiqaradi.

Ushbu murakkab muhit UUALar uchun oddiy chastota almashtirish yoki tasodifiy chastota almashtirish (ing. random hopping) kabi usullarni samarasiz holga keltiradi. Natijada, bunday intellektual va ko'p qatlamli tahdidlarga qarshi DQL asosida ishlaydigan, real vaqtli, adaptiv bosimga qarshi kurash strategiyalarini ishlab chiqish zarurati dolzarb bo'lib qolmoqda[6].

Avtomatlashtirilgan UUA tarmoqlari sanoat monitoringi, infratuzilma nazorati va xavfsizlik tizimlarida keng qo'llaniladi. Masalan, sanoat zonalarida uchuvchi dronlar IoT qurilmalar bilan integratsiyada ishlaydi va ma'lumotlarni yig'adi. Agar radioelektron bosim vositalari bu aloqani buzsa, tarmoqdagi sinxronizatsiya, signal almashinuvi va xavfsizlik algoritmlari izdan chiqadi. Aynan 868 MHz, 915 MHz va 2.4 GHz chastotalarga mo'ljallangan sanoat darajasidagi radioelektron bosim vositalari UUA monitoringiga qaratilgan hujumlarni amalga oshirishda keng ishlatilmoqda.

Favqulodda vaziyatlarda ishlatiladigan dronlar esa radioelektron bosim vositalari tahdidiga ochiq qoladi. Chunki bunday holatlarda — masalan, zilzila zonalarida, yong'in yoki suv toshqini joylarida — UUALar real vaqtli video va buyruqlarni markazga uzatadi. Agar radioelektron bosim vositalari orqali bu aloqa kanali bloklansa, qutqaruv operatsiyasi yoki xavfsizlik choralari o'z vaqtida bajarilmaydi. Radioelektron bosim vositalari aynan favqulodda signal uzatuvchi ochiq spektrlarni (masalan, GPS L1, DSRC, LTE-band) nishonga oladi va tezkor javob tizimlarini izdan chiqaradi.

Bundan tashqari, portativ va ko'chma radioelektron bosim vositalari — masalan, avtomobilga o'rnatilgan yoki UUAga integratsiyalangan radioelektron bosim vositalari modullari — maxsus kuzatuv kameralari yoki signal detektorlariga sezilmasdan ishlaydi. Bunday mobil vositalar dron signalini aniqlab, doimiy harakatda bo'lgan holatda ham nishonli bosimni amalga oshiradi. Aynan shunday yondashuv UUAlar tarmog'iga qarshi jangovar zonlarda yoki strategik inshootlar yaqinida keng qo'llanmoqda.

Dunyo miqyosida ko'plab yetakchi davlatlar — AQSh, Rossiya, Xitoy, Isroil, Germaniya va Turkiya — o'z harbiy va strategik infratuzilmalari uchun yuqori samaradorlikka ega radioelektron bosim berish vositalarini faol ishlab chiqmoqda. Ayniqsa, UUA tizimlariga qarshi qaratilgan bosim qurilmalari so'nggi yillarda ancha takomillashgan. Ular keng polosali spektrni qamrab oladi, signal harakatini tahlil qiladi va DRL asosida real vaqt rejimida strategik bosim choralarini qo'llaydi. Masalan, AQShning Northrop Grumman kompaniyasi ishlab chiqqan CEASAR (Counter Communications System) kompleksi sun'iy yo'ldosh orqali uzatilayotgan harbiy aloqa signallarini to'sishga mo'ljallangan mobil radioelektron bosim vositalari hisoblanadi. Tizim 20–100 km masofada faoliyat yuritadi va DRFM (Digital Radio Frequency Memory) texnologiyasi orqali signalni tahlil qilib, unga mos bosim yaratadi [1]. CEASAR GPS, COMSAT va UUAlar uchun muhim bo'lgan kanallarni izdan chiqarishga qodir (2-rasm).



2-rasm. CEASAR (Counter Communications System) radioelektron bosim majmuasi

Rossiyaning Krasukha-4 tizimi ham UUALarning aloqa va navigatsiya tizimlariga qarshi ishlatiladi [7]. 8–18 GHz chastota diapazonini qamrab oladigan bu majmua radar va uzatish signallarini aniqlab, yo'naltirilgan elektromagnit to'lqinlar yordamida bosim hosil qiladi. Krasukha-4 real jangovar holatlarda UUA signalini bloklay, missiya boshqaruvini ishdan chiqarishga muvaffaq bo'lgan (3-rasm).



3-rasm. Krasukha-4 radioelektron bosim vositasi

Xitoy tomonidan ishlab chiqilgan CHL-906 tizimi esa mobil bazaga o'rnatiladi va 20 Vt quvvatda ishlaydi (4-rasm). Bu qurilma bir vaqtning o'zida ko'pkanalli bosim hosil qila oladi [8]: Wi-Fi, 2G/3G/4G, Bluetooth, GPS va boshqa UUAga xos aloqa protokollariga nishonli bosim yuboradi. Qurilma foydalanuvchi signalining strukturasi, uzatish usullari va chastota takrorlanishiga mos strategiyani ishlab chiqish uchun sun'iy intellektli yadro moduliga ega.



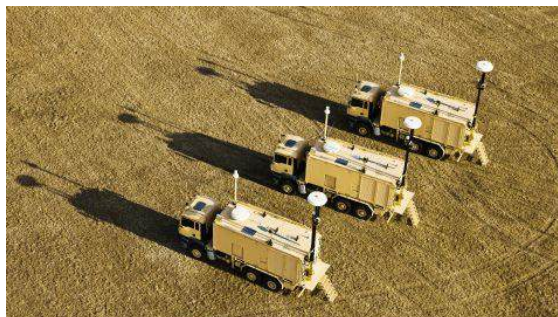
4-rasm. CHL-906 radioelektron bosim majmuasi

Isroilning Drone Dome tizimi esa UUA tahdidlariga qarshi maxsus ishlab chiqilgan (5-rasm). U radar, optik kuzatuv, signal aniqlovchi modul va radioelektron bosim vositalari bloklaridan tashkil topgan bo'lib, UUA signalini aniqlab, ayniqsa GPS va Wi-Fi kanal orqali nishonli bosim yuboradi [9]. Bunday tizimlar UUA ni yo'naltirish va missiyani avtomatik bajarmaslikka olib keladi.



5-rasm. Drone Dome radioelektron bosim vositasi

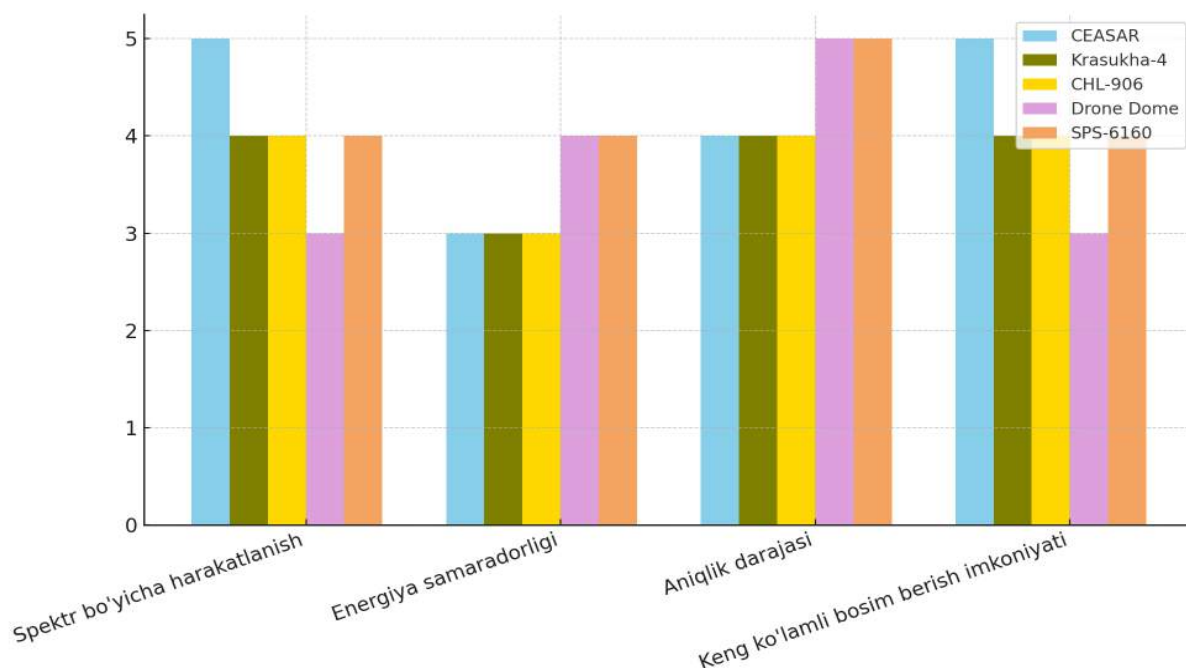
Germaniyaning Rohde & Schwarz kompaniyasiga tegishli SPS-6160 tizimi esa selektiv radioelektron bosim vositalari sifatida ishlab chiqilgan (6-rasm). U faqat kerakli chastota kanaliga nishonli bosim yuboradi. SPS-6160 UUA tarmoqlaridagi signal zichligini, uzatish strukturasi va chastota profilini tahlil qilib, sun'iy intellekt asosida "optimal bosim zonasi"ni aniqlaydi [10].



6-rasm. SPS-6160 radioelektron bosim vositasi

Ushbu qurilmalarning aksariyati DRL yoki DQL asosida boshqariladi, ya'ni ular signal faolligini kuzatadi, spektr xaritasini shakllantiradi va foydalanuvchi signalining xatti-harakatiga mos ravishda bosim strategiyasini doimiy ravishda yangilaydi. Aynan shuning uchun ular kognitiv radiotizimlar va dronlarga asoslangan moslashuvchan aloqa tizimlari uchun eng murakkab tahdid manbaiga aylanmoqda.

1-diagrammada zamonaviy REBBVlarning asosiy xususiyatlarining qiyosiy tahlili keltirilgan.



1-diagramma. Zamonaviy REBBV asosiy xususiyatlarining qiyosiy-tahliliy diagrammasi.

Ushbu diagrammadan quyidagicha xulosalarga kelishimiz mumkin:

- Spektr bo'yicha harakatlanish erkinligi: CEASAR eng yuqori darajada keng polosali tezkor spektr adaptatsiyasini amalga oshiradi, SPS-6160, Krasukha-4 va CHL-906 ham kuchli spektr qamrovini ta'minlaydi, Drone Dome esa biroz cheklangan.

- Energiya samaradorligi: Drone Dome va SPS-6160 energiyani tejaydi, portativ va uzoq muddatli operatsiyalarga mos keladi; CEASAR, Krasukha-4 va CHL-906 esa o'rtacha darajada samarali ishlaydi.

- Aniqlik darajasi: SPS-6160 va Drone Dome yuqori selektivlik bilan maqsadga yo'naltirilgan bosim strategiyalarini qo'llaydi, CEASAR, Krasukha-4 va CHL-906 biroz kamroq aniqlikni ta'minlaydi.

- Ko'lamli jamming imkoniyati: CEASAR va SPS-6160 keng hududlarni yuqori quvvat bilan yengil qamrab oladi; Krasukha-4 va CHL-906 balansli keng qamrovni taklif etadi; Drone Dome esa kichik maydonlarda samaraliroq.

Yuqorida keltirilgan REBBVlarning asosiy xususiyatlari 2-jadvalda keltirilgan.

2-jadval.

Zamonaviy REBBVlarning asosiy xususiyatlari qiyosiy tahlili

REBBV nomi	Spektr (GHz)	Quvvat (W)	Aniqlik	Qamrov (km)	Asosiy afzalliklari	Asosiy kamchiliklari
CEASAR	0,02–6, moslashuvchan	25000	protokol darajasiga nishonli aralashuv	20–100	real vaqtli adaptiv strategiya	juda yuqori energiya sarfi, murakkab logistika va katta og'irlik

REBBV nomi	Spektr (GHz)	Quvvat (W)	Aniqlik	Qamrov (km)	Asosiy afzalliklari	Asosiy kamchiliklari
Krasukha-4	8–18, ko'pkanalli	100000	radar signallarini aniqlik bilan yo'naltirilgan to'liqlar yordamida bloklash	100–150	yuqori protokol darajasi qo'llab-quvvatlanishi	og'ir mobil platforma, joylashtirish va texnik xizmat ko'rsatish murakkabligi
CHL-906	1,2–6, ko'pkanalli	20–50	telemetriya va boshqaruv paketlarini aniqlik bilan nishonga olish	3–5	portativ konteyner tizimi, ko'pkanalli bosim	past quvvat va nisbatan qisqa qamrov masofasi
Drone Dome	0,4–6, radio+optik	2–20	360° qamrovda 0,1° aniqlik bilan dron trayektoriyasini aniqlash	1–3	signalni yuqori aniqlik va tezkorlikda aniqlash	cheklangan bosim berish masofasi va tor spektr qamrovi
SPS-6160	0,9–18, moslashuvchan	20–40	protokol va yuqori qatlam paketlarini ham nishonga olish	10–20	uzoq muddat davomida bosim berish	katta radiusli maydonlarni qamrab olishda biroz cheklangan

O'tkazilgan tahlillar shuni ko'rsatmoqdaki, zamonaviy radioelektron bosim berish vositalari aloqa tizimlariga tahdid soluvchi omil sifatida nafaqat signalning energetik parametrlariga, balki uzatish protokoli, kodlash strukturalari, vaqt domenidagi xatti-harakatlar va sinxronizatsiya jarayonlariga ham chuqur aralasha oladigan ko'p qatlamli tizimlar sifatida shakllangan. Ayniqsa chuqur kuchaytirilgan o'rganish algoritmlariga asoslangan aqlli radioelektron bosim vositalari jamg'irish strategiyalarini real vaqt rejimida foydalanuvchi signalining statistik xatti-harakatlariga moslashtira olish qobiliyatiga ega.

Xalqaro amaliyotda keng qo'llanilayotgan CEASAR, Krasukha-4, Drone Dome, CHL-906, SPS-6160 kabi ilg'or tizimlarning texnik-analitik tahlili shuni ko'rsatdiki, radioelektron bosim vositalari harbiy kommunikatsiya, sanoat IoT, favqulodda aloqa tizimlari va strategik xavfsizlik infratuzilmalarida uzatilayotgan raqamli signal oqimlarini to'xtatish, yo'naltirish yoki soxtalashtirishga qaratilgan murakkab algoritmik yondashuvlarga ega. Ayniqsa protokol qatlamiga nishonlangan, selektiv va reaktiv jamming usullarining evolyutsiyasi passiv va statik himoya choralarining samarasizligiga olib kelmoqda.

Shuningdek, radioelektron bosim vositalarining spektral monitoring, signal sinxronizatsiyasi va retranslyatsiya davrlarini tahdidga aylantirish imkoniyati kognitiv aloqa tizimlarini yangi arxitekturaviy yondashuvlar asosida loyihalashni taqozo etmoqda. Kognitiv qurilmalar endilikda nafaqat real vaqtli signal muhitini tahlil qila olishi, balki o'z harakat strategiyasini moslashtirib, DRL yoki boshqa o'rganuvchi agentlar asosida adaptiv uzatish protokollarini shakllantira olishi talab qilinmoqda.

Shu bois, keyingi bo'limda aynan spektrdan foydalanishni moslashtirish, shovqinbardosh uzatish usullari va DRL asosidagi kognitiv boshqaruvga ega signal uzatuvchi va qabul qiluvchi qurilmalar tahlil qilinadi. Bu yondashuv radioelektron bosim vositalari tahdidlariga nisbatan zamonaviy, aqlli va ilg'or qarshi chora-tadbirlar ishlab chiqishga yo'l ochadi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

- [1] Department of Defense (USA). Counter Communications System (CCS) Overview, 2020. – [Electronic resource]. – URL: <https://www.afspc.af.mil/News/Article-Display/Article/CCS>
- [2] Шестаков В.А., Коршунов Н.А. Электронная борьба: современные средства и технологии. – М.: Радиотехника, 2020. – 276 с.

- [3] Liu, Z., Wang, H., Li, Y. Deep reinforcement learning-based intelligent jamming against cognitive radio networks. // IEEE Access, 2020. – Vol. 8. – pp. 25471–25482.
- [4] Xu, H., Shi, Y., Zhang, X. Anti-jamming communication using spectrum waterfall prediction and Deep Q Networks. // IEEE Transactions on Communications, 2021. – Vol. 69(10). – pp. 6503–6516.
- [5] Wang, Z., Liu, W. Design of adaptive jamming systems using DRL for UAV defense. // Defence Technology, Elsevier, 2022. – Vol. 18(3). – pp. 589–601.
- [6] International Telecommunication Union. Handbook on Spectrum Monitoring, Geneva: ITU, 2019. – 432 p.
- [7] Красуха-4: мобильный комплекс радиозлектронной борьбы. – [Электронный ресурс]. – URL: <https://mil.ru/krasykha4>
- [8] China Electronics Technology Group Corporation (CETC). CHL-906 Multi-band Jamming System, Technical Report, 2022.
- [9] Advanced Defense Systems Ltd. Drone Dome Anti-UAV System. – Technical brochure, 2021. – URL: <https://www.rafael.co.il/worlds/drone-dome/>
- [10] Rohde & Schwarz GmbH & Co. SPS-6160 Selective Jamming Platform – Technical Data Sheet, 2023. – URL: <https://www.rohde-schwarz.com/products/sps6160>

MINA MAYDONLARINI BOSHQARISH USULLARINI TAKOMILLASHTIRISH YO'LLARI

dotsent M.S. TOSHTEMIROV

O'R MV Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti

Annotatsiya. Ushbu maqolada mina maydonlarini boshqarishning usullarini takomillashtirish yo'llari, vositalari, radio boshqaruv yo'nalishining rivojlanishi, KRAB-IM, UMP, VPKM qurilmalari va NVU-P "Oxota" rusumli kontaktsiz portlatuvchi qurilmasi, ularning taktik texnik tavsiflari, kamchiliklari va zamonoviy jang talablaridan kelib chiqib muammolari hamda mina maydonlarini boshqarish usullarini takomillashtirish yo'llari to'g'risida ma'lumotlar keltirilgan.

Kalit so'zlari: muhandislik to'siqlari, mina, mina maydonlari, boshqarish qurilmalari, portlatishni boshqaruv radioyo'nalishlari, radio portlatgichlar, radio orqali boshqariladigan fugas, radio orqali boshqariladigan minalar, PD-420, PD-430 va PD-530 qurilmasi, NVU-P "Oxota" rusumli kontaktsiz portlatuvchi qurilmasi.

Аннотация. В данной статье рассматриваются вопросы развития способов управления минных полей, средств, радиотехнических устройств управляемого взрыва, устройств КРАБ-ИМ, УМП, ВПКМ и неконтактного взрывного устройства НВУ-П "Охота", их тактико-технические характеристики, недостатки и проблемы в применении с учетом требований современного боя, а также даны информации по перспективам развития управления минных полей.

Ключевые слова: инженерные заграждения, мина, минные поля, управляемые устройства, радиоуправляемый взрыв, радиовзрыватели, радиоуправляемый фугас, радиоуправляемая мины, изделия ПД-420, ПД-430 и ПД-530, неконтактное взрывательное устройство НВУ-П "Охота".

Abstract. In this article information relevant to ways of modernizing of controlling of mine fields, development of radio controlling lines, machines of KRAB-IM, UMP, VPKM and nonconnected explosion machine named NVU-P "Oxota" and their details, lacks and problems from origin of modern fighting demands also ways of modernizing of controlling of mine fields are given.

Key words: engineering obstacles, mine, mine fields, control machine, radio controlled explosion, radio controlled explosion lines, radio frequency fuse, radio-controlled land mine, radio-controlled mine, products PD-420, PD-430 and PD-530, radio demolition machine, nonconnected explosion machine named NVU-P "Oxota".

So'nggi yillarda nafaqat dunyodagi geosiyosiy va harbiy-strategik vaziyatda, balki zamonaviy urushlarning mohiyati va salohiyati, qurolli to'qnashuvlarda vositalardan foydalanishning shakllari va usullari haqidagi qarashlarda ham tub o'zgarishlar yuz berdi.

Nizolar va urushlarning (1-rasm) shakli hamda xarakteri tubdan o'zgarib, an'anaviy yondashuvlarning amaliy ahamiyatlik darajasi pasayib bormoqda, harbiy harakatlarni amalga oshirishni yangi tur va vositalari vujudga kelmoqda.

XXI-asrda bo'lib o'tayotgan harbiy mojarolar (Rossiya-Ukraina, Isroil-Falastin, Livan va Eron)da olib borilayotgan maxsus harbiy operatsiyalarning tajribalari kelajakdagi qurolli to'qnashuvlarni olib borishning asosiy yo'nalishlarini belgilab berdi. Bu asosiy yo'nalishlarni ijodiy anglash, uni tahlil qilish barcha harbiy mutaxassislarning aktual vazifalariga aylanmoqda.

Rossiya-Ukraina, Isroil-Falastin, Livan va Eron) davlatlarida hozirgi kunda masofadan boshqariladigan piyodaga qarshi boshqariladigan mina maydonlari dan keng tarzda foydalanib kelmoqda.



1-rasm. Dunyoda sodir bo'layotgan qurolli to'qnashuvlar

Harbiy to'qnashuv va urushlar har doim qurol-aslaha va jangovar texnikalar vositasida bir tomonning ikkinchi tomonga nisbatan kuch ishlatishi bilan davom etgan.

Bugun barcha jang turlarida muhandislik ta'minoti vazifalarining o'rni juda muhimligini qurolli to'qnashuvlar tajribalari isbotlab berdi, shunday ekan bu vazifalarni muvaffaqiyatli bajarmasdan dushman ustidan g'alaba qozonishning imkoni yo'q. Muhandislik to'siqlari dushmanni tirik kuchlari va texnikalariga qiyinchiliklar tug'dirish, ularning harakatlarini cheklash va muhandislik o'q-dorilari yordamida yakson qilish maqsadida qo'llaniladi.

Bugungi harbiy to'qnashuvlar va urushlarning tahlili natijasi shuni ko'rsatmoqdaki (2-rasm), jangovar harakatlar masshtabi va dinamikasining o'sishida minali janglar va mina maydonlarini boshqarish, hamda ularni qisqa va xohlagan vaqt ichida belgilangan masofadan turib ularga talofat yetkazish vazifalarining o'rni muhim ekanligini talab etmoqda.



2-rasm. Bugungi harbiy to'qnashuvlar mina maydonlarini boshqarish

Bugungi kunda harbiy to'qnashuvlarda va urushlarda mina maydonlarining o'rni va ularni boshqarish juda katta ahamiyatni kasb etadi, chunki dushman qo'shinlarining harakatlarini cheklash, qiyinlashtirish va ularga muhandislik o'q-dorlari bilan xohlagan vaqtda talofat yetkazish bilan bog'liq vazifalar yuklanadi. Bundan tashqari, ular mudofaa polosasi va pozitsiyalarini o'z vaqtida to'liq mustahkamlash, ekstremal sharoit va vaziyatlarda joy hududlarni va har xil ob'ektlarni mina maydonlari bilan yopish, yuqori harakatchan hujumga qarshi jangovar operatsiyalarni o'tkazish va ehtiyoj tug'ilganda mina maydonlaridan bo'linmalarni to'g'ri o'tkazish, ularning harakatchanligini oshirish, hamda dushmanni kerakli vaqtda va joyda harakatini qiyinlashtirish, minali jang bilan yakson qilish imkoniyatlarini amalga oshiradi.

Mina maydonlarini boshqarish qurilmalarining paydo bo'lish tarixi

Minalar maydonini boshqarish bilan birga yangi minalar namunalari ham barpo etildi. Mudofaa jangi paytida mina maydonlari va ularni boshqarish katta ahamiyatga ega, bo'linmalar qarshi hujumga uchragan taqdirda ham, o'rnatilgan mina maydonlari birinchi bo'lib qo'shinlarning harakatlariga to'sqinlik qiladi, garchi ularning chegaralari ma'lum bo'lsa-da, bu o'tish joylarini tartibga solishni osonlashtiradi. Jang vaqtida dushmanga qarshi turadigan va kerak bo'lsa, o'z qo'shinlarimizning o'tishiga xalaqit bermaydigan mina maydonlarini tashkil qilish maqsadida boshqariladigan mina maydonlari yaratildi.

Boshqariladigan mina maydonlari vazifasiga ko'ra tanklarga qarshi va piyodalarga qarshi turlariga bo'linadi.

Boshqariladigan mina maydonlarining asosiy elementlari mina yoki PM zaryadlari, taqsimlovchi tarmoq, boshqaruv liniyasi va boshqaruv pulti hisoblanadi.

Dastlab, 2-jahon urushining boshlarida, parchalanadigan minalar (va boshqa turdagi minalar ham) yo'qligi sababli, sovet sapyorlari mudofaa liniyalarini o'rnatish uchun artilleriya snaryadlaridan minalar yasashdi. Simlar orqali boshqariladigan va simli arqon bilan o'rnatiladigan piyodalarga qarshi va tanklarga qarshi minalarni ishlab chiqarishdi.

Urush boshlarida uy sharoitida ishlab chiqarilgan turli xil qo'lbola mina maydonlarini boshqarish vositalari qo'llanilgan, masalan: bular eng oddiy o'q tutashtirgichlar yoki elektrlashtirilgan tarmoqlar yordamida simli tortqilarni tutashtirish bilan bog'liq bo'lgan.

Shuni ta'kidlash kerakki, turli xil rasmiy qo'llanmalar va risolalarda boshqaruv qurilmalari turli xil nomlarga ega bo'lishi mumkin. Shunday qilib, 1943 yildagi "Minalashtirish va minalardan tozalash vositalari to'g'risidagi qo'llanmada" va 1943 yil nashrining "Boshqariladigan minalar maydoni" kitobida "KRAB" va "Krab-IM" qurilmalari alohida tasvirlangan (3-rasm).



3-rasm. KRAB-IM qurilmasi

Minalar maydonlarini boshqarish uchun yuqoridagi barcha qurilmalardan foydalanish oson va ular bilan ishlash uchun maxsus ko'nikmalar talab qilinmaydi. O'sha davr uchun ular juda mukammal edilar, ayniqsa boshqa mamlakatlarda (ittifoqchilarda) bunday tizimlar mavjud emasligini hisobga olsak! Biroq urush paytida muhandislik bo'linmalari tomonidan tez-tez oldindan jihozlangan mudofaa liniyalarida piyodalarga qarshi boshqariladigan minalar yaratildi.

Rostov-Donni himoya qilish paytida uning sovet sapyorlari tomonidan boshqariladigan minalar maydoni (UMP) tashkil etilganligini va u yerda uy sharoitida sakrovchi OZMlarning turli xil versiyalari ishlab chiqilganligini yozadi. Shuningdek, Kursk ostonasidagi janglar davomida boshqariladigan minalar maydonlaridan foydalanilgan. Ko'pincha tankga qarshi UMP qurilmasi yuqori natija bergan va FOG fugasli ognyomyotlari bilan birgalikda qo'llanilgan [1.2].

1944 yilda "Krab-IM" qurilmasi paydo bo'ldi. "Krab-IM" to'plami piyodalarga qarshi min maydonlarida (aylanma) tanlab portlatishni sim orqali boshqarish uchun mo'ljallangan. Portlatiladigan guruhlar soni 11 tadan oshmasligi va guruhdagi minalar soni liniya qarshiligiga

qarab hisoblash yo'li bilan aniqlangan. Qurilma boshqaruv pulti va kalitdan iborat bo'lib, kalit asosiy simlar bilan minalar maydoniga o'rnatilganda ulanadi.

UMP-3 mina maydonlarini boshqarish to'plami V.K. Bryuxov boshchiligidagi konstruktorlar tomonidan ishlab chiqilgan va o'z navbatida bir qancha boshqa muhandislik o'q-dorilarini ham yaratgan.

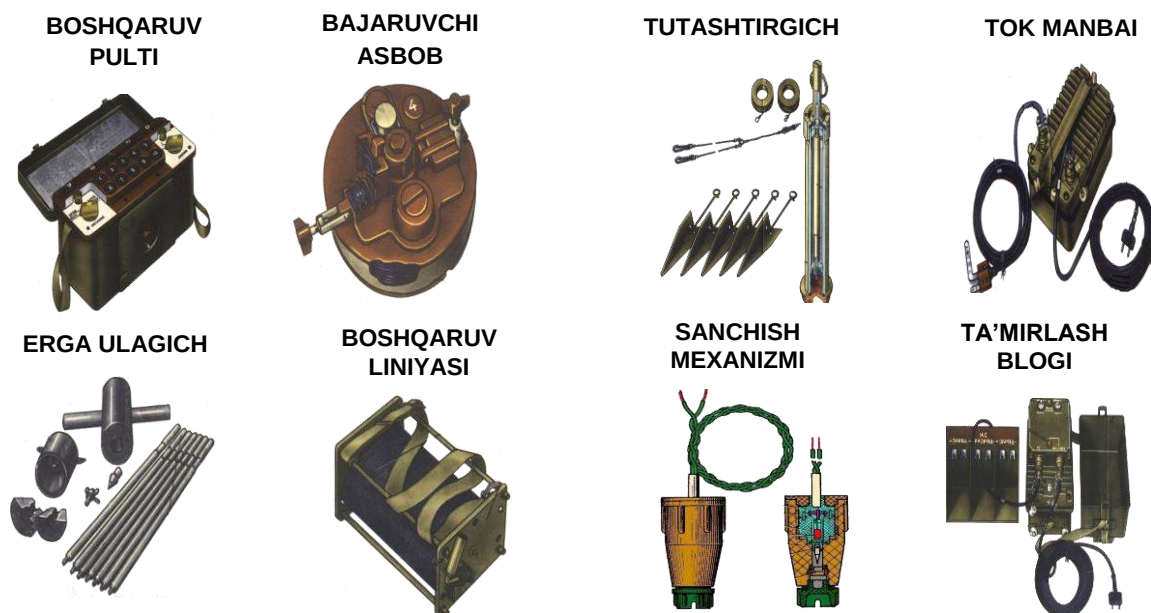
UMP-3 komplekti piyodalarga qarshi mina maydonlarini (jangovar va xavfsiz holatda) o'tkazgich orqali boshqarish va minalarni tanlab portlatish uchun mo'ljallangan. Jangovar holati ikkita variantdan iborat bo'lishi mumkin:

1) faqat operatorning xohishiga binoan portlatish (bajaruvchi priborlar

MVE-72 portlatgichisiz yoki tutashtirgichsiz o'rnatiladi);

2) tanlab portlash (portlash operator xohishiga ko'ra amalga oshiriladi va avtomatik ravishda - dushman nishon sensoriga ta'sir qilganda).

UMP-3 to'plamida minlarni portlatish uchun maxsus tortganda harakatga keluvchi tutashtirgichlar yoki MVE-72 portlatgichlari (4-rasm) bilan jihozlangan uziluvchi nishon sensori o'rnatiladi. Bunday holatlarda minalar nishon sensori uzilganda yoki tortilganda ishga tushirish, shu bilan birga boshqaruv pultidan yuborilgan impuls yordamida ham bo'lishi mumkin. To'plam to'rtta simli tarmoqdan iborat minalar maydonini o'rnatishga imkon beradi.



4-rasm. UMP-3 to'plami

UMP-3 va Krab-IM to'plamlari hajmi jihatidan juda katta (ular tashish uchun bir nechta qutilarni talab qiladi) va ular muhandislik bo'linmalariga yetkazib beriladi. Ular bilan ishlash yuqori darajadagi ko'nikmalarni talab qiladi va ular hamma joyda ham qo'llanilavermaydi [2].

UMP-3, VKPM-1 va VKPM-2 mina maydonlarini boshqarish to'plamlari Afg'onistonda samarali qo'llanildi. Ularni harbiy ob'ektlarni, kichik garnizonlarni va blok postlarni himoya qilishda qo'lladilar, ular yordamida pistirmalarni tashkil qildilar (bunday holatda mina maydonlarini boshqarish ham operator, ham radio portlatish vositasi sifatida ham qo'llanilardi), VKPM-1 va VKPM-2 to'plamlari ayniqsa qulay bo'lgan.

Afg'onistonda boshqariladigan tanklarga qarshi minalar to'plamlari ishlatilmadi chunki, oppozitsiya kuchlarida shunchaki sezilarli darajada tanklar va boshqa zirhli texnikalar yo'q edi va ular mavjud bo'lgan joyda tanklarga qarshi boshqariladigan mina maydonlarini yaratish uchun uni keng ishlatish xavfi yo'q edi.

Sovet konstruktorlari tomonidan ishlab chiqilgan UMP-3, VKPM-1 va VKPM-2 boshqariladigan mina maydonlari to'plamlari Shimoliy Kavkazda terroristik tashkilotlariga qarshi o'tkazilganda muhim ob'ektlarni yopish va qo'shinlar joylashgan joylarini qo'riqlashda faol qo'llanilgan [4].

Xalqaro cheklovlar natijasida aholi punktlari yaqinida minalarni boshqarilmaydigan varianti taqiqlangan va bu yerda minalar boshqarish juda samarali bo'lgan.

VKPM qurilmalari. Tashib yuriladigan piyodalarga qarshi minalar VKPM-1 va VKPM-2 to'plami (5-rasm) minali-portlovchi to'siqlarni o'rnatish uchun mo'ljallangan bo'lib, qo'shinlar pozitsiyalarini va harbiy ob'ektlarni qo'riqlashda himoyalash (yopish) maqsadida qo'llaniladi. VKPM-1 va VKPM-2 (5-rasm), to'plamlari faqat o'z ichiga olgan minalar turidan farq qiladi. VKPM-1 to'plamida OZM-72 minalari bo'lsa, VKPM-2 to'plamida esa MON-50 minalari qo'llaniladi. Bundan tashqari, har bir to'plam 12 dona signal minalarini o'z ichiga oladi.



5-rasm. UMP-3 to'plami

To'plam ikki xil variantda tayyorlanadi: 1) Jangovar; 2) Amaliy.

Jangovar to'plamda jangovar oskolkali va signalli minalar, jangovar detonatorlar, kapsyul detonatorlar va sanchuvchi mexanizmlar saqlanadi.

Amaliy to'plamlar qo'shinnlarni jangovar tayyorgarlik jarayonida o'qitish uchun qo'llaniladi va signal beruvchi minalar ham o'zida saqlanadi.

Tanklarga qarshi mina maydonlarini boshqarish uchun UMPN-68, UMP va UMP-2 to'plamlari ishlab chiqildi.

Boshqariladigan tanklarga qarshi minalar boshqariladigan piyodalarga qarshi minalardan farq qiladi, chunki ulardagi portlatgichlar jangovar holatga va orqaga qaytish imkoniyatlariga ega bo'lib, bu juda muhim xususiyatni kasb etadi. Tanklarga qarshi minalar maydonlarining barcha to'plamlarida xalqalangan liniyalar mavjud bo'lib, boshqaruv liniyalaridan birida shikastlangan holatlar bo'lganda ishonchli boshqaruvni ta'minlaydi.

1968 yilda UMPN-68 to'plami qurollanishga qabul qilindi.

Ushbu to'plamda kontaktsiz harakatga keladigan MVN-62 portlatgichlari qo'llaniladi. Portlatgichning tuzilishi oddiy. Uning tarkibiga magnit datchigi, detonatsiyalovchi-saqlovchi qurilma, portlatgichni portlatishni ta'minlovchi va uni xavfsiz jangovar holatiga o'tkazadigan o'tkazuvchi moslama joylashtirilgan.

Portlatgichni boshqarish, boshqaruv liniyasi orqali unga quvvatni yetkazib beradi va portlatgichning jangovar kondensatori o'qlanadi, qachonki dushmanning zirhli mashinasi kelib urilganda portlatgichning ishlab ketishini ta'minlaydi [3].

1970 yilda UMP to'plamining o'rniga UMP-2 to'plami ishlab chiqarildi, bu UMP dan deyarli kam farq qiladi.

UMP-2 to'plami UMP portlatgichlari bilan jihozlanadi, odatda TM-57 yoki TM-62 minalarida o'rnatiladi, lekin maxsus adapter bilan o'rnatiladi. Boshqaruv pultidan impuls yuborilganda jangovar holatga keltiradi, portlatgich kondensatori zaryadlanadi va u jangovar holatga o'tiladi. Turli xil mashqlar o'tkazish vaqtida barcha boshqariladigan minalar maydonlarining qiziqarli xususiyati paydo bo'ldi.

Minalashtirilgan maydonni boshqarish liniyasi zanjirli zirhli texnikalarning izlariga juda "muvaffaqiyatli" o'ralgan edi va bundan so'ng avval yotqizilgan uzilgan boshqaruv liniyalarni bartaraf etishdan ko'ra yangi boshqaruv liniyasini yotqizish osonroq edi [4].

1-jadval

UMP portlatgichlari solishtirma tahlili

	UMP-68	UMP	UMP-2	UMP-3	Krab-IM
To'plamning og'irligi (minasiz), kg	490	490	440	370	40
Mina maydoniga o'rnatiladigan to'plamning o'lchami, m: front bo'ylab uzunligi; chuqurligi	100-30 gacha	100-30 gacha	100 yoki 300 40 gacha	Qo'llaniladigan minani turiga bog'liq	Qo'llaniladigan minani turiga bog'liq
Boshqarish masofasi, km	1 gacha	1 gacha	0,8 gacha	0,1 gacha	1 gacha
Jangovar ishlash vaqti, oylar	3	3	3	3	6
Qo'llaniladigan minalar turlari	TM-62	TM-57 yoki TM-62	TM-57 yoki TM-62	OZM-72, MON-50, MON-100, MON-200	MON-100, MON-200, OZM UVK bilan, OZM-160
Qo'llaniladigan portlatgichlar	MVN-62	UMP	UMP	MVE-72 maxsus tutashtirgichlar	-

Afg'onistondagi urush paytida (6-rasm) Sovet armiyasining ob'ektlarini himoya qilish uchun boshqariladigan minalar keng ishlatilgan. Ular shuningdek razvedka-signalizatsiya vositalari (RSV) va radioliniyalari bilan birgalikda ishlatilgan. Shunday qilib, isyonchilarning intensiv harakati amalga oshirilgan Vardak viloyatidagi karvon marshrutlaridan birida piyodalarga qarshi minalarni boshqarish vositasi bilan birgalikda RSV datchiklarining ikkita liniyasi o'rnatildi (300 metr oldida 40 mina). Karvondagi odamlar va hayvonlar sonini aniqlash uchun bitta RSV datchigi o'rnatildi, keyingi datchik esa, birinchisidan 400 m masofada yo'lga o'rnatildi va u karvon boshini minalar maydoni tomon harakatlanganligi to'g'risida signal beradi.



6-rasm. Razvedka-signalizatsiya vositalari (RSV) ishlatilishi

II-jaxon urushidan keyingi davrlarda boshqariladigan mina maydonlari, radio liniyalar yordamida masofadan turib boshqarish imkoniyatiga ega bo'ldi. Qo'llanmalarda shuni ko'rsatadiki,

boshqariladigan mina maydonlarini boshqarish uchun RL-62, PD-420, PD-430 va PD-530 radio yo'nalishlari ishlatiladi, ammo boshqa radio yo'nalishlari ham ushbu maqsadlar uchun ishlatilishi mumkin.

Piyodalarga qarshi minalar talofatidan har yili minglab tinch aholi qurbon bo'ladi. Ko'p davlatlar bu qurollarga aniqrog'i o'q-dorilarga ta'qiq qilish bo'yicha o'z chiqishlarini qildi, 1980 yilda 53 davlat Jeneva kelishuvi va 1999 yili 133 ta davlat Ottava kelishuviga "Piyodalarga qarshi minalarni qo'llash ta'qiqi" imzo chekishdilar va a'zo bo'ldi. (AQSh va Rossiya bu ro'yxatga kirmaydi).

Amerikaliklar tomonidan tinch aholining xavf xatarini qisqartirish bo'yicha aqlli minalar tashkil qilish bo'yicha qaror qabul qilindi va bu minalarni ta'qiqlamaslik uchun yana bitta sabab bo'ldi. 2016 yilda minalarni ishlatish dasturi yo'lga qo'yildi.

Bu loyiha ya'ni aqlli mina ustida nafaqat Amerika balkim, Rossiya konstruktorlari ham PTM-5 aqlli minasini yaratganligi va u qurollangan odamlar bilan tinch axolini bir biridan farqlay olish imkoniyatiga ega. Bu ikki gegomon davlatlar bugun piyodalarga qarshi minalarni boshqarish orqali qo'llash mumkinligini, ya'ni tinch aholiga zarar yetkazmasligini isbotlab berdi.

Shunday ekan, eski tizimlarni modernizatsiya qilish bilan bir qatorda yangi mina maydonlarini boshqarish qurilmalari ham ishlab chiqildi.

S.S. Kovalenko boshchiligidagi "Tadqiqot instituti" Aksionarlik jamiyati tashkilotida UMP-4 piyodalarga qarshi boshqariladigan mina maydoni to'plamini ishlab chiqdi. Har bir UMP-4 to'plamiga quyidagilar kiradi: bitta boshqaruv pulti, 4 ta bajaruvchi blogi ikkita 10 metrli liniyasi bilan sanchish mexanizmini ulash uchun, ikkita seysmik va optik nishon datchiklari, 400 m uzunlikdagi ikkita boshqaruv liniyasi va bajaruvchi blokka qismlarni ulash uchun ikki tanovcha va tarmog'i bilan, boshqaruv liniyalari uchun ikkita katushka, PD-440 radioliniyasiga ulash uchun bitta kabel, o'nta sanchish mexanizmlaridir.

Boshqariladigan minalar maydoni to'plami to'rt qatorli minalashtirish maydonini (50 m uzunlikdagi to'rtta zona) o'rnatish uchun foydalaniladi. Maydondagi har bir liniya seysmik yoki optik sensorli nishoniga ulangan bo'lib, uning qamrov zonasi OZM-72 minasining ta'sir qilish radiusiga muvofiq lashtirilgan. Minalarni portlatish operatorning o'zi bergan komandasi bo'yicha (boshqaruv pultida yoki radioliniyani qo'llash orqali) va avtonom tarzda amalga oshirilishi mumkin. To'plamda to'rtta ish rejimi mavjud: jangovar boshqariladigan, jangovar avtonom va jangovar radio boshqariladigan. UMP-4 to'plamini minalarni sanchish mexanizmlariga ulanmasdan foydalanish mumkin. Bunday hollarda, bu esa radio signalizatsiya tizimi bo'ladi [2].

2-JADVAL

UMP-4 to'plamining tavsifi

Bir qatorli to'siqlarni o'rnatish masofasi, m	200
Minalar maydonini boshqarish uzoqligi, m	400
Radio liniyani qo'llanganda minalar maydonini boshqarish uzoqligi, km	2
O'rnatish vaqti, soat	1
Uzluksiz ishlash vaqti, kun	30
Ta'minot manbalari	R7 elementlari (sovet davridagi nomlanishi 373 elementi) yoki MRL- 3460 elementi
Gabarit o'lchamlari:	
Boshqaruv pulti, mm	190x150x135
Bajaruvchi blogi, mm	160x135x55

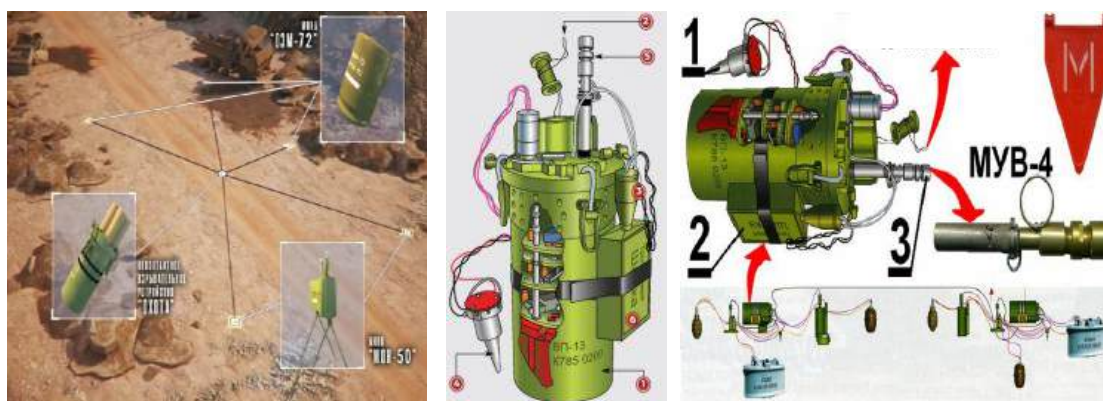
Mina maydonlarini boshqarish usullari bizga ma'lumki - bu radio boshqaruv va simli boshqaruvlarni o'z ichiga qamrab oladi, mina maydonlarini boshqarish usullarini takomillashtirish yo'llarini bugungi kunda dunyo mamlakatlari armiyalarining ko'pchiligi potlatishning radio

boshqaruvi va robot texnika to'plamini (RTT) harbiy maqsadlarda qo'shnlarda joriy qilishni amalga oshirmoqda.

Xususan AQSh, Rossiya, Germaniya va bir qancha ilg'or davlatlar armiyalarida radio boshqaruv va robotlashtirish tizimi yaxshi yo'lga qo'yilgan.

NVU-P "Oxota" rusumli kontaktsiz portlatuvchi qurilmasi. Yangi turli xildagi minalar sinflanishining paydo bo'lishi ularni zararsizlantirish metodikasini ishlab chiqishga to'g'ri keldi. Mana shularni rivojlanishi davri natijasida NVU-P "Oxota" rusumli kontaktsiz portlatuvchi qurilmasi paydo bo'ldi (7-rasm).

Bu qurilma piyodalarga qarshi minalarni boshqarish uchun mo'ljallangan bo'lib, dushman sapyorlariga minalarni zararsizlantirishga imkoniyat qoldirmaydi.



7-rasm. NVU-P "Oxota" rusumli kontaktsiz portlatuvchi qurilmasi

NVU-P qurilmasi o'tgan asrning 70-yillarida piyodalarga qarshi mina-portlovchi to'siqlarning samaradorligini oshirish maqsadida ishlab chiqilgan bo'lib, Afg'onistondagi urushda eng ko'p qo'llanilgan.

Asosiy kamchiliklari, o'sha vaqtdagi mavjud barcha piyodalarga qarshi minalarni maxsus vositalar yordamida ularni zararsizlantirish va yakson qilishda aniqlash extimoli yuqori bo'lgan.

Shu tarzda mina maydonlarining samaradorligini oshirish uchun yangi qurol talab qilindi, u dushman sapyori yoki jangchisi yaqinlashishi bilan oldindan sezadi va aniqlash hamda zararsizlantirish bo'yicha barcha urinishlarini barbad qiladi.

Tinimsiz izlanishlar natijasida yangi loyiha bo'yicha perespektiv to'plamning umumiy ko'rinishi tuzildi.

To'plam tarkibida "Oxota" nomini olgan qurilma, belgilangan talablar asosida har xil turdagi piyodalarga qarshi minalarda qo'llanilishi mumkin. Birinchi navbatda sakrovchi OZM-72 minalarida, bundan tashqari MON-50 va POMZ-2 va boshqa minalarda qo'llaniladi.

"Oxota" qurilmasi shartli ravishda bajaruvchi taqsimlovchi qurilma, seysmik nishon datchigi va batareya bloklaridan iborat qismlarga bo'linadi. Bundan tashqari u bir qancha elektr sanchish qurilmalari, sim g'altagi bilan, ta'minlash elementlari va boshqalar bilan butlanadi. Hamda to'plam tarkibiga beshtagacha piyodalarga qarshi minalar modeli qo'shiladi.

NVU-P "Oxota" rusumli kontaktsiz portlatuvchi qurilmasi belgilangan o'lchamdagi chuqurlikka o'rnatiladi va unga SV-20P seysmik datchigi yerga ko'yilgan holda o'rnatiladi. OZM-72 minalari boshqaruv qurilmasida 2 metrdan 15 metrgacha bo'lgan masofada o'rnatiladi. Bu qurilma insonning qadamidan eshitadi va 15 metr masofadan ularni ovozidan farqlaydi.

NVU-P "Oxota" va alohida minalar joylashuvi bir qancha faktorlarga bog'liq. Mavjud ma'lumotlar ko'ra NVU-P seysmik datchigi 150 metr masofada kelayotgan odamni aniqlash qobiliyatiga ega. 90 metr masofada nishonni topadi. Nishonning 15-20 metr masofaga yaqinlashishi bilan qurilma minalarni portlatishga komanda beradi. Shu manoda minalar ana shu radius hisobida joylashtirilishi kerakki, bunda to'liq o'sha hudud yopilishi lozim.

“Oxota” to‘plami kontaktsiz portlatuvchi qurilmasi bilan zararsizlantirilmaydigan hisoblanadi.

So‘nggi yillarda nafaqat dunyodagi geosiyosiy va harbiy-strategik vaziyatda, balki zamonaviy urushlarning mohiyati va salohiyati, qurolli to‘qnashuvlarda vositalardan foydalanishning shakllari va usullari haqidagi qarashlarda ham tub o‘zgarishlar yuz berdi. O‘zbekiston Respublikasi o‘z Qurolli Kuchlarini qayta tashkil etish jarayonini tubdan yangiladi desak adashmaymiz, ularning istiqbolli ko‘rinishi, tarkibi va tuzilishi aniqlandi, qo‘shinlarning bo‘linmalari yangi zamonaviy qurol-aslaha va vositalari bilan ta‘minlandi.

Yuqoridagilardan kelib chiqib xulosa o‘rnida shuni ta’kidlab o‘tish joizki boshqariladigan minalar zamonaviy janglarda o‘z ahamiyatini yo‘qotgani yo‘q, ayniqsa, ular turli xalqaro shartnomalarda cheklovlar mavjud bo‘lishiga qaramay, zamonaviy harbiy to‘qnashuvlarni o‘tkazishda o‘zlarining samaradorligini namoyish etmoqda va mina maydonlaridan o‘z bo‘linmalarining tez va oson o‘tkazilishini ta‘minlab bermoqda.

Dunyo armiyalari safida mina maydonlarini boshqarish usullarini takomillashtirish yo‘llarining harbiy sohada rivojlanayotganligining tahlili shuni ko‘rsatmoqdaki, O‘zbekiston Respublikasi Qurolli Kuchlarining intellektual va ishlab chiqarish imkoniyatlarining oshishi natijasida, milliy armiyamizda zamonaviy janglarni moxirlik bilan boshqarish, kuzatish va lozim bo‘lganda aynan o‘sha nishonni yakson qilish imkoniyatlari mavjud bo‘lgan universal radio yo‘nalishli boshqaruv portlatish qurilmalarining yangi avlodini ishlab chiqish zarur.

Yangi zamonaviy ishlab chiqilayotgan mina maydonlarini boshqarish qurilmalarining ijobiy xususiyatlari shundaki:

mina maydonlarini boshqarish qurilmasi masofasining yuqoriligi va har bir minalarni tanlash va portlatish imkoniyatlari ko‘pligi;

mina maydonlarini boshqarish bajaruvchi priborining soni ko‘payganligi va u o‘z o‘rnida jangovar tayyorgarlik mashg‘ulotlarini o‘tkazishda, turli xil o‘yinlar va o‘quvlarni o‘tkazish jarayonida portlatishlarni imitatsiyalash (o‘xshatish) imkoniyatlari ko‘payganligi yaqqol misol bo‘ladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

[1] D.T. Artikbayev, Radioboshqaruvli portlatish qurilmalarining rivojlanish istiqbollari va ular bilan kurashish usullari / D.T. Artikbayev // Harbiy ta’lim va fanda innovatsiyalar. – 2019. –№ 4 (6) S. 47-51.

[2] Б.Р.Исхаков, Радиоэлектронное подавление радиоуправляемых взрывных устройств / B.R. Isxakov, L.O. Yudin, K.S. Fomichev // Электроника НТБ. – 2009. – № 2.S. 47-53.

[3] М.Ф. Карогодин, Возимые комплекты противопехотных мин ВКПМ-1 и ВКПМ-2: руководства по материалной части / М.Ф. Карогодин. – М.: Воен. изд., 2011. - 32 с.

[4] Muhandislik o‘q-dorilar III-qismi qўllanma. 98-130 bet.

[5] Istochnik kontenta: <https://naukatehnika.com/obzor-minnyix-polej-htmlnaukatehnika.com>

[6] Po materialam saytov: <http://saper.etel.ru/http://army.lv/http://rusarmy.com/http://popmech.ru/>

РОЛЬ ЛОЖНЫХ УЗЛОВ СВЯЗИ В СОВРЕМЕННЫХ БОЕВЫХ ОПЕРАЦИЯХ**З.А. ТАДЖИБАЕВ***Военной институт информационно-коммуникационных технологий и связи МО РУ*

Аннотация. Рассмотрены современные проблемы обеспечения разведывательной защищенности и живучести узлов связи пунктов управления, представлены основанные на комплексном системном подходе, с учетом широкого спектра факторов, способы их решения. Даны рекомендации по направлениям исследований и практических мероприятий, проводимых в войсках связи, обеспечивающих повышение устойчивости системы управления войсками, силами и оружием при ведении военных действий.

Рассматривается значение ложных узлов связи пунктов управления в современных военных и кибероперациях. Анализируются методы создания и использования ложных узлов связи для дезинформации противника, повышения безопасности собственных сетей и снижения риска перехвата данных. Подчеркивается важность интеграции ложных узлов связи в комплексные стратегии информационной безопасности.

Ключевые слова: Разведывательная защищенность системы связи, живучесть системы связи, узел связи, транспортная сеть связи, ложные узлы связи, дезинформация, кибербезопасность, военные операции, информационные технологии, сетевые технологии.

Аннотация. Мақолада бошқарув пунктлари алоқа узеллари разведхимоёланганлиги ва яшовчанлигини таъминлаш бўйича муаммолар, уларни келтириб чиқадиган омиллар ва бартараф этиш чора-тадбирлари кўриб чиқилган. Қўшинларда олиб борилаётган тадқиқотлар ва амалий тадбирларнинг жанговар харакатлар даврида қўшинларни, кучларни ва қуролларни бошқариш тизимининг барқарорлигини таъминлаш бўйича таклифлар берилган. Замонавий ҳарбий характларда ва кибероперацияларда ёлгон бошқарув пунктлари алоқа узелларининг тутган ўрни кўриб чиқилган.

Душманни чалғитиш, ўзининг алоқа тармоқлари ҳавфсизлигини таъминлаш ва душман томонидан алоқа тизим ва тармоқларига бўлган таъсирни камайтириш бўйича ёлгон алоқа узелларини тузиш ва ишлатиш усуллари таҳлил қилинган. Ёлгон алоқа узелларининг ахборот ҳавфсизлигини таъминлаш бўйича комплекс чора-тадбирларнинг муҳимлиги кўрсатиб ўтилган.

Калит сўзлар: Алоқа тизимининг разведхимоёланганлиги ва яшовчанлиги, алоқа узеллари, алоқанинг транспорт тармоғи, ёлгон алоқа узеллари, дезинформация, киберҳавфсизлик, ҳарбий операциялар, информацион технологиялар, тармоқ технологиялари.

Практически все современные концепции ведения военных операций вооруженными силами ведущих государств мира ориентированы на первоочередное достижение превосходства над противником в управлении войсками, силами и оружием. Достижение превосходства в управлении реализуется в ходе информационного противоборства путем комплексного воздействия на систему управления противника и защиты своей системы управления.

Информационное противоборство в современных войнах будет сопровождаться постоянным ведением всех видов разведки, нацеленных на вскрытие системы управления противника с последующим оказанием на нее деструктивного воздействия. Конечной целью является срыв управления войсками (силами) противника. Устойчивость функционирования системы управления войсками, силами и оружием объединения во многом определяется живучестью системы связи.

Основными объектами поражения в операциях являются пункты управления (ПУ) и элементы системы связи (узлы, центры и линии связи)[1].

Оперативно-тактические требования, предъявляемые к системе связи объединения в современных операциях коррелируются между собой, выдвигая в качестве главных - требования к разведывательной защищенности системы связи и устойчивости ее функционирования.

Функционирование системы связи прежде всего не должно позволить противнику вскрыть систему управления войсками, сделать доступными его разведке характеристики информационных направлений и передаваемую в них информацию. В возможных военных конфликтах XXI века противоборствующими сторонами разведка будет вестись постоянно, комплексно всеми видами и средствами. Наибольшую значимость при решении задачи вскрытия структуры системы связи имеют радио- и радиотехническая разведки [1].

Скорость функционирования автоматизированных комплексов радиотехнической разведки постоянно повышается. Сегодня на выявление радиоэлектронного средства и его место определение уходят считанные секунды. Вся система управления объединения может быть вскрыта в течение нескольких часов. Как правило, эти мероприятия проводятся за сутки до начала военных действий. При реализации сетцентрического управления по разведанным объектам управления будет нанесено поражение наиболее эффективными средствами и наиболее оптимальным способом. В условиях комплексного воздействия противника элементы системы связи должны обладать объектовой живучестью, развертываемые сети - структурной избыточностью, возможностью маневра сетевыми ресурсами, обеспечивающими непрерывную и своевременную передачу необходимых потоков информации.

На основе проведенного анализа применения системы и войск связи в различных мероприятиях оперативной подготовки, проводимых в войсках связи, можно констатировать, что системы связи объединений весьма благоприятствуют всем видам разведки [4]:

узлы связи пунктов управления (ПУ) громоздки и обладают характерными признаками размещения;

радиоцентры легко вскрываемы из-за большой мощности излучения передатчиков и больших антенных полей;

радиорелейные линии демаскируют расположение ПУ управления высокоподнятыми крупногабаритными, легко распознаваемыми антеннами и непрерывным радиоизлучением;

потоки информации неравномерно распределяются по информационным направлениям и во времени, что позволяет выявлять направления и объекты сосредоточения основных усилий группировок войск в операции.

Данные проблемные вопросы должны разрешаться на основе системного подхода, с учетом широкого спектра факторов, определяющих разведывательную защищенность и живучесть системы связи.

К решению задачи обеспечения высокой разведывательной защищенности и живучести системы связи в операциях необходимо подходить комплексно, поэтапно, начиная с обоснования тактико-технических характеристик средств и комплексов связи, проводя мероприятия заблаговременной подготовки связи объединения к операциям, определяя формы и способы применения системы и войск связи при организации связи

в ходе непосредственной подготовки к боевым действиям, обеспечивая опережающее развертывание системы связи и ее перестроение в ходе ведения операции, реализуя устойчивое организационное, оперативно-техническое и технологическое управление, создавая необходимые резервы сил и средств связи, грамотно и рационально применяя их для восстановления элементов системы связи.

Начнем рассмотрение вопросов обеспечения живучести системы связи объединения с узлов связи ПУ.

Узел связи является неотъемлемой составной частью, технической основой пункта управления любого звена управления. Узел связи пункта управления объединения является

основным элементом системы связи объединения при выполнении им оперативных задач в ходе ведения военных действий в различных физико-географических условиях.

Основное предназначение узла связи заключается в обеспечении совместной информационной работы оперативного состава, качественной передачи информации по управлению войсками путем предоставления различных видов связи, функционирования автоматизированных систем управления войсками, силами и оружием, поддержании направлений связи с узлами связи пунктов управления всех элементов оперативного построения. Оперативно-тактические требования к узлам связи объединений определяются прежде всего оперативными условиями ведения современной операции, принятыми способами и технологиями управления войсками, силами и оружием.

Узел связи ПУ должен обладать такой разведывательной защищенностью, чтобы продолжительность распознавания узла связи средствами разведки противника была больше, чем время нахождения узла связи в одном районе. Поэтому важное значение для обеспечения разведывательной защищенности и живучести узла связи имеет его мобильность [2].

В условиях возрастания возможностей разведки и средств поражения противника одной из наиболее эффективных мер, позволяющих существенно снизить вероятность нанесения удара противником по ПУ, является своевременное совершение маневра.

Прогнозируемый уровень развития разведки противника обуславливает частоту перемещения ПУ оперативного, стратегического звеньев управления не менее двух, а в определенных условиях, и более раз в сутки.

Согласно требованиям руководящих документов продолжительность развертывания узла связи не должна превышать двух часов.

Анализ различных способов перемещения ПУ оперативного звена управления позволяет сделать вывод, что период времени 2-3 часа на совершение перемещения оперативного состава является предельной. На качественном уровне узлы связи полевых подвижных ПУ должны сохранить свой функционал до конца операции.

На узле связи должны отсутствовать критически важные объекты, поражение которых выводит из строя весь узел связи. Функционал узла связи не должен существенно снижаться при выходе из строя до 20 % средств связи.

Особое значение имеет грамотное сочетание способов скрытия и имитации. При имитации системы связи основное внимание должно уделяться созданию ложных узлов и объектов связи.

Ложные узлы связи - представляют собой специально созданные элементы сетевой инфраструктуры, которые внешне и функционально имитируют реальные узлы - серверы, маршрутизаторы, коммутаторы, точки доступа, рабочие радиостанции или передающие устройства. Однако их главная цель - не выполнение реальных рабочих функций, а создание ложных полноценных компонентов системы связи для определённых тактических и стратегических целей.

В военных операциях ложные узлы применяются для сокрытия истинного расположения критически важных командных пунктов и центров управления. В кибербезопасности они используются как часть концепции honeypot - систем, предназначенных для мониторинга и анализа атак [10].

Основные характеристики ложных узлов:

1. Эмуляция поведения реальных узлов. Ложные узлы способны воспроизводить сетевой трафик, протоколы и ответы, характерные для реальных устройств. Например, они могут обрабатывать запросы на подключение, поддерживать открытые порты, отвечать на ping, имитировать приложения и сервисы (например, веб-серверы или базы данных), организации связи на радиосетях и радионаправлениях, проведение маскирующего радиообмена.

2. Прозрачность и незаметность для противника. Для эффективности ложные узлы связи должны быть максимально приближены к реальным узлам связи пунктов управления с точки зрения сетевой топологии, конфигурации и поведения. Это достигается путём тщательной настройки и постоянного мониторинга, чтобы противник не смог быстро распознать их как фальшивые.

3. Использование технологий виртуализации и контейнеризации. Часто ложные узлы связи реализуются с резерва связи находящихся в штате подразделения связи, с помощью виртуальных машин, контейнеров (например, Docker), специализированных honeypot-систем или симуляторов сетевых устройств.

Основные задачи ложных узлов:

- отвлечение внимания и ресурсов противника на несуществующие цели;
- сбор разведывательной информации о попытках атаки;
- создание «ловушек» для выявления и анализа вредоносных действий;
- усиление общей устойчивости сети и предотвращение утечки информации.

Примеры использования ложных узлов в современных операциях

В современном военном деле ложные узлы связи приобретают особое значение благодаря необходимости сокрытия информации и создания комплексных систем обороны и дезинформации.

Одной из ключевых задач является защита критически важных объектов от обнаружения и уничтожения противником. Ложные узлы позволяют создавать виртуальные командные центры, имитирующие активность настоящих пунктов управления.

Например, сеть ложных радиостанций, серверов или терминалов связи может транслировать поддельные координаты и данные, сбивая с толку разведывательные средства врага - спутники, радиолокационные станции и электронные разведывательные комплексы (SIGINT). Это снижает вероятность успешного удара по реальным объектам и дает стратегическое преимущество.

В рамках РЭБ ложные узлы используются для создания помех и поддельных сигналов, которые маскируют реальные коммуникационные линии. Например, в ходе операций по подавлению связи противника ложные узлы могут принимать и ретранслировать радиосигналы, создавая иллюзию присутствия крупных сил или важных объектов в местах, где их нет.

Ложные узлы способствуют проведению психологических операций, направленных на сбивание с толку противника, создание хаоса в его разведывательных данных и принятие неверных решений. Демонстрация активности ложных коммуникационных узлов может заставить врага распределить свои ресурсы неправильно.

Во время Второй мировой войны широко применялись ложные объекты и радиопередатчики для отвлечения внимания противника (например, операции по маскировке Дюнкерка). Сегодня технологии эволюционировали, и ложные узлы связи стали цифровыми и сетевыми, но принципы остались те же. В цифровом пространстве ложные узлы стали неотъемлемой частью систем активной защиты от кибератак, в первую очередь в виде honeypot и honeynet - систем «ловушек» для хакеров [9].

Honeypot системы - это ложные узлы, которые имитируют уязвимые серверы, базы данных, сети или приложения, специально предназначенные для введения противника в заблуждения. Цель - выявить попытки вторжения, понять методы и инструменты атакующего, а также отсрочить или предотвратить атаку на реальные ресурсы. Honeypot может быть «низкоуровневым» (эмулирующим только определённые порты и сервисы) или «высокоуровневым» (функционирующим как полноценный сервер).

Honeynet - сети из ложных узлов. Более сложный вариант - это целая сеть ложных узлов, объединённых между собой и взаимодействующих с атакующими. Honeynet позволяет

получать более глубокую информацию о поведении злоумышленников и тактиках, используемых для продвижения внутри сети.

Преимущества использования ложных узлов связи

1. Повышение безопасности и устойчивости к воздействию атакам противника.

Ложные узлы связи создают отвлекающий манёвр. Вместо того, чтобы напрямую атаковать реальные узлы связи ПУ, противник вынужден сначала взаимодействовать с ложными целями, что значительно снижает риск успешного уничтожения.

Путём распределения ресурсов противника на ложные цели сокращается возможность проведения координированных и мощных атак на настоящие узлы. Это позволяет защитным системам иметь больше времени для обнаружения и реагирования на угрозы.

Ложные узлы могут выполнять роль буфера, снижая нагрузку на реальные компоненты сети в условиях атаки и предотвращая перегрузку или отказ критически важных сервисов.

Использование ложных узлов затрудняет противником определение настоящей архитектуры узлов связи пунктов управления, что усложняет планирование и проведение успешных атак.

2. Снижение вероятности уничтожения противником настоящего узла связи пункта управления.

Ложные узлы специально созданы так, чтобы сбивать с толку противника - имитируя реальный узел связи или реальные устройства и сервисы, что вызывает у противника ложное ощущение успеха, что может привести к ошибкам и раскрытию его методов.

Для того чтобы выявить и уничтожить ложные узлы, противник вынужден тратить больше времени и вычислительных ресурсов, что снижает общую эффективность его действий.

Информация, получаемая с ложных узлов, может использоваться для анализа целей и намерений противника, выявления новых векторов атак и уязвимостей, которые требуют дополнительной защиты.

Данные, собранные в результате взаимодействия с ложными узлами, позволяют создавать более эффективные механизмы защиты, обновлять политики безопасности и корректировать конфигурации телекоммуникационных систем.

Ограничения:

для строительства ложных узлов связи пунктов управления оперативного и стратегического назначения требуется значительный ресурс сил и средств связи;

могут усложнять управление сетью;

при некачественном внедрении становятся уязвимыми для выявления противником.



Рис.-1. Использование тепловых ловушек типа КПФ-1-180

Ложные узлы связи также должны организовать свою работы как настоящий узел связи пункта управления.

При этом обязательном порядке производится маскировка узла связи и их элементов, охрана и оборона УС, организация работы радиосредств, режимы работы, ведение маскированного радиообмена.

Актуальной проблемой остается разработка штатных маскирующих средств для антенно-мачтовых устройств, высота подъема которых до 30 м. Снижение эффективности поражения боеприпасами с инфракрасной головкой самонаведения осуществляется за счет применения более контрастных тепловых целей (тепловых ловушек) на удалении 50-100 м от электропитающих станций и другой техники связи и оборудования над ними теплоотражающих экранов (асбестовое полотно, брезент, стеклоткань, специальные теплоткани, подручные материалы с присыпкой грунтом) [2].

Для снижения эффективности радиолокационного наведения средств поражения из подручных материалов создаются ложные радиолокационные цели (аппаратные, центры).



Рис.-2. Ложные радиолокационные цели

Устойчивость работы узла связи напрямую зависит от непрерывного электроснабжения его элементов. Большинство перерывов связи на полевых узлах связи связано с нарушением электроснабжения. Система электроснабжения элементов узла связи не должна иметь явно выраженные разведывательные признаки. Она должна обеспечивать поддержание высокой мобильности и живучести узла связи с вероятностью бесперебойного электропитания за время выполнения задачи связи. Данные требования обеспечиваются трехкратным резервированием и раздельным питанием от первичных источников электропитания средств жизнеобеспечения и средств связи и автоматизации.

В значительной степени эффективность проведения мероприятий по обеспечению разведывательной защищенности и живучести пункта управления зависит от маскировки и оборудования в инженерном отношении района разворачивания. При решении задачи маскировки узлов связи ПУ комплексно используются традиционные способы: скрытие, имитация, демонстративные действия и дезинформация [2].



Рис.-3. Маскировка узлов и станции

Инженерное оборудование пункта управления осуществляется совместно инженерными подразделениями, подразделениями обеспечения и связи.

Следует особо подчеркнуть, что проведение мероприятий маскировки и инженерного оборудования требует больших трудозатрат и, самое главное, ресурса времени, что входит в противоречие с требованием обеспечения высокой мобильности ПУ.

Организация применения полевых узлов связи должна быть направлена на определение районов, благоприятных для развертывания пунктов управления, обеспечение возможности совершения узловыми подразделениями своевременного маневра в данные районы и упреждающего скрытого развертывания узлов связи пунктов управления, накопление материальных и технических средств для проведения мероприятий всестороннего обеспечения. Транспортная сеть связи создает технологическую основу для устойчивого функционирования направлений связи.

Основным принципом построения транспортной сети связи остается комплексное использование опорной сети связи и линий прямой связи. Необходимо отметить, что транспортная сеть связи строится на основе сочетания стационарного и полевого компонента. При этом основу транспортной сети связи объединения составляет стационарная сеть связи, которая обеспечивает необходимую пропускную способность системы связи.

В мирное время при организации связи в операции основное внимание должно уделяться разработке различных вариантов резервирования стационарной сети связи, в том числе и региональных сетей операторов связи, полевыми подразделениями связи, а также наращиванию транспортной сети связи в возможных районах ведения военных действий, не оборудованных в отношении связи.

Стационарные узлы связи пунктов управления необходимо проектировать с учетом не менее 30 % резерва телекоммуникационных возможностей для решения задач связи в операции. В итоге структура создаваемой транспортной сети связи должна быть максимально инвариантна к характеру ведения операции.

Важное значение для решения данной задачи имеет взаимодействие с доверенным оператором связи.

В настоящее время значительную долю возможностей региональной стационарной сети связи объединения определяет арендованный у операторов связи телекоммуникационный ресурс, который представлен в виде наложенной сети связи со значительной долей аренды VPN-соединений. Существующая телекоммуникационная инфраструктура региональной сети распределена неравномерно, в основном сосредоточена в районах мегаполисов. Низкая разветвленность и устойчивость сетей операторов усложняет их использование в условиях ведения военных действий и чрезвычайных ситуаций. Следует отметить не соответствующий современным требованиям уровень стойкости сетевых узлов операторов связи к воздействию различных видов оружия.

Серьезную обеспокоенность относительно обеспечения информационной безопасности вызывает наличие на сетях связи оборудования иностранного производства, а также снижение доли присутствия в бизнесе государственных структур, участие в телекоммуникационном секторе иностранного капитала. Не способствуют решению проблем и ограниченные возможности операторов и войск связи по восстановлению вышедших из строя сетей связи общего пользования (ССОП). Стоит заострить внимание на том факте, что многие из вышеназванных проблем использования телекоммуникационного ресурса операторов ССОП вызваны несовершенством законодательной базы в сфере регулирования отношений в телекоммуникационном секторе экономики при введении в стране военного положения, либо в отдельных районах - чрезвычайного положения [3].

В ходе ведения военных действий деградация возможностей системы управления неизбежна, но она должна быть контролируемой.

В боевых условиях при постоянном деструктивном воздействии противника бывает более важным не обеспечить качественное обслуживание большинства пользователей, а обеспечить функционирование ограниченного количества приоритетных направлений связи. В полевой транспортной сети связи необходимо реализовать телекоммуникационные протоколы, предполагающие возможность адаптивного снижения пропускной способности в условиях сложной помеховой обстановки. Увеличение пропускной способности системы связи в современных условиях должно достигаться не возрастанием полосы пропускания отдельных линий связи, а путем создания распределенной множественной, многосвязной с эффективной системой технологического управления процессами обмена данными, построенной на базе автономных коммутационных модулей адаптивной сети.

Серьезные задачи требуется решить и для адаптации существующих радиорелейных линий к новым условиям связи.

Выше уже отмечалось, что они сверх всякой меры демаскируют расположение наших группировок войск и пунктов управления, в основном из-за режима непрерывного радиоизлучения и высокоподнятых антенн радиорелейных станций.

Одним из возможных решений может быть уменьшение высоты подъема антенно-фидерных устройств примерно вдвое при сокращении интервала связи до 20-30 км и применение специализированных маскировочных средств. Наряду с этим в радиорелейных линиях целесообразно применить режим сеансовой связи. Для той же цели следовало бы проработать и возможность применения пассивных и активных воздушных ретрансляторов. Актуальным является разработка наземных автономных, необслуживаемых ретрансляционных пунктов контейнерного исполнения. Для решения задачи сопряжения полевых сетей связи с сетями связи операторов связи необходимо разработать единый военный технический стандарт на подключение к сети военной связи. В составе полевой транспортной сети связи должны разворачиваться постоянно функционирующие, скрытые, резервные и ложные опорные узлы связи.

На основе проведенного моделирования применения системы связи объединения в операции целесообразным в составе транспортной сети связи разворачивать от количества постоянно функционирующих узлов связи 20-25 % - скрытых, 20-30 ложных и 10-20 % - резервных опорных узлов.

Взросшие требования по мобильности пунктов управления указывают на то, что основным родом связи будет оставаться радиосвязь, но способы ее осуществления должны учитывать целый ряд противоречивых требований, главным из которых является постоянный рост потребности в пропускной способности каналов связи, повышения их качества, защищенности и скрытности. Радиосвязь на основе применения технологий «программно определяемого радио» должна обрести качественно новые характеристики, обеспечивающие скрытую и помехоустойчивую передачу больших объемов информации на большие расстояния. Данные характеристики могут быть достигнуты путем применения сложных кодовых конструкций радиосигналов, построения сетевой структуры на основе автоматической ретрансляции сигналов и динамической маршрутизации передаваемых сообщений.

Примеры использования ложных узлов связи показывают, что это универсальный инструмент для защиты информации и создания стратегических преимуществ как в физических, так и в цифровых пространствах. Их эффективное внедрение требует комплексного подхода, учитывающего специфику конкретной операции, угроз и инфраструктуры.

Несмотря на значительные преимущества, использование ложных узлов связано с техническими и организационными сложностями. Требуется грамотное планирование,

выделение достаточных ресурсов и высококвалифицированный персонал для эффективного внедрения.

Использование ложных узлов связи не только укрепляет защиту сетевой инфраструктуры пунктов управления, но и превращает процесс атаки противника в источник ценной информации, что повышает общую безопасность, снижает риски и улучшает адаптивность системы связи основных узлов связи ПУ к новым угрозам. Это делает ложные узлы связи важнейшим компонентом современных комплексных стратегий информационной безопасности.

Заключение. Ложные узлы связи играют важную роль в обеспечении безопасности основных узлов связи пунктов управления в современных операциях. Их использование повышает эффективность защиты информации и позволяет создание многоуровневые системы безопасности основных узлов связи, способные адаптироваться к разным угрозам со стороны противника на пункты управления.

Несмотря на существующие ограничения численного состава подразделений связи, дальнейшее развитие технологий ложных узлов связи и их интеграция в современном бою станет одним из ключевых направлений в совершенствование современных сетевых и военных операций.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

- [1] Таджикибаев З.А., Мадрахимов У.А. Живучесть узлов связи под воздействием физических разрушений. Научно-технический журнал ВИИКТис. 1(21) 2025. 81-88 с.
- [2] Таджикибаев З.А., Мадрахимов У.А. Защита элементов узла связи от атак беспилотных летательных аппаратов (дронов). Научно-технический журнал ВИИКТис. 1(17) 2025. 224-231 с.
- [3] Таджикибаев З.А. Современные угрозы кибератаки на узлы связи. Научно-технический журнал ВИИКТис. 12.02.2025. 71-76 с.
- [4] Киргизова Н.П. Анализ применения войск связи в современных военных конфликтах // Социогуманитарные коммуникации. 2023 г. № 4/6- с. 64-70.
- [5] Таджикибаев З.А. Пути совершенствования разведывательной защищенности и живучести системы связи в операциях // INNOVATION TECHNOSYSTEMS. Научно-технический журнал ВИИКТис № 1(9) 23 г, с.91-96.
- [6] Лобанов В.Д. Высокоточное оружие: применение и перспективы развития // Вестник Восточно-Казахстанского государственного Университета им. Д. Серикбаева. № 2. 2016 г. С 149-155.
- [7] Иванов С.В., Петров А.М. Информационная безопасность в современных сетях. — М.: Техносфера, 2020.
- [8] Smith J., Brown L. Cyber Deception: Techniques and Applications. — New York: Springer, 2019.
- [9] Волков Д.Н. Методы защиты информации в военных сетях. — СПб.: Питер, 2021.
- [10]. Кузнецов В.В. Honeypot технологии и их использование в кибербезопасности. // Журнал «Информационные технологии», 2022, №3, с. 45–53.
- [11] Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. — Wiley, 2020.

FAYL TIZIMI BOSHQARUVINI TASHKIL ETISH VA ELEKTRON MA'LUMOTLAR XAVFSIZLIGINI TA'MINLASH MUAMMOLARI

**PhD., profesor B.K. YUSUPOV,
PhD, dotsent B.O. MUHAMADOV**

O'R MV Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti

Annotatsiya. Ushbu maqolada fayl tizimi boshqaruvini tashkil etish va elektron ma'lumotlar xavfsizligini ta'minlash muammolari tahlil qilingan. Bundan tashqari zamonaviy fayl tizimi va uning turlari, fayl tizimi tomonidan hal qilingan muammolar, xotira qurilmasidagi bo'sh joyni boshqarish hamda fayl tizimi himoyasini ta'minlash masalalri tadqiqi amalga oshirilgan.

Kalit so'zlar: fayl, katalog, tizim, boshqaruv, elektron ma'lumot, xavfsizlik, Windows, Linux, macOS, HarmonyOS, FAT, NTFS, ext, HFS, APFS, EROFS, HMDFS, ruqsat, himoya, samaradorlik, guruhlash, ikki darajali, iyerarxik, bo'sh blok, taqsimot, ikkilik bitli, bo'sh joy.

Аннотация. В данной статье проанализированы проблемы организации управления файловой системой и обеспечения безопасности электронных данных. Кроме того, проведено исследование современных файловых систем и их видов, проблем, решаемых файловой системой, управления свободным пространством на запоминающем устройстве, а также обеспечения защиты файловой системы.

Ключевые слова: Файл, каталог, система, управление, электронные данные, безопасность, Windows, Linux, macOS, HarmonyOS, FAT, NTFS, ext, HFS, APFS, EROFS, HMDFS, доступ, защита, эффективность, группировка, двухуровневый, иерархический, свободный блок, распределение, двоичный бит, свободное пространство.

Abstract. This article analyzes the issues related to the organization of file system management and the protection of electronic data. Furthermore, the study explores modern file systems and their types, the problems addressed by file systems, the management of free space on storage devices, and mechanisms for ensuring file system security.

Keywords: File, directory, system, management, electronic data, security, Windows, Linux, macOS, HarmonyOS, FAT, NTFS, ext, HFS, APFS, EROFS, HMDFS, permission, protection, efficiency, grouping, two-level, hierarchical, free block, allocation, binary bit, free space.

XXI asrga kelib raqamli axborotlar hajmi va ularning oqimi tobora ortib borib, fayl tizimining samarali boshqaruvi va elektron ma'lumotlar xavfsizligini ta'minlash masalalari muhim vazifalardan biriga aylanib bormoqda. Har qanday axborot tizimining asosiy tarkibiy qismi sifatida fayl tizimi ma'lumotlarni saqlash, ularga tezkor kirish, tartiblash va himoyalash funksiyalarini o'z ichiga oladi. Zamonaviy operatsion tizimlar, turli formatdagi fayl tizimlari va xavfsizlik mexanizmlari orqali foydalanuvchi ma'lumotlarining yaxlitligi, konfidensialligi hamda foydalanuvchanligini ta'minlashi lozim.

Axborotlashtirish vositalarida yaratiladigan fayllarni, ma'lumotlarni kompyuter tizimida saqlash va boshqarish uchun ishlatiladigan vosita sifatida ta'riflashimiz mumkin. Axborot tizimlaridagi ma'lumotlar to'liq raqamli formatda saqlanadi. Ushbu ma'lumotlarni raqamli formatda saqlash uchun biz bugingi kunda har xil fayl turlaridan foydalanamiz.

Fayl tizimlari har qanday operatsion tizimning muhim qismi hisoblanadi. Ular qattiq disklar, qattiq jisimli xotira qurilmasi (SSD) va USB flesh xotira qurilmalari kabi saqlash qurilmalarida ma'lumotlarni strukturalangan saqlash, tashkil qilish va boshqarishni ta'minlaydi. Asosan, fayl tizimi operatsion tizim va ma'lumotlarni saqlash uchun ishlatiladigan fizik uskunalar o'rtasida bog'lovchi bo'g'in vazifasini bajaradi. U foydalanuvchilar va dasturlarga fayllarni tartibli va samarali tarzda yaratish, o'qish, yangilash va o'chirish imkoniyatini taqdim etadi.

Fayl tizimi va uning turlari.

Fayl tizimi - bu operatsion tizim ma'lumotlarni saqlash, fayl va katalog (papka)larni tashkil etish hamda ularni boshqarish uchun foydalaniladigan usul hisoblanadi. Amalda hozirgi kunda operatsion tizimlarda ko'p tarqalgan fayl tizimlari turlariga quyidagilar kiradi [1, 2]:

- FAT (File Allocation Table - Fayllarni taqsimlash jadvali): Bu ancha eski fayl tizimi bo'lib, Windows operatsion tizimining eski versiyalarida va boshqa operatsion tizimlarda qo'llaniladi.

- NTFS (New Technology File System - Yangi texnologiyali fayl tizimi): Windows operatsion tizimida qo'llaniladigan zamonaviy fayl tizimi bo'lib, fayllar va papkalar uchun siqish, ruxsatlarni boshqarish hamda shifrlash kabi funksiyalarni qo'llab-quvvatlaydi.

- ext (Extended File System - Kengaytirilgan fayl tizimi): Odatda ushbu fayl tizimi Linux hamda Unix asosidagi operatsion tizimlarda keng qo'llaniladi.

- HFS (Hierarchical File System - Iyerarxik fayl tizimi): macOS operatsion tizimida qo'llaniladigan fayl tizimi hisoblanadi.

- APFS (Apple File System - Apple fayl tizimi): Apple kompaniyasi tomonidan Mac kompyuterlari va iOS qurilmalari uchun taqdim etilgan yangi fayl tizimi hisoblanadi.

- EROFS (Enhanced Read-Only File System - Takomillashtirilgan faqat o'qish uchun fayl tizimi)/HMDFS (Harmony Distributed File System - Harmony taqsimlangan fayl tizimi): HarmonyOS operatsion tizimi uchun Huawei kompaniyasi tomonidan ishlab chiqarilgan bo'lib, ushbu fayl tizimi HarmonyOS operatsion tizimida ishlovchi kompyuterlar va mobil qurilmalar uchun taqdim etilgan yangi fayl tizimi hisoblanadi.

- LROFS (Light Read-Only File System - Yengil faqat o'qish uchun mo'ljallangan fayl tizimi): HyperOS 2.0 operatsion tizimi uchun Xiaomi kompaniyasi tomonidan ishlab chiqarilgan fayl tizimi hisoblanadi. HyperOS 2.0 operatsion tizimida ishlovchi mobil qurilmalar uchun taqdim etilgan yangi fayl tizimi hisoblanadi.

Fayl - bu bir-biri bilan bog'liq ma'lumotlar to'plami bo'lib, ikkilamchi xotiraga yoziladi. Yoki faylni mantiqan bog'langan obyektlar to'plami deb ham qarash mumkin. Foydalanuvchi nuqtai nazaridan fayl - bu mantiqiy ikkilamchi xotiraning eng kichik hajmi hisoblanadi.

Fayl nomi quyida ko'rsatilganidek ikki qismdan iborat bo'ladi:

1. Nomi;
2. Nuqta bilan ajratilgan kengaytmasi.

1-jadval.

Fayl atributlari va ular bilan bajariladigan amallar

№	Fayl atributlari	Fayl turlari	Fayl ustida bajariladigan amallar
1.	Nomi	*.docx	Yaratish (Create)
2.	Turi	*.xlsx	Ochish (Open)
3.	Hajmi	*.exe	O'qish (Read)
4.	Yaratilishi haqidagi ma'lumotlar	*.jpg	Yozish (Write)
5.	Muallifi	*.pdf	Oxiriga qo'shish (Append)
6.	Oxirgi o'zgartirish	*.mp4	Qisqartirish (Truncate)
7.	Holati	*.txt	O'chirish (Delete)
8.	Joylashgan manzili	*.gif	Nomini o'zgartirish (Rename)
9.	Oxirgi kirish vaqti	*.mp3	Joyini o'zgartirish, Nusxalash (Move, Copy)
10.	Ruxsatlar	*.rar	Ruxsatlarni o'rnatish (Change permissions)
11.	Himoya	*.zip	Himoya parametrlari bilan ishlash (Set protection)

Fayl tizimi tomonidan hal qilingan muammolar. Ushbu paragrafda fayl o'zida saqlanishi mumkin bo'lgan ma'lumotlar tuzilmalarini ko'rib chiqamiz. Fayl tizimining vazifasi - fayllarni eng optimal tartibda tashkil etish va boshqarishni ta'minlashdir. Har safar qattiq diskdan fayl o'chirilganda, unda bo'sh joy paydo bo'ladi. Ushbu bo'sh joylarni boshqa fayllar uchun qayta taqsimlash zarur bo'lishi mumkin. Bo'sh joylarni hisobini yuritish ko'pincha zaruriyatga aylanadi. Qattiq diskda fayllarni saqlash uchun joy tanlash, fayllar bilan bog'liq asosiy muammo hisoblanadi. Faylni saqlash uchun bitta blok ishlatilishi yoki ishlatilmasligi ham mumkin. Fayllar ketma-ket bo'lmagan diskning bir nechta bloklarida saqlanishi ham mumkin. Shuningdek, biz fayl tizimi to'g'ri ishlashi uchun fayllarning qismlari joylashgan barcha bloklarini kuzatib borishimiz ham kerak. Bu jarayon fayllarni to'g'ri boshqarish va ularni optimal saqlash uchun muhim sanaladi [2, 3].

Ushbu atributlar va amallar, asosan, operatsion tizim va fayl tizimi orqali boshqariladi. Buni natijasida fayllar bilan qulay, tizimli va xavfsiz ishlash imkoniyati paydo bo'ladi. Fayl atributlari va ular bilan bajariladigan amallar 1-jadvalda keltirilgan.

Fayl kataloglari va ularning xususiyatlari. Fayllar to'plami fayllar katalogini ifodalaydi. Katalog (Papka) fayllar haqidagi ma'lumotlarni, jumladan atributlar, joylashuvi va yaratuvchisini o'z ichiga oladi. Ushbu ma'lumotlarning katta qismi, ayniqsa saqlash bilan bog'liq bo'lgani, operatsion tizim tomonidan boshqariladi. Katalogning o'zi ham fayl hisoblanib, unga boshqarish protseduralari orqali murojaat qilish mumkin.

Quyida xotira qurilmasi katalogida saqlanadigan ma'lumotlar keltirilgan:

- Nomi;
- Turi;
- Manzili;
- Joriy uzunligi;
- Maksimal uzunligi;
- Oxirgi murojaat sanasi;
- Oxirgi yangilangan sanasi;
- Egasining identifikatori;
- Himoya haqidagi ma'lumot.

Katalog ustida bajariladigan amallar quyidagilardan iborat:

- Faylni qidirish;
- Fayl yaratish;
- Faylni o'chirish;
- Katalogni ko'rsatish;
- Faylni qayta nomlash;
- Fayl tizimini ko'rib chiqish.

Kataloglarni yuritishning afzalliklari:

- Samaradorlik: Fayllar tezroq topiladi.
- Nomlash: Bu foydalanuvchilar uchun qulay, chunki ikkita foydalanuvchi turli fayllar uchun bir xil nomdan foydalanishi yoki bir xil fayl uchun har xil nomlardan foydalanishi mumkin.

• Guruhlash: Fayllarni mantiqiy ravishda guruhlash mumkin, masalan, barcha Java dasturlari, barcha o'yinlar va hokazo.

Bir bosqichli katalog.

Bir bosqichli katalog – bu fayl tizimini tashkil qilishning eng sodda usuli bo'lib, unda barcha fayllar bitta umumiy katalogda saqlanadi. Barcha foydalanuvchilar bir xil katalogda ishlaydi va fayllarini shu yerda saqlaydi.

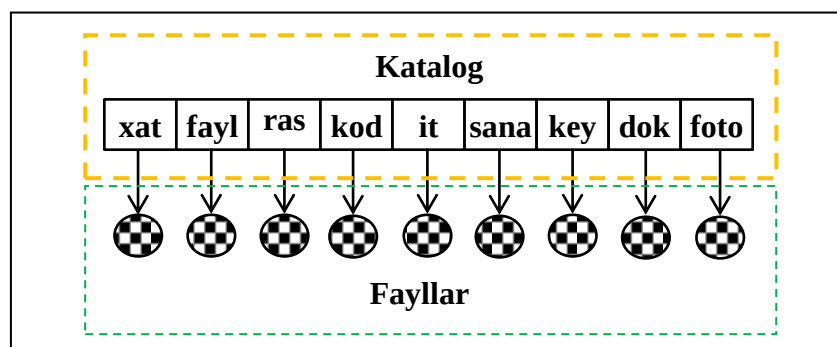
Bu yerda barcha foydalanuvchilar uchun bitta umumiy katalog mavjud.

Nomlash muammosi: Foydalanuvchilar ikki fayl uchun bir xil nomdan foydalana olmaydi.

Guruhlash muammosi: Foydalanuvchilar fayllarni o'z ehtiyojlariga ko'ra guruhlay olmaydi.

Bir bosqichli katalogning tuzilishi:

Asosiy katalog
 fayl.txt
 loyiha.doc
 rasm.png
 kod.py
 hisobot.pdf
 kod.html



1-rasm. Bir bosqichli katalog va unda joylashgan fayllar arxitekturası

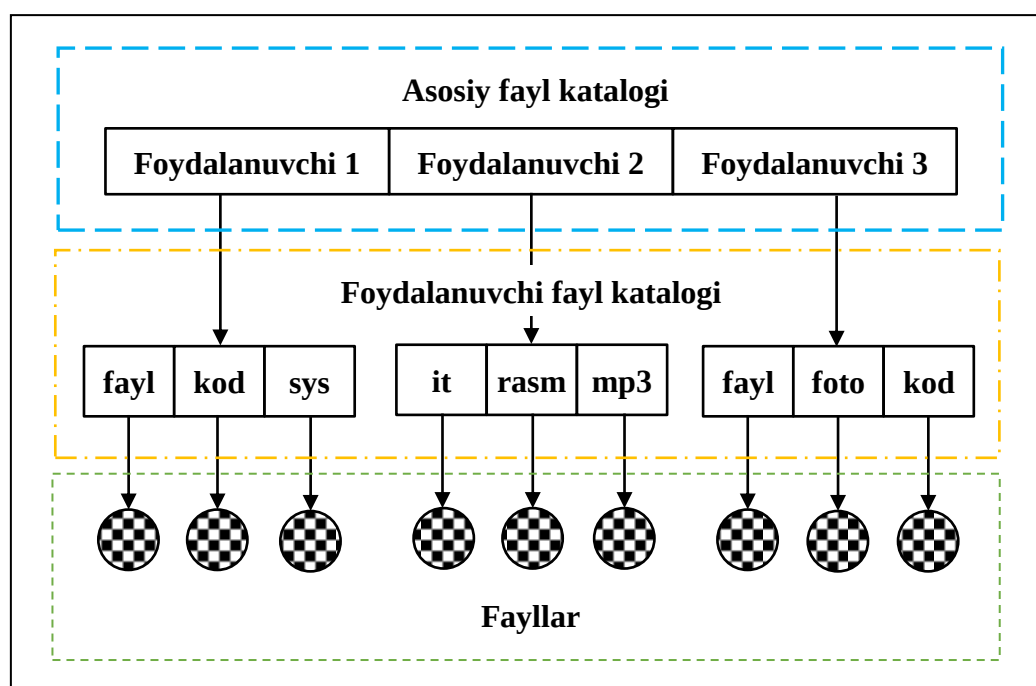
Yuqoridagi katalog va fayllarning aniq bajaradigan vazifasini bilish uchun ularning tizimda qanday ishlashini yaxshi tushinishimiz kerak bo‘ladi. Bir bosqichli katalog va unda joylashgan fayllar arxitekturası 1-rasmda keltirilgan.

Ikki darajali katalog.

Ikki darajali katalog tuzilishi - bu fayl tizimini tashkil qilishning oddiy usullaridan biri bo‘lib, unda har bir foydalanuvchi o‘z shaxsiy katalogiga ega bo‘ladi. Ushbu modelda kataloglar ikki darajaga ajratiladi:

Asosiy katalog - bu barcha foydalanuvchilarni o‘z ichiga oladi.

Foydalanuvchi kataloglari - bu har bir foydalanuvchi o‘z katalogiga ega bo‘lib, faqat shu joyda o‘z fayllarini saqlaydi.



2-rasm. Ikki darajali kataloglar va unda joylashgan fayllar arxitekturası

Bunda har bir foydalanuvchi uchun alohida kataloglar qo'llab-quvvatlanadi.

Yo'l (joylashgan manzil) nomi: Ikki darajali tuzilish tufayli har bir fayl uchun, uni topish mumkin bo'lgan yo'l nomi mavjud bo'ladi.

Endi turli foydalanuvchilar uchun bir xil fayl nomidan foydalanish mumkin bo'ladi. Ushbu usul qidiruv jarayonida samarali hisoblanadi. Ikki darajali kataloglar va unda joylashgan fayllar arxitekturasini 2-rasmda keltirilgan.

Ikki darajali katalogning tuzilishi [2]:

Asosiy katalog.

Foydalanuvchi 1

fayl1.txt

fayl2.doc

Foydalanuvchi 2

loyiha1.pdf

loyiha2.ppt

Foydalanuvchi 3

kod.py

kod.html

Iyerarxik tuzilishga ega katalog. Iyerarxik katalog tuzilishi – bu fayllar va kataloglarni iyerarxik (daraxt) shaklida tashkil qilish usuli bo'lib, u foydalanuvchilarga ma'lumotlarni tartib bilan saqlash va boshqarish imkoniyatini beradi.

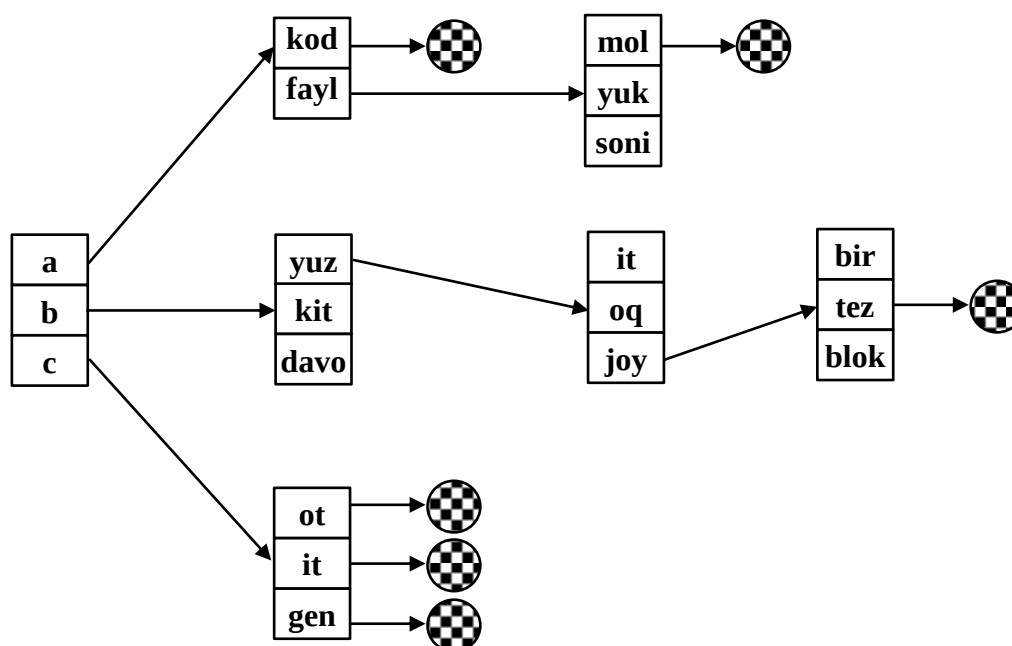
Katalog iyerarxik tuzilishga ega shaklda qo'llab-quvvatlanadi. Ushbu arxitekturada qidiruv jarayoni samarali bo'lib, bundan tashqari, katalog va fayllarni guruhlash imkoniyati ham mavjud bo'ladi. Shu tariqa bizda faylga absolyut yoki nisbiy yo'lni mavjud bo'lishiga ham imkon beradi.

Iyerarxik katalogning tuzilishi:

Asosiy katalog bu - har qanday fayl tizimining eng yuqori darajasi bo'lib, barcha boshqa katalog va fayllarni o'z ichiga oladi.

Ichki kataloglar bu - asosiy katalog ichida joylashgan kataloglar bo'lib, ular ham o'z ichida fayllar va boshqa kataloglarni saqlashi mumkin.

Fayllar bu - katalog ichidagi asosiy ma'lumotlarni o'z ichiga oluvchi elementlar hisoblanadi. Iyerarxik tuzilishga ega katalog va unda joylashgan fayllar arxitekturasini 3-rasmda keltirilgan.



3-rasm. Iyerarxik tuzilishga ega katalog va unda joylashgan fayllar arxitekturasini

Fayllarni taqsimlash usullari. Fayllarni taqsimlashning bir necha keng tarqalgan turlari mavjud bo'lib, ular quyida keltirilgan:

- Uzluksiz taqsimot;
- Bog'langan taqsimot (bir-biriga tutash bo'lmagan taqsimot);
- Indekslangan taqsimot.

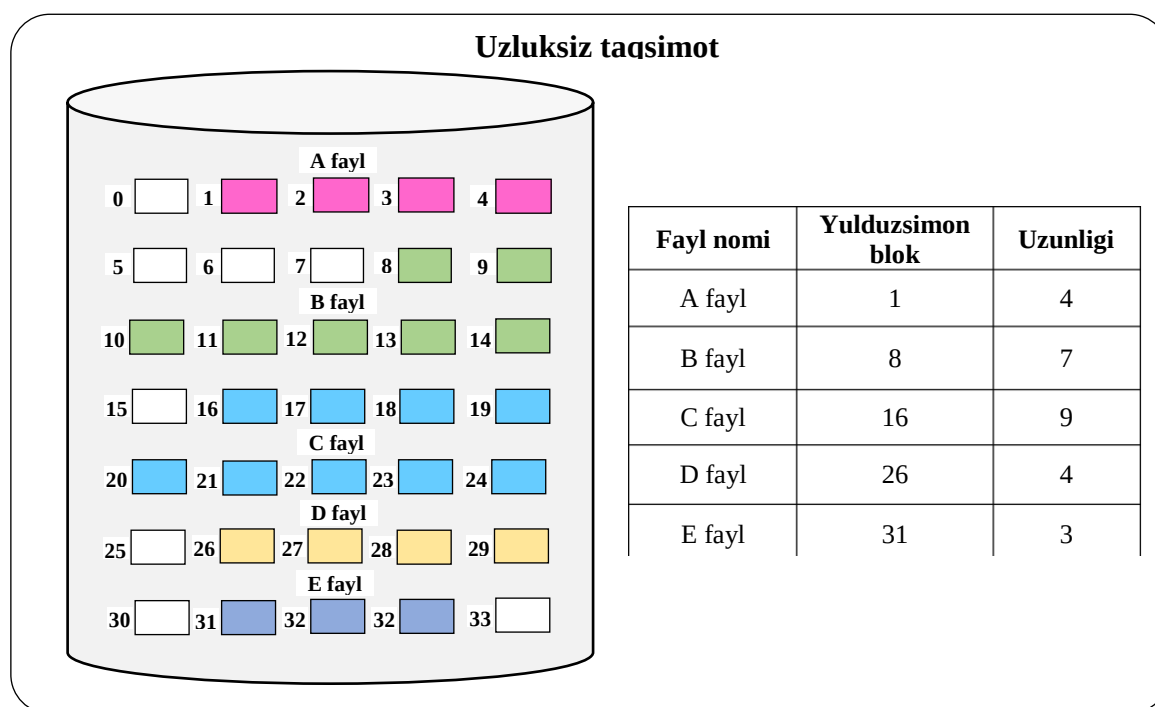
Uzluksiz taqsimot

Uzluksiz taqsimot – bu fayllarni xotira qurilmasida uzluksiz, ketma-ket sektorlar sifatida saqlash usuli hisoblanadi. Ushbu usulda har bir faylga saqlash joyi uzluksiz ajratiladi, ya'ni faylning barcha bloklari xotira qurilmasida bir-biriga yondosh joylashadi.

Fayl yaratilishi paytida faylga uzluksiz bloklar to'plami ajratiladi. Shunday qilib, bu o'zgaruvchan o'lchamli qismlardan foydalanadigan oldindan taqsimlash strategiyasi hisoblanadi. Fayllarni taqsimlash jadvali uchun har bir faylga oid boshlang'ich blok va fayl uzunligini ko'rsatib turuvchi yagona, ya'ni bitta so'z talab qilinadi. Ushbu usul alohida ketma-ket fayl nuqtayi nazaridan eng yaxshi hisoblanadi. Bir vaqtning o'zida bir nechta bloklarni o'qish ketma-ketlik bilan ishlov berishda kiritish-chiqarish samaradorligini oshiradi. Shuningdek, bitta blokni olish ham juda oson. Masalan, agar fayl b blokidan boshlansa va faylning i-blokiga ehtiyoj bo'lsa, ikkilamchi xotirada uning joylashuvi shunchaki $b + i - 1$ bo'ladi.

Uzluksiz taqsimot usulining afzalliklari – bu katalog yoki faylga tezkor kirish, murojaat qilish hamda tezroq bajaradi, sababi barcha bloklar xotirada ketma-ket joylashgan bo'ladi. Shu tariqa xotira qurilmasida amalga oshiriladigan operatsiyalarining samaradorligi, o'qish va yozish operatsiyalari tez amalga oshiriladi.

Uzluksiz taqsimot usulining kamchiliklari - bu fayllarning fragmentatsiyasiga (tarqoq joylashishini) yuzaga kelishiga olib keladi. Vaqt o'tishi bilan xotira qurilmasidagi bo'sh joylar (sector) bo'linib ketishi yuzaga kelishi mumkin, natijada katta fayllar uchun uzluksiz joy topish qiyinlashadi. Bundan tashqari yangi fayl uchun xotiradan joy ajratish jarayoni bilan bog'liq murakkablik bo'lib, oldindan fayl uchun qancha joy ajratish kerakligini aniq bilish talab etiladi. Agar ajratilgan joy yetarli bo'lmasa, faylni kengaytirish qiyin bo'ladi. Ushbu usul CD/DVD disklar, oddiy fayl tizimi bo'lgan, eski FAT tizimida ishlovchi xotira qurilmalarida qo'llaniladi. Fayllarni xotira qurilmasida uzluksiz taqsimot asosida saqlash jarayoni 4-rasmida keltirilgan.



4-rasm. Fayllarni xotira qurilmasida uzluksiz taqsimot asosida saqlash jarayoni

Uzluksiz taqsimotning kamchiliklari:

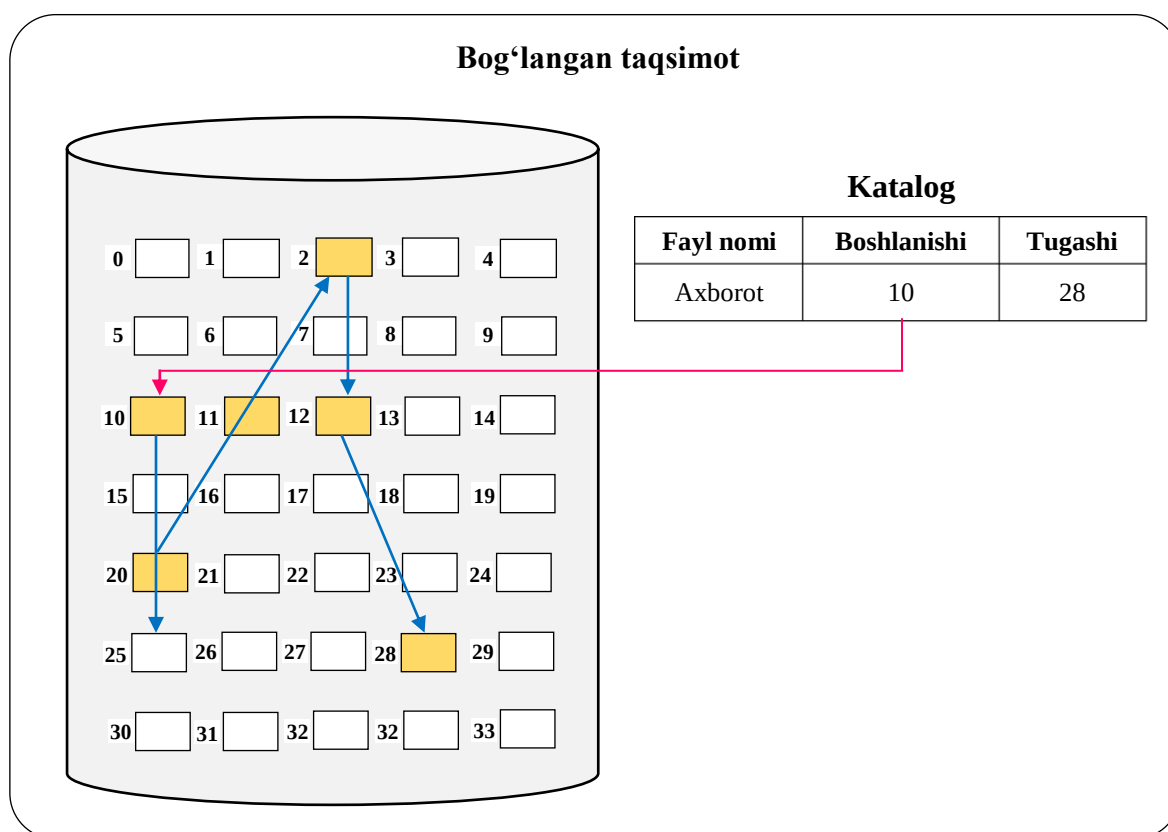
- Xotira qurilmasida uzluksiz taqsimot usulidan foydalanish jarayonida tashqi fragmentatsiya muammosi yuzaga keladi, bu esa ketma-ket joylashgan kerakli uzunlikdagi bloklarni topishni qiyinlashtiradi. Xotira qurilmasidan qo'shimcha joy bo'shatish uchun siqish algoritmi kerak bo'ladi;

- Bundan tashqari, xotira qurilmasidagi joyni oldindan taqsimlash jarayonida, ya'ni fayl yaratilayotganda uning hajmini belgilash talab etiladi.

Bog'langan taqsimot (bir-biriga tutash bo'lmagan taqsimot).

Bog'langan taqsimotli arxitekturaga ega fayl tizimi, faylni alohida bloklarga ajratish usuli bo'lib, har bir blok keyingi blokka ishora qiluvchi ko'rsatkichni o'z ichiga oladi. Bu usulda xotira qurilmasidagi bloklar ketma-ket bo'lishi shart emas, chunki har qanday bo'sh blok xotira zanjiriga qo'shilishi mumkin. Natijada tashqi fragmentatsiya yuzaga kelmaydi, biroq faylning oxirgi blokida ichki fragmentatsiya yuzaga kelish xavfi mavjud bo'ladi [3].

Ushbu usulda taqsimot alohida blok asosida amalga oshiriladi. Har bir blok zanjirdagi keyingi blokka ishora qiluvchi ko'rsatkichni o'z ichiga oladi. Yana shuni ta'kidlash joizki, fayl tizimi jadvali uchun har bir faylga faqat bitta so'z yetarli bo'ladi, unda faylning boshlang'ich bloki va uzunligi ko'rsatiladi. Garchi fayl uchun xotira qurilmasidagi joyni oldindan ajratish imkoniyati mavjud bo'lsada, ko'p hollarda bloklarni faqatgina zarurat tug'ilgandagina ajratish odatiy holga aylanib qolgan. Xotira qurilmasidagi istalgan bo'sh blok xotira zanjiriga qo'shilishi mumkin, bu jarayonda bloklar ketma-ket bo'lishi shart emas. Agar xotira qurilmasining bo'sh bloki mavjud bo'lsa, fayl hajmini oshirish har doim mumkin. Tashqi fragmentatsiya yo'q, chunki har safar faqat bitta blok ajratiladi, lekin ichki fragmentatsiya yuzaga kelishi mumkin, u faqat xotira qurilmasining fayl joylashgan oxirgi blokida yuz beradi.



5-rasm. Fayllarni xotira qurilmasida bog'langan taqsimot asosida saqlash jarayoni

Bog'langan taqsimotning ishlash tamoyiliga misol.

Misol uchun bizda, "Axborot.txt" nomli fayl bor va u xotira qurilmasida 3 ta blokdan iborat. Xotira qurilmasi bloklari ketma-ket, masalan, 1, 2, 3, 4, 5, 6, 7 ... shaklda raqamlangan bo'lsin;

O'R MV AKT VA ALOQA HARBIY INSTITUTI

- Bu faylning birinchi bloki - blok 4;
- Blok 4 ichida navbatdagi blok - blok 7 ga ishora qiluvchi ko'rsatkich mavjud bo'ladi;
- Blok 7 ichida esa keyingi blok - blok 2 ga ishora qiluvchi ko'rsatkich bo'ladi;
- Blok 2 faylning oxirgi bloki bo'lgani uchun boshqa blokka ishora qilmaydi (masalan, "0" yoki maxsus belgi bilan tugaydi).

Shunday qilib, faylning bloklari xotira qurilmasida ketma-ket joylashmagan ($4 \rightarrow 7 \rightarrow 2$), ammo bog'lanishlar orqali ketma-ketlik ta'minlanadi. Bu bog'langan taqsimot deb ataladi. Bunda diskning qayerida bo'sh joy bo'lsa, o'sha blok faylning keyingi qismi sifatida qo'shilishi mumkin va xotira qurilmasidan ajratiladigan joy uzluksiz (ketma-ket) joylashishi talab etilmaydi. Fayllarni xotira qurilmasida bog'langan taqsimot asosida saqlash jarayoni 5-rasmda keltirilgan.

Bog'langan taqsimotning kamchiliklari:

- Ichki fragmentatsiya xotira qurilmasidagi faylning oxirgi blokida mavjud bo'ladi;
- Har bir blokda ko'rsatkichni saqlash qo'shimcha resurs sarflashni talab qiladi;
- Agar biror blokka ko'rsatkich ishora yo'qolsa, fayl zararlangan (to'liq bo'lmagan) holga keladi;
- Fayllarga kirish faqat ketma-ket holda amalga oshiriladi.

Indekslangan taqsimot.

Indekslangan taqsimotli arxitekturaga ega fayl tizimi, faylni xotira qurilmasining bloklariga taqsimlash va ularni boshqarish usuli bo'lib, har bir fayl uchun alohida indeks (yoki indeks blok) yaratiladi. Ushbu indeksda faylga tegishli barcha bloklarning manzillari (xotira qurilmasidagi joylari) saqlanadi.

Indekslangan taqsimotda uzluksiz va bog'langan taqsimotning ko'plab muammolari samarali hal etiladi. Ushbu usulda xotira qurilmasidagi fayl taqsimlash jadvali har bir fayl uchun alohida bir bosqichli indeksni saqlaydi. Indeks faylga ajratilgan har bir blok uchun bitta yozuvni o'z ichiga oladi. Taqsimot doimiy (qat'iy) o'lchamdagi bloklar yoki o'zgaruvchan o'lchamdagi bloklar asosida amalga oshirilishi mumkin. Qat'iy o'lchamdagi bloklar asosidagi taqsimot tashqi fragmentatsiyani bartaraf etadi, o'zgaruvchan o'lchamdagi bloklar asosidagi taqsimot esa ichki taqsimotni yaxshilaydi. Bu taqsimlash usuli faylga ham ketma-ket, ham to'g'ridan-to'g'ri murojaat qilishni qo'llab-quvvatlaydi va shu bois fayllarni xotira qurilmasiga taqsimlashning eng ommabop shakli hisoblanadi.

Indekslangan taqsimotning afzalliklari:

- Oson boshqarish: Faylga tegishli bloklarning ro'yxati bitta indeks blokda saqlanadi, bu boshqarish va izlash jarayonini soddalashtiradi.
- To'g'ridan-to'g'ri ixtiyoriy kirish: Indeks blokidagi manzilga asoslanib, faylning istalgan blokiga tezda murojaat qilish mumkin.
- Juda kam tashqi fragmentatsiya: Fayl bloklari xotira qurilmasida ketma-ket bo'lishi shart emas, chunki indeks ularning joylashuvini oson topishga yordam beradi.
- Qulay kengaytirish: Fayl hajmini oshirish uchun xotira qurilmasidagi yangi bo'sh blok adresini indeks blokiga qo'shish kifoya.

Indekslangan taqsimotning kamchiliklari:

- Indekslangan blok hajmi: Agar fayl juda katta bo'lsa, uning bloklari haqida ma'lumot saqlash uchun ko'p joy kerak bo'ladi. Shuning uchun ko'p darajali indekslash kabi murakkab usullar qo'llanishi mumkin.
- Qo'shimcha xotira talabi: Indekslangan blokni saqlash va boshqarish uchun qo'shimcha resurslar kerak bo'ladi.

Fayl tizimining afzalliklari.

Fayl tizimi axbort tizimida ma'lumotlarni samarali saqlash, boshqarish va ulardan foydalanish imkoniyatini taqdim etuchi asosiy tuzilmalardan biri hisoblanadi. Uning bir qancha muhim afzalliklari mavjud. Quyida ushbu afzallikni ko'rib chiqamiz [5]:

1. Tartiblash va boshqarish qulayligi;

Fayl tizimi ma'lumotlarni kataloglar va qism kataloglar orqali tartibga solishga imkon beradi. Bu esa foydalanuvchilarga kerakli ma'lumotlarni osongina topish va boshqarish imkonini taqdim etadi.

Agar fayllar tartiblanmagan bo'lsa, katta hajmdagi ma'lumotlar ichidan kerakli faylni topish qiyin va ko'p talab qilishi mumkin. Fayl tizimi har xil turdagi ma'lumotlarni (rasmlar, hujjatlar, dasturlar) turli kataloglarga ajratish orqali ularni tartiblab va saqlab boradi. Korporativ axborot tizimida, tashkilotning hujjatlari xodimlar, bo'limlar yoki muhimligiga qarab turlariga ajratilishi mumkin. Fayl tizimi foydalanuvchilar o'rtasida samarali hamkorlik qilish imkonini taqdim etadi, chunki har kim o'z fayllarini xotira qurilmasining o'ziga tegishli joyda saqlashi mumkin.

2. Ma'lumotlarni himoya qilish;

Fayl tizimlari odatda ma'lumotlarni himoya qilish uchun maxsus vositalarni taqdim etadi. Misol uchun foydalanuvchi va administrator huquqlari (qaysi foydalanuvchi qanday fayllarga kirishi mumkinligi nazorat qilinadi). Ma'lumotlarni zahira nusxalarni yaratish va tiklash imkoniyati. Fayl tizimidagi xatolarni aniqlash va tuzatish funksiyalari va boshqa jarayonlarni misol qilib keltirish mumkin.

Agar fayllarga ulardan foydalanish ruxsatlari to'g'ri o'rnatilmasa, maxfiy yoki muhim ma'lumotlar ruxsatsiz sirqib chiqishi mumkin. Masalan, Windows operatsion tizimidagi NTFS (New Technology File System) fayl tizimi har bir fayldan kim foydalanishi mumkinligini aniqlash va belgilash imkonini taqdim etadi. Tashkilot axborot tizimlarida saqlanayotgan ma'lumotlarni zahira nusxalarini olib borish, axborot xavfsizligi hodisalardan keyin axborot tizimini qayta tiklash imkoniyatini yaxshilashga yordam beradi. Fayl tizimlari zararli dasturlar va xakerlik hujumlaridan himoyani ta'minlash jarayonida ham muhim rol o'ynaydi.

3. Yuqori unumdorlik;

Samarali ishlaydigan fayl tizimi ma'lumotlarni tez o'qish va yozish imkonini beradi. Bu esa operatsion tizim va ilovalarning ishlash tezligini oshiradi.

Fayl tizimi ma'lumotlarni xotira qurilmasining bloklari bo'ylab bir tekis taqsimlab, ularning tezkor ishlashini ta'minlashi lozim. Ko'p ishlatiladigan fayllar operativ xotirada vaqtincha saqlanib, ularning yuklanish tezligi oshiriladi. Zamonaviy SSD disklar uchun fayl tizimlari optimallashtirilgan bo'lib, ma'lumotlarni tezroq yozish va o'qishga imkon yaratadi.

4. Xotira qurilmasining bloklaridan samarali foydalanish;

Fayl tizimi ma'lumotlarni ixcham joylashtirish orqali xotira qurilmasi bloklaridan optimal foydalanish imkonini beradi:

- Fayllarni siqish: Ba'zi fayl tizimlari avtomatik siqish funksiyasini qo'llab quvvatlaydi, bu esa ma'lumot hajmini kamaytiradi;

- Klaster hajmini moslash: Katta hajmli fayllar va kichik hajmli fayllarni saqlash usullari har xil bo'lishi mumkin, bu esa joyni tejash imkonini beradi;

- Zahira nusxalarni optimallashtirish: Ba'zi tizimlar bir xil fayllarning bir necha nusxasini avtomatik ravishda optimallashtirib, disk maydonini tejaydi.

5. Ko'p foydalanuvchili muhitni qo'llab-quvvatlash imkoniyati;

Fayl tizimi bir vaqtning o'zida bir nechta foydalanuvchi tomonidan foydalanish imkonini taqdim etadi. Bu imkoniyatlar quyidagilarni o'z ichiga oladi.

- Kompyuter tarmoqlariga asoslangan fayl tizimlari: Tashkilot serveridagi fayllarga bir nechta foydalanuvchi bir vaqtning o'zida kirishi va foydalana olishi mumkin;

- Fayl tizimiga kirish huquqini na'zoratlash: Bir foydalanuvchi fayl ustida ishlayotganda boshqasi uni o'zgartirishini oldini olish mumkin;

- Fayl tizimidan foydalanish jarayonidagi ruxsatlarni belgilash: Har bir foydalanuvchiga alohida huquqlar berilishi mumkin (o'qish, yozish, o'chirish).

6. Moslashuvchanlik va turli platformalarda qo'llab-quvvatlashi.

Fayl tizimlari turli operatsion tizimlar va qurilmalar o'rtasida moslikni ta'minlaydi.

- NTFS (Windows), ext4 (Linux), APFS (macOS) kabi turli fayl tizimlari mavjud;

- FAT32 va exFAT tizimlari universal bo'lib, Windows, macOS, va Linuxda operatsion tizimlarida ishlaydi;

- Bulutli saqlash tizimlari (Google Drive, OneDrive, Dropbox) ham zamonaviy fayl tizimlari asosida ishlaydi va har xil qurilmalar uchun moslasha oladi.

Fayl tizimi kompyuter va serverlarning asosiy komponentlaridan biri bo'lib, ma'lumotlarni samarali saqlash, tartiblash, xavfsizligini ta'minlash va ular ustida bajariladigan jarayonlarni tezkor hal qilish imkonini beradi.

Fayl tizimining kamchiliklari.

Fayl tizimi ma'lumotlarni boshqarish va saqlash uchun juda muhim vazifani bajarsa ham ba'zi kamchiliklardan holi emas. Quyida fayl tizimining asosiy kamchiliklari ko'rib chiqamiz.

1. Moslashuvchanlik muammolari;

Turli operatsion tizimlar har xil fayl tizimlaridan foydalanadi, bu esa ularning bir-biri bilan moslashuvchan ishlashini qiyinlashtiradi. Misol uchun Windows operatsion tizimi NTFS fayl tizimidan foydalanadi, ammo macOS operatsion tizimi uni faqat o'qiy oladi, yozish esa qo'shimcha dasturlar orqali amalga oshiriladi. Linux operatsion tizimidagi ext4 fayl tizimidan foydalanadi, ammo Windows operatsion tizimi uni standart ravishda qo'llab-quvvatlamaydi. USB flesh xotira va boshqa tashqi xotira qurilmalari uchun FAT32 yoki exFAT fayl tizimi ko'p hollarda universal variant bo'lsa ham, FAT32 4 GB dan katta fayllarni saqlay olmaydi.

Agar foydalanuvchi turli operatsion tizimlarda ishlasa, bir turdagi operatsion tizimda yaratilgan fayl formatlari boshqasiga mos kelmasligi muammosi yuzaga kelishi mumkin. Fayl tizimini ishlab chiqaruvchilar yoki axborot texnologiyalari mutaxassisleri muammolarni bartaraf etish uchun boshqa qo'shimcha dasturlarni ishlab chiqishiga to'g'ri keladi. Ushbu kamchilik tarmoq arxitekturasida ishlaydigan fayl tizimlari va bulutli saqlash tizimlari orqali qisman hal qilinishi mumkin.

2. Xotira qurilmasi maydonlaridan samarasiz foydalanish;

Fayl tizimlari ma'lumotlarni saqlash uchun klaster deb ataluvchi birliklardan foydalanadi. Har bir fayl ushbu klasterlarga joylashtiriladi. Agar fayl hajmi klasternikidan kichik bo'lsa, bo'sh joy isrof bo'lishiga olib keladi. Misol uchun NTFS fayl tizimida klaster hajmi 4 KB bo'lsa, hajmi 1 KB bo'lgan fayl 4 KB joy egallaydi, ya'ni xotira qurilmasida 3 KB bo'sh qoladi, ammo ushbu joy ishlatilmaydi. Shu sababli xotira qurilmasida kichik fayllar ko'p bo'lsa, katta hajmdagi diskda ham foydalanilmagan bo'sh joylar ko'payib ketadi.

Bu muammo ayniqsa katta ma'lumotlar bazalari va serverlar uchun sezilarli darajada katta bo'lishi mumkin. Ba'zi fayl tizimlari siqish algoritmlariga ega bo'lib, bu muammoni qisman hal qilish imkonini beradi. Xotira qurilmasi maydonini optimallashtirish uchun SSD va HDD disklar uchun moslashtirilgan fayl tizimlaridan foydalanish tavsiya etiladi [6].

3. Ma'lumotlarning butunligini buzilishi va xavfsizlik muammolari;

Fayl tizimlari turli sabablar tufayli ma'lumotlarning butunligini buzilishiga yoki yo'qolishiga olib kelishi mumkin. Misol uchun elektr ta'minotidagi uzilishlar sababli xotira qurilmasiga yozilayotgan fayl to'liq saqlanmay qolishi mumkin. Zararli dasturlar (viruslar) fayl tizimi yoki fayllarni shikastlanishi yoki ruxsatsiz shifrlanishi mumkin. Fayl tizimida turli xatoliklar, misol uchun noto'g'ri o'chirilgan fayllar yoki diskda nosozliklar yuzaga kelishi mumkin.

NTFS kabi fayl tizimlari journaling texnologiyasidan foydalanib, avariya va kritik holatlarida fayllarni tiklash imkonini beradi. Journaling texnologiyasi ma'lumotlarni yozish, kuzatish va qayta tiklash jarayonini qo'llab-quvvatlaydigan texnologiya bo'lib, odatda ma'lumotlar bazalari, fayl tizimlari va log fayllarni yuritish tizimlarida qo'llaniladi. Zahira nusxalardan foydalanish ma'lumotlarni yo'qolishiga qarshi eng samarali himoya usuli hisoblanadi. Antivirus dasturlaridan foydalanish zararli dasturlardan himoyalashga yordam beradi.

4. Fragmentatsiya muammosi;

Fayllar xotira qurilmasida aniqlangan bo'sh joylarga joylashtiriladi. Agar faylga qo'shimchalar kiritilsa, u butunlay boshqa joyga bo'linib ketishi mumkin. Bu holat fragmentatsiya deb ataladi va quyidagi muammolarni keltirib chiqaradi:

- Xotira qurilmasidan o'qish tezligi pasayadi;
- Xotira qurilmasi boshqaruvchi tizimning resurslarini ortiqcha sarf bo'lishiga olib keladi.

HDD disk kabi xotira qurilmalari fragmentatsiyadan ko'proq zarar ko'radi, sababi aylanuvchi mexanizmlar fayllarni o'qish uchun ko'proq vaqt sarflashiga olib keladi. SSD disklar uchun fragmentatsiya unchalik katta muammo emas, ammo haddan tashqari ma'lumotlarni ko'p marta yozish xotira qurilmasining hayotiy siklini qisqartirishiga olib kelishi mumkin. Defragmentatsiya usuli va vositalari orqali HDD disklar uchun bu muammoni bartaraf etilishi mumkin.

5. Fayl yoki fayl tizimi ustida bir vaqtda ikki va undan ortiq foydalanuvchini ishlashi bilan bog'liq cheklovlar;

Fayl tizimlari ko'p foydalanuvchili muhitda ishlash uchun mo'ljallangan bo'lsada, ba'zi kamchiliklarga ega hisoblanadi. Ushbu kamchiliklar quyidagilardan iborat:

- Faylga bir vaqtning o'zida ikkita foydalanuvchi yozish bilan bog'liq o'zgartirish kiritishi mumkin emas;
- Ba'zi fayl tizimlari tarmoq orqali ishlaganda kechikishlar bilan ishlashiga sabab bo'lishi mumkin.

Faylni bloklash texnologiyasi yordamida bitta foydalanuvchi faylni tahrirlayotganda boshqalarning kirishini cheklashi mumkin.

6. Xotira qurilmasining eskirishi va boshqa texnologik muammolar.

Ba'zi eski fayl tizimlari (FAT32) zamonaviy talablarni qondira olmaydi. Sababi yangi texnologiyalar bilan moslashuvchanligi cheklangan bo'lishi mumkin. Yangi SSD va NVMe disklar uchun maxsus optimallashtirilgan fayl tizimlari talab qilinadi. Yangi ZFS (Zettabyte File System) va Btrfs (B-tree File System) kabi ilg'or fayl tizimlari o'z-o'zini tiklash funksiyalariga ega bo'lib, bu muammoni qisman hal qiladi. Btrfs ma'lumotlarni yaxlit saqlash, hajmni dinamik boshqarish va snapshot funksiyalari bilan ajralib turadi.

Fayl tizimlari ma'lumotlarni samarali saqlash va boshqarishda muhim rol o'ynaydi, ammo u ham yuqorida ko'rib chiqilgan kamchiliklardan holi emasligi aniqlandi. Barcha kamchiliklarga qaramasdan, zamonaviy fayl tizimlari (NTFS, ext4, ZFS, Btrfs) bu muammolarni minimallashtirishga imkon beradi. Ma'lumotlarni saqlash uchun fayl tizimini tog'ri tanlash va uni muntazam optimallashtirib turish fayl tizimi samaradorligini oshirishga xizmat qiladi.

Fayl tizimlari operatsion tizimlarning muhim komponentalaridan biri bo'lib, ular xotira qurilmalarida ma'lumotlarni saqlash, tartibga solish va ularga murojatlarni boshqaradi. Fayl tizimlari fayllar va kataloglarni yaratish, ularni boshqarish hamda himoya qilish uchun zarur bo'lgan tuzilma va qoidalarni to'g'ri ishlashini ta'minlaydi. Xotira qurilmalarida ma'lumotlarni saqlashni samarali boshqarish, fayllar joylashivini oson navigatsiya qilish va ishonchli xavfsizlik mexanizmlari orqali fayl tizimlari kompyuter tizimlarining funkcionalligi, samaradorligi va ishonchliligiga o'z hissasini qo'shadi.

Fayl tizimi himoyasini ta'minlash.

Axborot tizimlarida foydalanuvchi va unga tegishli bo'lgan juda ko'p ma'lumot saqlanadi. Operatsion tizimning asosiy vazifasi fayl tizimidagi foydalanuvchi ma'lumotlariga g'araz niyatli shaxslarni ruxsatsiz suqilib kirishidan himoya qilish hisoblanadi. Ushbu himoyani ta'minlanish turli usul va vositalar yordamida amalga oshiriladi. Bitta shaxshiy kompyuter, noutbuk yoki axborot saqlash qurilmasidagi ma'lumotni himoya qilish uchun ushbu axborotlashtirish vositasini temir javon tortmasiga yoki maxsus shkafiga qulflab qo'yish yetarli bo'ladi. Ko'p foydalanuvchili axborot tizimlarida esa axborot xavfsizligini ta'minlash uchun turli xil himoyani mexanizmlari keng qo'llaniladi [7].

Katalog va fayllardan foydalanish huquqlarining turlari.

Axborot tizimining barcha foydalanuvchilarga bir xil huquq berilib, ular to'g'ridan-to'g'ri kirish imkonini mavjud bo'lgan fayllar axborot xavfsizlik modellari tomonidan homoyalaniishi talab etiladi. Axborot tizimining barcha foydalanuvchilariga bir xil foydalanish huquqiga berilmagan fayllar esa hech qanday himoya mexanizmini talab qilmaydi. Himoya mexanizmi foydalanuvchilarga fayl tizimiga nazorat ostida kirish va foydalanish imkoniyatini taqdim etadi, ya'ni faylga kirish va undan foydalanish huquqlarini oldindan berilgan qoidalar asosida nazorat qiladi. Fayldan foydalanishga ma'lum shaxsga ruxsat berilishi yoki berilmasligi bir nechta omillarga orqali amalga oshiriladi. Ushbu omillardan biri fayldan foydalanish uchun shaxsga berilgan foydalanish huquqi hisoblanadi. Ushbu huquqlar orqali katalog va fayllar ustida amalga oshiriladigan turli operatsiyalarni boshqarish mumkin:

- o'qish – fayldan ma'lumot o'qish;
- yozish – faylga ma'lumot yozish yoki mavjud faylni qayta yozish;
- bajarish – faylni yuklagandan so'ng, uning bajarilish jarayonini boshlanishi;
- tahrirlash – mavjud faylga yangi ma'lumotlar yozish va qo'shishni o'z ichiga olib, tahrir jarayoni faylning oxirida yakunlanishi lozim.
- o'chirish – keraksiz faylni o'chirib tashlash va u egallab turgan xotira maydonini boshqa ma'lumotlar uchun bo'shatish va qayta ishlatish uchun tayyorlash;
- ro'yxat – fayl nomi va uning atributlarini ko'rsatish.

Shuningdek, katalog yoki fayl ustida ularni qayta nomlash, mavjud faylni tahrirlash va nusxa ko'chirish kabi operatsiyalarni ham bajarilishi mumkin. Fayl tizimida foydalaniladiugan himoya usullari, vositalari va mexanizmlari juda ko'p bo'lib, ularning har biri o'zining afzallik hamda kamchiliklariga ega. Shu sababli ushbu himoya vositalari faylni himoyalash darajasidan kelib chiqib tanlanish va foydalanish talab etiladi.

Katalog va fayllardan foydalanish huquqlarini nazorat qilish.

Axborot tizimining foydalanuvchilari turli fayl tizimlariga murojatni amalga oshirish uchun turli usullardan foydalanadilar. Fayl tizimidagi axborot himoyasini tashkil qilishning samarali usuli bu - barcha fayl va kataloglarga identifikator asosida bog'langan "Foydalanish huquqlarini boshqarish ro'yxati" (Access Control List) shaklida taqdim etish hisoblanadi. Ushbu ro'yxatda foydalanuvchilarning ismlari va har bir foydalanuvchiga tegishli huquqlar va ularning turlari ko'rsatiladi.

Foydalanish huquqlarini boshqarish ro'yxatining asosiy muammosi bu - ushbu ro'yxatining nihoyatda uzunligi sanaladi. Masalan, agar faylni har bir foydalanuvchiga o'qish uchun ruxsat bermoqchi bo'lsak, o'qish huquqiga ega bo'lgan barcha foydalanuvchilarni ro'yxatda sanab chiqishimiz kerak bo'ladi. Bu usul ikkita kamchilikka ega hisoblanadi. Ushbu usulning kamchiliklari quyidagilardan iborat:

1. Foydalanish huquqlarini boshqarish ro'yxatini to'liq ishlab chiqish juda zerikarli va murakkab jarayonni o'z ichiga olishi mumkin;

2. Agar tizimda kimlar foydalanuvchi ekanini oldindan aniq bilmasak, bu jarayon yanada murakkablashadi.

Hisobot nomli katalogida joylashgan fayl oldin aniq (fiksirlangan) xotira hajmiga ega edi, ammo endi u o'zgaruvchan hajmga ega falga aylangani sababli, xotira qurilmasidagi joyni boshqarish murakkabligi yuzaga keladi. Ushbu muammoni foydalanish huquqlarini boshqarish ro'yxatining qisqartirilgan variantidan foydalanish orqali hal qilish mumkin. Foydalanish huquqlarini boshqarish ro'yxati hajmini qisqartirish maqsadida aksariyat (LINUX) operatsion tizimlar har bir fayl bo'yicha foydalanuvchilarni uch toifaga ajratadi:

1. Yaratuvchi (owner) bu - faylni yaratgan foydalanuvchi, ya'ni uning egasi hisoblanadi;
2. Guruh (group) bu - o'xshash xususlarga ega bo'lgan va bitta fayldan birgalikda foydalanadigan ishtirokchilar jamoasi to'plami hisoblanadi;
3. Boshqalar (other) bu - tizimda qolgan barcha foydalanuvchilar boshqalar deb nomlanuvchi huquqga ega toifaga kiradi [8].

6-rasmda keltirilgan $rw\bar{x}$ kombinatsiyasi ikkilikda 111, sakkizlikda 7 ga teng. Har bir bit - mos ravishda $r=4$, $w=2$, $x=1$ ballardan iborat holda tuziladi. Ballarning yig'indisi katalog yoki fayl uchun kerakli ruxsatlar sonini va qiymatini ifodalaydi.

Katalog va fayllarga ruxsatlarni boshqarish jarayoni			
Ikkilik	Sakkizlik	Satr koʻrinishi	Ruxsatlarning turlari
000	0 (0+0+0)	---	Ruxsat yoʻq
001	1 (0+0+1)	--x	Ishga tushirish
010	2 (0+2+1)	-w-	Yozish
011	3 (0+2+1)	r--	Yozish + Ishga tushirish
100	4 (4+0+0)	r-x	Oʻqish
101	5 (4+0+1)	rw-	Oʻqish + Ishga tushirish
110	6 (4+2+0)	rw-	Oʻqish + Yozish
111	7 (4+2+1)	rw x	Oʻqish + Yozish + Ishga tushirish

Foydalanuvchilarga berilgan rollar

Yaratuvchi

r w x

r	Oʻqish	4	7
w	Yozish yoki Tahrirlash	2	
x	Ishga tushirish	1	

Guruh

r w -

r	Oʻqish	4	6
w	Yozish yoki Tahrirlash	2	
-	Ruxsat yoʻq	0	

Boshqalar

r - x

r	Oʻqish	4	5
-	Ruxsat yoʻq	0	
x	Ishga tushirish	1	

6-rasm. Katalog va fayllardan foydalanish huquqlarini boshqarish uchun ularni toifalarga ajratish hamda mos ruxsatlarni belgilash jarayoni

Oxirgi yillarda eng keng tarqalgan yondashuv bu – yaratuvchi, guruh va boshqalar kabi umumiy foydalanish huquqlari nazorat sxemasini foydalanish huquqlarini nazorat qilish ro'yxati bilan birlashtirishdan iborat hisoblanadi. Misol uchun Solaris operatsion tizimi odatda foydalanuvchilarning uchta toifasidan foydalanadi, ammo zarur bo'lganda aniqroq foydalanish huquqlarini boshqarish uchun ayrim fayl va kataloglarga qo'shimcha boshqaruv ro'yxatlarini qo'shish imkoniyatini ham taqdim etadi. Katalog va fayllardan foydalanish huquqlarini boshqarish uchun ularni toifalarga ajratish hamda mos ruxsatlarni belgilash jarayoni 7-rasmda keltirilgan.

Fayl tizimini himoya qilishning boshqa yondashuvlari.

Har qanday fayl tizimga kirish parolli himoya mexanizimi bilan boshqariladi. Agar parol tasodifiy tanlansa va vaqtning ma'lum bir davri davomida tez-tez almashtirib turilsa, bu faylni ruxsatsiz foydalanishdan samarali himoyalashga olib kelishi mumkin.

Faylga ruxsatlarni boshqarishda parollardan foydalanishning bir nechta kamchiliklari ham mavjud bo'lib, ular quyidagilardan iborat [9]:

1. Parolning uzunligi juda katta bo'lishi mumkinligi tufayli ularni yodda saqlash qiyinchiligi yuzaga keladi;

2. Agar tizimdagi barcha fayllar uchun bitta paroldan foydalanilgan bo'lib, ushbu parolning o'brusizlanishi yuzaga kelgan bo'lsa, buzg'unchiga tizimdagi barcha fayllardan ruxsatsiz to'liq foydalanishiga olib keladi. Ushbu himoya tizimi "Hammasi yoki hech narsa" tamoyili bo'yicha axborot xavfsizligini ta'minlash jarayonini anglatadi.

Fayl tizimlarida ma'lumotni himoyalash mexanizmlari.

Fayl tizimlarida ma'lumotni himoya qilish axborot xavfsizligi sohasidagi nihoyatda muhim va dolzarb masalalardan biri hisoblanadi. Fayl tizimida yuzaga kelgan xatolik ko'pincha xotira qurilmalarining ishdan chiqishi natijasida paydo bo'ladigan muammolardan kam bo'lmagan qiyinchiliklarni tug'diradi. Fayl tizimidagi ma'lumotlarni qayta tiklash jarayoni qiyin kechadigan, uzoq vaqt talab qiladigan va ba'zan umuman imkonsiz bo'lgan ishga aylanishi mumkin. Bu jarayonda juda ko'p narsa amalda foydalanilayotgan fayl tizimiga bog'liq bo'ladi. Shu sababli ishonchlilik, fayllar yaxlitligini ta'minlash, xatoliklarga bardoshlilik va tiklash imkoniyati kabi omillar fayl tizimini tanlashda hal qiluvchi ahamiyat kasb etishi kerak. Ko'plab fayl tizimlari uchun formatlash, adashib o'chirib yuborish yoki jiddiy xatoliklardan natijasida kuchli fragmentatsiyaga uchragan xotira qurilmasidagi ma'lumotlarni to'liq tiklash deyarli imkonsiz vazifaga aylanib qolishi mumkin.

Fayl tizimlarida foydalanish huquqlarini cheklash ham rivojlantirilishi kerak bo'lgan dolzarb yo'nalishlardan biri sanaladi. Sababi eng keng tarqalgan foydalanish huquqlarini cheklashning diskretion modelining imkoniyatlari ko'p hollarda fayl tizimidagi himoyani ta'minlash uchun yetarli bo'lmay qolmoqda. Ba'zi holatlarda fayl tizimi xavfisligini taminlash uchun mandatli, rolli yoki semantik kabi foydalanishni cheklash modellaridan foydalanish maqsadga muvofiq hisoblanadi [10].

Fayl tizimidagi ma'lumotlarini kriptografik himoya qilish uning xavfsizligini, balki operatsion tizimning qonuniy foydalanuvchilarini ma'lumotlardan hech qanday to'siqlarsiz foydalanish imkoniyatini ham ta'minlashi lozim. Fayl tizimi himoyaning mustahkamligi va undan foydalanish qulayligi o'rtasida oqilona muvozanat o'rnatilish zarur hisoblanadi. Misol uchun BitLocker yordamida kriptografik himoyalangan xotira qurilmasidagi ma'lumotlarni deshifrlash ko'p hollarda juda murakkab vazifa sanaladi. Fayl tizimini shifrlashining mustahkamligi esa ma'lumotlarni shifrlagan yoki ulardan foydalanish huquqiga ega bo'lgan foydalanuvchi parolining mustahkamligiga bevosita bog'liq jarayon hisoblanadi.

Fayl tizimini xotira qurilmasining turiga moslashtirish ham dolzarb muammolardan sanaladi. Sababi bu xotira qurilmasining xatolik va nosozliklarga yuqori darajada chidamli bo'lishi hamda xizmat muddatining uzayishiga yordam beradi. Qattiq disklar (HDD)da fayl tizimi iloji boricha yuqori tezlikda ishlashi muhim bo'lib, avvalo fayllar bilan ishlash jarayonida ma'lumotlarni o'quvchi mexanizmini (read/write head) ortiqcha harakatlanishini oldini olish orqali erishiladi. Shu tariqa, xotira qurilmasi samarali ishlashi uchun kerakli sharoitlar mavjud bo'lgandagina, qattiq disklar uzoqroq muddat davomida ma'lumotlarni ishonchli saqlab turish imkonini beradi [11].

Xulosa qilib shuni aytish mumkinki SSD disk yoki USB flesh (Flash-karta) kabi axborot tashuvchi xotira qurilmalaridan foydalanish jarayonida asosan ma'lumotlarni har safar bir xil xotira bloklariga yozishni minimallashtirish masalasi birinchi o'ringa ko'tariladi. Hozirgi kunda USB flesh xotira bilan ishlashga moslashtirilgan bir necha fayl tizimlari ishlab chiqilgan. Ammo ushbu turdagi xotira qurilmasining tezligi va samaradorligi jadal sur'atlarda rivojlanayotgani sababli, fayl tizimlarida foydalanilayotgan algoritmlarni tezkorligini biroz pasaytirish hisobiga bo'lsa ham xavfsizlik, ishonchlilik va xatoliklarga bardoshlilikini oshirishga etibor qaratish muhim ahamiyat kasb etmoqda.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

[1] Lai, J.-F., & Heng, S.-H. "Secure File Storage On Cloud Using Hybrid Cryptography" //

Journal of Informatics and Web Engineering, vol. 1, no. 2, Sept 2022, pp. 1-18.

[2] Goswami P.; Faujdar N., Debnath S. “Investigation on storage-level data integrity strategies in cloud computing: classification, security obstructions, challenges and vulnerability” // Journal of Cloud Computing, vol. 13, 2024, pp. 45-51.

[3] Gharib Mohammed, Fazli Mohammad Amin, “Secure cloud storage with anonymous deduplication using ID-based key management” // Journal of Supercomputing, vol. 79, Feb 2023, pp. 2356-2382.

[4] Yi Jiangyi. “The key security management scheme of cloud storage based on blockchain and digital twins” // Journal of Cloud Computing, vol. 13, 2024; pp. 15-20.

[5] Kumar Jaydip, Kumar Hemant, Singh Karam Veer, Saxena Vipin. “Secure Data Storage and Retrieval over the Encrypted Cloud Computing” // International Journal of Computer Network and Information Security, vol. 16, no. 4, 2024, pp. 52-64.

[6] Sharma Pankajeshwara, Govorov Michael, Martin Michael. “A Usable Encryption Solution for File-Based Geospatial Data within a Database File System” // Journal of Cybersecurity and Privacy, vol. 4, no. 2, 2024, pp. 298-323.

[7] Jlil Manal, Jouti Kaoutar, Boumhidi Jaouad, Loqman Chakir. “Improving Traceability in e-Governance File-Sharing Systems: the Moroccan Justice System as a Use Case” // International Journal of Information Security, 2025, pp. 29-33.

[8] Gonburunova V.L., Faizulina A.I. “Prospects for the application of archigraphs in data and knowledge storage systems” // Журнал “Проблемы информационной безопасности. Компьютерные системы”, 2024, pp. 109–139.

[9] Plata I., Panganiban E., Bartolome B. A security approach for file management system using data encryption standard (DES) algorithm. // International Journal of Advanced Trends in Computer Science and Engineering. 8. 2019, pp. 2042-2048. 10.30534/ijatcse/2019/30852019.

[10] Piddubna L. V., Pavlichenko V. M. Information security in electronic document management systems. // Scientific Bulletin of PUET. Series “Economic Sciences”, 4 (95) 2019, pp. 59-66.

[11] Zhang Hao, Li Zhuolin, Shahriar Hossain, Lo Dan. Protecting Data in Android External Data Storage. 2019. pp 924-925. 10.1109/COMPSAC.2019.00143.

**SHAXSIY MA'LUMOTLARNI HIMOYALASHDA MATEMATIK
MODELLASHTIRISHNI ZARURLIGI (MISOLLAR YORDAMIDA)****DSc, profesor B.Z. TO'RAYEV,***O'R MV Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti***B.N. MIRZOODILOV, O.S. MIRZAMURODOV***Toshkent Davlat Iqtisodiyot universiteti*

Annotatsiya. Raqamli texnologiyalarning jadal rivojlanayotgan sharoitda shaxsiy ma'lumotlar xavfsizligini ta'minlash masalasi alohida dolzarblik kasb etmoqda. Zamonaviy axborot tizimlari katta miqdordagi shaxsiy ma'lumotlarni, jumladan identifikatsiya, biometrik, tibbiy va boshqa nozik ma'lumotlarni qayta ishlaydi. Bunday ma'lumotlarning maxfiylikni buzish jiddiy oqibatlariga, shu jumladan foydalanuvchining ishonchini yo'qotish, moliyaviy yo'qotishlar va huquqiy sanksiyalar olib kelishi mumkin.

Kalit so'zlar: Shaxsiy ma'lumotlar, kompyuterlar, Tahdid va buzuvchi modeli, Markov zanjiri. Matematik modellash.

Abstract. In the context of the rapid development of digital technologies, the issue of ensuring the security of personal data is becoming particularly urgent. Modern information systems process a large amount of personal data, including identification, biometric, medical and other sensitive data. Violation of the confidentiality of such data can lead to serious consequences, including loss of user trust, financial losses and legal sanctions.

Keywords: Personal data, computers, Threat and attacker model, Markov chain. Mathematical modeling.

Rossiya Federatsiyasining "Shaxsiy ma'lumotlar to'g'risida" No152-FZ-sonli Federal qonuni va Evropa Ittifoqining "Ma'lumotlarni himoya qilish to'g'risida"gi umumiy nizomi (GDPR) kabi shaxsiy ma'lumotlar to'g'risidagi qonunchilik, shaxsiy ma'lumotlarni to'plash, saqlash, qayta ishlash va himoya qilishga qat'iy talablarni o'rnatadi. Amalda esa ushbu talablarni qondirish juda qiyin, ayniqsa doimo o'zgarib turadigan tahdidlar qarshisida. Yevropa Ittifoqi – Ma'lumotlarni Muhofaza qilish bo'yicha umumiy nizom (GDPR). AQSh - yagona qonun yo'q, sohaga oid qonunlar qo'llaniladi: HIPAA (sog'liqni saqlash), CCPA (Kaliforniya) va boshqalar.

Ushbu ishning maqsadi zamonaviy tahdidlar, axborot tizimlari ishlashining xususiyatlari, shuningdek amaldagi qonunchilik talablarini hisobga olgan holda shaxsiy ma'lumotlarni qayta ishlashda axborot xavfsizligini ta'minlash modelini ishlab chiqishdan iborat.

Tadqiqot obyekti informatsion tizimlarda shaxsiy ma'lumotlarni qayta ishlash jarayoni hisoblanadi. Tadqiqot mavzusi shaxsiy ma'lumotlarni ruxsatsiz kirish, ruxsatsiz tarqalishi, buzish va yo'q qilishdan himoya qilish usullari va vositalaridir.

Ishning ilmiy yangiligi xavflarning keng qamrovli modelini va zamonaviy raqamli platformalar sharoitiga moslashtirilgan himoya tizimini ishlab chiqishdan iborat.

Tadqiqotning amaliy ahamiyati shundaki, shaxsiy ma'lumotlarni qayta ishlovchi tashkilotlarda himoyalangan axborot tizimlarini loyihalashtirishda ishlab chiqilgan modelni qo'llash imkoniyatiga bog'liq.

O'zbekiston Respublikasining shaxsiy ma'lumotlar to'g'risidagi qonuni Qonunchilik palatasi tomonidan 2019 yil 16 aprelda qabul qilingan. Senat tomonidan 2019 yil 21 iyunda ma'qullangan. O'zbekiston Respublikasining "shaxsiy ma'lumotlar to'g'risida" gi qonunga o'zgarishlar 2021 yil 14 yanvarda qabul qilingan. Uning asosiy maqsadi shaxsiy ma'lumotlarni qayta ishlash va himoya qilish sohasidagi munosabatlarni tartibga solishdir. 2021-yil 16-apreldan kuchga kirgan va ma'lumotlar bilan bog'liq barcha munosabatlarni qamrab oladi. Qonun 7 ta bob va 37 ta moddadan iborat.

Ushbu Qonunning amal qilishini shaxsga doir ma'lumotlarga ishlov berish va ularni ximoya qilish chog'ida qo'llaniladigan ishlov berish vositalaridan, shu jumladan axborot texnologiyalaridan qat'iy nazar yuzaga keladigan munosabatlarga nisbatan tatbiq etiladi [1].

Ushbu Qonun 2019 yil 1 oktyabrdan e'tiboran kuchga kirgan. "Shaxsiy ma'lumotlar to'g'risida" qonun talablari kuchga kirishi munosabati bilan shaxsiy ma'lumotlarni qayta ishlash bo'yicha axborot tizimlarini ushbu qonun talablariga muvofiqlashtirish muammosi barcha tashkilotlar uchun dolzarbdir. Davlat va xususiy mulk shakli bilan ushbu qonun talablarini bajarish uchun hal qilinishi kerak bo'lgan asosiy muammolardan biri bu shaxsiy ma'lumotlarni o'z vaqtida yo'q qilish uchun saqlanadigan va qayta joylashtirilgan axborot tizimining xavfsizligiga dolzarb tahdidlarni aniqlashdir. Yuqoridagilar ushbu tadqiqotlari mavzusining dolzarbligini belgilaydi.

O'rganilayotgan muammoning rivojlanish darajasi. Xavfsizlikka tegishli tahdidlarni aniqlash, ya'ni amalga oshirish ehtimoli yuqori bo'lgan va ular shaxsiy ma'lumotlar uchun xavfli bo'lgan tahdidlar nafaqat Qonunchilik talablarini rasmiy bajarish uchun, balki turli vazirlik va idoralar bo'linmalarida ishlatiladigan axborot tizimlari uchun ayniqsa dolzarb bo'lgan zarur va yetarli himoya darajasini aniqlash uchun ham zarurdir. Bu shaxsiy ma'lumotlarni o'z ichiga olgan katta ma'lumotlar to'plami va tizimga ko'plab foydalanuvchilarga kirishni ta'minlash zarurati bilan bog'liq.

Shaxsiy ma'lumotlarni qayta ishlashning yirik axborot tizimlari (Ispdn) xavfsizligiga dolzarb tahdidlarni aniqlash muammosi so'nggi paytlarda xavfsizlik bo'yicha mutaxassislar tomonidan faol muhokama qilinmoqda, ammo ilmiy nashrlarda kam aks ettirilgan.

Shaxsiy ma'lumotlar-bu shaxsni to'g'ridan-to'g'ri yoki bilvosita aniqlaydigan va tavsiflaydigan har qanday ma'lumot. Ushbu shaxsiy ma'lumotlar iste'molchilarga, ishdagi hamkasblarimizga, biznes sheriklarimizga yoki boshqa uchinchi shaxslarga tegishli bo'lishi mumkin. Shaxsiy ma'lumotlarni himoya qilish-bu odamlarning shaxsiy ma'lumotlari qanday va nima uchun to'planishi va qayta ishlanishini bilish va ta'sir qilish huquqi. Bundan tashqari, biz biznes yuritadigan deyarli hamma joyda shaxsiy ma'lumotlarni himoya qilish to'g'risidagi qonunlar mavjud. Ushbu qonunlarga rioya qilmaslik kompaniyaga ham, individual xodimlarimizga ham jarimalar, qonuniy choralar yoki jinoiy javobgarlikka olib kelishi mumkin. Sub'yekt o'zining shaxsga doir ma'lumotlarini berishni rad qilgan taqdirda, o'zining rad qilish saboblarini ko'rsatmaslik huquqiga ega [1].

Shaxsiy ma'lumotlar bilan ishlash tartibini buzish, shuningdek, ishbilarmonlik obro'sini yo'qotish bilan tahdid qiladi. Bunday faktlarni aniqlash kompaniya ko'pincha mijozlarning chiqib ketishiga sabab bo'ladi. Bu shuni anglatadiki, ShM (Shaxsiy ma'lumotlar) sohasini tartibga soluvchi va nazorat qiluvchi tuzilmalar ko'rsatmalariga rioya qilish shaxsiy ma'lumotlar bilan bevosita yoki bilvosita ishlaydigan har bir kompaniya uchun hayotiy zaruratdir.

Shaxsga doir ma'lumotlar to'g'risidagi qonun hujjatlarni buzganlikda aybdor shaxslar belgilangan tartibda javobgar bo'ladi [1].

Regulyatorlar nazorati ostida bo'lgan barcha tashkilotlar tomonidan talablarni bajarishga universal yondashuv mavjud emas. Eng murakkab va qimmat jarayon – bu sub'ektning irqi va millati, e'tiqodi, sog'lig'i, samimiy hayoti, siyosiy va falsafiy qarashlari to'g'risidagi ma'lumotlarni qayta ishlaydigan shaxsiy ma'lumotlar axborot tizimining xavfsizligini ta'minlashning to'liq kompleksini joriy etish. Qonun ushbu toifadagi ma'lumotlarni himoya qilishni ayniqsa ehtiyotkorlik bilan ta'minlashni talab qiladi.

Xavfsizlik va biometrik ma'lumotlar bazasini ta'minlash uchun qonun talablari yuqori: ma'lumotlar mavzusini aniqlashga imkon beradigan biologik va fiziologik xususiyatlar. To'liq ismi, tug'ilgan sanasi va joyi, uy manzili, kasb to'g'risidagi ma'lumotlar, aloqa ma'lumotlarini qayta ishlash uchun mijozning yozma roziligini olgan kompaniya ommaviy ShM (Shaxsiy ma'lumotlar) operatoriga aylanadi. Bunday ma'lumotlar, masalan, telefon kataloglarini tuzish uchun ishlatiladi. Umumiy shaxsiy ma'lumotlarni himoya qilish uchun Qonunchilik boshqa toifalarga nisbatan minimal talablarni qo'yadi.

Shaxsiy ma'lumotlarni himoyalashda nega matematik modellash tirish zaruriy omil.

Modellashtirish murakkab tizimlarning xatti-harakatlarini o'rganishning asosiy usuli hisoblanadi[2]. "Modellashtirish-bu bilishning asosiy usullaridan biri, bu haqiqatni aks ettirish shakli bo'lib, u boshqa ob'ektlar, jarayonlar, hodisalar yordamida yoki mavhum tavsif yordamida haqiqiy ob'ektlar, ob'ektlar va hodisalarning ba'zi xususiyatlarini aniqlash yoki ko'paytirishdan iborat".

"Model" deganda bilish, tahlil qilish jarayonida haqiqiy ob'ektni (yoki tizimni) almashtiradigan, shu bilan birga uni o'rganish uchun eng muhim xususiyatlarning bir qismini saqlab turadigan va uni o'rganish bizga ob'ekt haqida yangi ma'lumotlarni beradigan aqliy tasavvur qilingan yoki moddiy jihatdan amalga oshirilgan tizim" tushuniladi[3].Turli jarayonlar va tizimlarni tavsiflash uchun amalda qo'llaniladigan bir nechta asosiy model turlari mavjud [4]:

- kontseptual model-tizimni maxsus belgilar, belgilar, ulardagi operatsiyalar yoki tabiiy yoki sun'iy tillardan foydalangan holda tavsiflovchi model;

- jismoniy model-simulyatsiya qilingan tizim hodisalarning o'xshashligidan kelib chiqadigan o'xshashlik nisbati asosida takrorlanadi;

- strukturaviy va funktsional-sxemalar (oqim diagrammalari), diagrammalar, grafikalar, jadvallar, ularni birlashtirish va o'zgartirish uchun maxsus qoidalarga ega chizmalar model sifatida ishlatiladi;

- matematik model-bu voqelikning matematik tasviri, hodisalarni tavsiflash, matematik tushunchalar, ramziylik yordamida tizim;

- simulyatsiya modeli-elektron kompyuterlar (kompyuterlar) yordamida tizimlar yoki hodisalarni eksperimental o'rganish jarayonida qo'llaniladigan iqtisodiy va matematik model.

Tizimlarni o'rganishda ushbu modellash tirish turlari mustaqil ravishda yoki bir vaqtning o'zida bir nechta qo'llanilishi mumkin, bundan tashqari, simulyatsiya simulyatsiyalaridan foydalanganda, u yoki bu darajada, yuqorida sanab o'tilgan barcha modellash tirish turlari yoki ularning alohida usullari qo'llaniladi. Bundan tashqari, simulyatsiya modeli dinamikada yakuniy yoki oraliq natijani vizual ravishda taqdim etishga imkon beradi, bu uning rivojlanishida ishtirok etmagan shaxslar tomonidan olingan natijalarni muvaffaqiyatli tushunish uchun muhim jihatdir.

Zamonaviy adabiyotda simulyatsiya modellash tirishning yagona ilmiy ta'rifi mavjud emas [5]. Shunday qilib simulyatsiya "kompyuterda vaqt o'tishi bilan ishlaydigan murakkab haqqoniy tizim modelini yaratish va tizimning xatti-harakatlarini tushunish yoki ma'lum bir tizimning ishlashini ta'minlaydigan turli strategiyalarni baholash maqsadida ushbu model ustida tajribalar o'tkazish jarayoni" deb ta'riflanadi. Murakkab tizimlarni ishlab chiqishda eng kuchli tahlil vositalaridan biri va ularning ishlash jarayonlarini tahlil qilish, simulyatsiya modellash tirish ilmiy tadqiqot usuli sifatida turli xil jarayonlar yoki operatsiyalarni taqlid qilish uchun kompyuter texnologiyalaridan foydalanishni o'z ichiga oladi"[6]. Modellashtirish, simulyatsiya tizimning xatti-harakatlari to'g'risida kerakli ma'lumotlarni to'plash usuli sifatida ko'rib chiqiladi, uning kompyuterlashtirilgan modelini yaratish orqali- "analitik yechimlar asosida yoki raqamli usullar yordamida tuzilgan muammoning aniq raqamli echimlarini olish usuli" sifatida [7]. I.A.Shuvalov maqolalarida ichki va tashqi tahdidlarning axborotga ta'sirining matematik modeli taklif etiladi tizimida yo'l harakati xavfsizligi davlat inspeksiyasi axborot resurslarini keltiradi. Davlat xavfsizlik inspeksiyasi xodimlarining xizmat faoliyatida Rossiya Ichki ishlar vazirligining Krasnodar o'lkasi bo'yicha bosh boshqarmasi. Axborot tizimining ikki matematik modelini yaratish jarayoni bosqichma-bosqich tavsiflanadi:

- a) uzluksiz vaqtga ega Markov zanjiri;

- b) diskret daqiqalarga ega Markov zanjiri yordamida[8].

Kompyuter texnologiyalaridan foydalanish, masalan, statistik jihatdan olingan dastlabki ma'lumotlarga ega bo'lgan holda, kerakli natijalarni hisoblashni avtomatlashtirishga imkon beradi. Bu, ayniqsa, ko'plab tug'unlardan tashkil topgan murakkab tizim ko'rib chiqilganda to'g'ri keladi chunki qoida tariqasida, kerakli natijalarni hisoblash uchun noqulay formulalarni qo'llash kerak.

Simulyatsiya modellashtirish turli xil tizimlarning, shu jumladan axborotning xatti-harakatlarini o'rganish uchun ishlatiladi. Asosan, axborot tizimlarini modellashtirishda maqsad haqida ma'lumot olishdir. Arizani qayta ishlash vaqti, har qanday resursning yuk darajasi va boshqalar. Biroq, shaxsiy ma'lumotlarni qayta ishlashning axborot tizimining xatti-harakatlarini o'rganish uchun simulyatsiya modellashtirishdan foydalanish hozirgi kungacha keng ko'rib chiqilmagan.

NATIJALAR

Tahdid va buzuvchi modeli

Tahdid turlari:

1. Shaxsiy ma'lumotlarning ruxsatsiz chiqib ketishi – buzilish, xodimlarning xatosi, kirishni boshqarishning yo'qligi tufayli.
2. Ruxsatsiz kirish - bu tajovuzkorning ichki resurslarga kirib borishi.
3. Ma'lumotlarni buzish – sabotaj, manipulyatsiya maqsadida axborotni o'zgartirish.
4. Qasddan yoki tasodifiy bo'lgan ma'lumotlarni o'chirish yoki yo'q qilish.
5. Xizmatni rad etish - tizimning mavjudligining uzilishi.

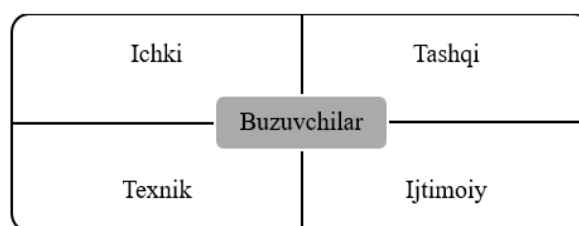
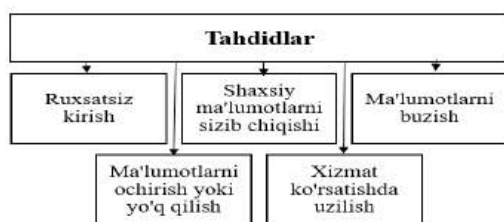
1-jadval

Buzuvchi modeli

Tur	Xususiyatlari	Misollari
Ichki	Huquqiy kirish huquqiga ega, ammo undan vijdotsiz xodimga zarar keltiradi	vijdotsiz xodim
Tashqi	Kirish huquqi yo'q, tizimga tashqaridan kiradi	xaker, raqobatchilar
Texnik	Tahdid apparat buzulishi tufayli yuzaga keladi	dasturiy ta'minot apparat xatolari
Ijtimoiy	inson omilidan foydalanish	phishing, aldash

Asosiy qarshi choralar:

- Kirishni boshqarish (RBAC / ACL)
- Ma'lumotlarni shifrlash (diskda va tranzitda)
- Faoliyatni nazorat qilish va hisobga olish
- DLP (ma'lumotlarning ruxsatsiz chiqishining oldini olish) tizimlari
- Xodimlarni tayyorlash



1-rasm. Tahdid va buzuvchi modeli

2-jadval

Shaxsiy ma'lumotlarga tahdidlar

№	Tahdid	Tahdid manbasi (tajovuzkor)	Sodir bo'lishi mumkin bo'lgan oqibatlar	Himoya qilish choralari
1	Shaxsiy ma'lumotlarning ruxsatsiz chiqib ketishi	Ichki, Tashqi	Maxfiylikni buzish, jarima, obro'sini yo'qotish	Shifrlash, kirishni boshqarish, DLP tizimlari

№	Tahdid	Tahdid manbasi (tajovuzkor)	Sodir bo'lishi mumkin bo'lgan oqibatlar	Himoya qilish choralari
2	Ruxsatsiz kirish	Tashqi, ichki	Maxfiy ma'lumotlarga kirish uchun ruxsat, uni buzish yoki o'chirish	Authentication, kirish jurnallari, IDS / IPS
3	Ma'lumotlarning buzilishi	Ichki, texnik	Tizimdagi nosozliklar sababli ishonchli ma'lumotlarning yo'qolishi	Butunligini nazorat qilish, zaxiralash
4	Ma'lumotlarni o'chirish yoki yo'q qilish	Ichki, texnik	Axborotni yo'qotish, zaxiralashni tiklashning imkoni yo'qligi	Huquqlarning farqlanishi, o'chirishdan himoya qilish
5	Xizmatdan bosh tortish (DoS)	Tashqi, texnik	Tizimga kirishning mavjud emasligi, ma'lumotlarni qayta ishlashni to'xtatib turish	xavfsizlik devorlari, DDoSga qarshi, zaxira imkoniyatlari
6	Ijtimoiy muhandislik	Ijtimoiy	Loginlar, parollar, kirish huquqlarining ijtimoiy o'g'irlanishi	Xodimlarni o'qitish, phishing filtrlari, 2FA

Ichki tahdidlarning Markov modellari ([11-12])

Rosenko va boshqalarning ishi ichki tahdidlarning maxfiy ma'lumotlar xavfsizligiga ta'sirini baholash uchun Markov modellaridan foydalanadi.

Markov modellarini qo'llash:

1. Ichki tahdidlarning ta'sirini baholash: Tadqiqotlar ichki tahdidlarning (IT) muxim ma'lumotlar xavfsizligiga (MX) ta'sirini baholash uchun Markov tasodifiy jarayonlaridan foydalanish bilan bog'liq muammolarni ko'rib chiqadi. Ushbu modellar turli xil ichki tahdidlar bilan bog'liq xatarlarni rasmiylashtirish va hisoblashga yordam beradi

2. Matematik modellar: Ishlarda ichki tahdidlar ta'siri ostida tizimning bir holatdan ikkinchisiga o'tishini tahlil qilish imkonini beruvchi matematik model taqdim etilgan. Bunday modellar ham mustaqil, ham qaram tahdidlarni, shuningdek ularning avtomatlashtirilgan axborot tizimlari (AAT) ishlashiga ta'sirini hisobga oladi.

3. Simulyatsiya modellashtirish: Tadqiqot nozik ma'lumotlarning xavfsizligini baholash uchun simulyatsiya usullarini qo'llashni o'z ichiga oladi. Bu ichki tahdidlarning ta'siri senariylarini yanada moslashuvchan tahlil qilishga imkon beradi va xavflarni minimallashtirish uchun asosli qarorlar qabul qiladi.

- ATShM ning zaif holatlarga o'tish ehtimollarini modellashtirish;

- Tahdidni qaytarishning muvaffaqiyati yoki muvaffaqiyatsizligini hisobga olish;

- O'tish ehtimollari matritsasi "yutuvchi holat" ga qadar quriladi.

Ichki tahdidlarga tizim turg'unligining taxlili (masalan, xodimlarning xatti-harakatlariga chidamliligini tahlil qilish) muhimdir.

Markov jarayoni asosida modelni yaratish

Aytaylik, tizim ,balkim $S = \{x_0, x_1, x_2, \dots, x_n, x_{n+1}\}$ holatdir , bu yerda:

x_0 – boshlang'ich xavfsiz holat;

$x_1, x_2, \dots, x_n$ — har biri amalga oshirilgandan keyin n tahdidlar;

x_{n+1} - yutilish holati (tanqidiy tahdidni anglash).

O'tishlar:

$P_{i,i} = R_i$ – tahdidni muvaffaqiyatli qaytarish ehtimoli;

$P_{i,n+1} = 1 - R_i$ – tahdidni qaytaraolmaslik ehtimoli.

O'tish matritsasi tuziladi:

$$P = \begin{bmatrix} q_0 & q_1 & \dots & q_n & 0 \\ 0 & R_1 & \dots & 0 & 1 - R_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & R_n & 1 - R_n \\ 0 & 0 & \dots & 0 & 1 \end{bmatrix}$$

Bu yerda: q_i – i -chi tahdidning paydo bo'lish ehtimoli; R_i – uni muvaffaqiyatli qaytarish ehtimoli; x_{n+1} – tahdidni amalga oshirish holatiga o'tish (shaxsiy ma'lumotlarning yo'qolishi, sizib chiqish va h.k.). Zaif holatga tushib qolish ehtimolini baholash. bu yerda k – qadam

$$P_i^{(k)} = \sum_{j=0}^n P_j^{(k-1)} \cdot P_{ji}$$

Excel, Python, Matlablarda raqamli tajriba o'tkazish mumkin — 3-5 qadamda agar q_i, R_i berilgan tizimning x_{n+1} ga o'tish ehtimolini hisoblash mumkin. Bu barqarorlikning miqdoriy bahosini beradi.

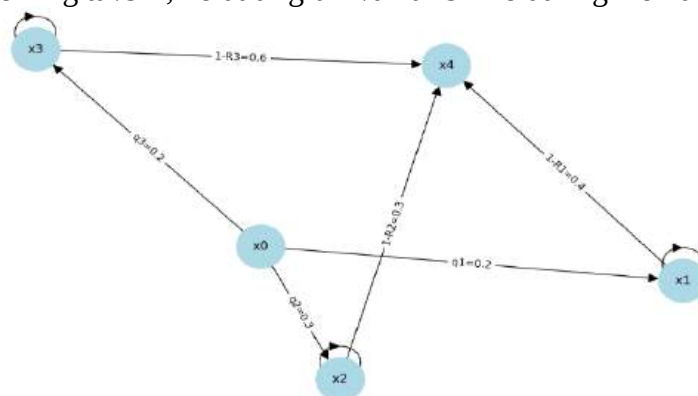
3-jadval

Namuna qiymatlar

N ^o - tahdid	Tahdid	q_i	R_i
1	Fleshka orqali ma'lumotning tarqalishi	0,2	0,6
2	Email-pochta orqali virus	0,3	0,7
3	Wi-Fi orqali NTD	0,2	0,4

ATShMning ichki tahdidlarga chidamliligini baholashning matematik modeli

Ichki tahdidlar ta'sirida shaxsiy ma'lumotlar axborot tizimi (ShMAT) modeli (o'tish grafi) sxemasi. Hujjatda modelning tavsifi, holatlar grafi va har bir holatning izohlari jadvali mavjud.



2-rasm. O'tish grafi:

Model holatlatining izohi

Quyidagi jadvalda ATShM ning o'tish modelidagi har bir holatning ma'nosi tushuntiriladi:

x_0 – boshlang'ich (xavfsiz) holat

Bu quyidagi holatlarda axborot tizimining normal holati hisoblanadi:

O'R MV AKT VA ALOQA HARBIY INSTITUTI

- himoya normal ishlaydi;
- tahdidlar hali amalga oshmadi;
- ShM buzilmaydi.

4-jadval

Tizim yoqilgan, ma'lumotlar himoyalangan va tahdidlar yo'q.

Holati	Tavsifi	Amaliy tadqiqotlar
x_0	Boshlang'ich xavfsiz holat	Tizim normal ishlaydi, tahdidlar yo'q
x_1	1-tahdid aniqlandi	Kodlanmagan flesh-uskuna qo'shildi
x_2	2-tahdid aniqlandi	Zararli(virusli) elektron pochta qabul qilindi
x_3	3- tahdidi aniqlandi	Wi-Fi ulanishga urinish
x_4	Muhim holat (tahdidni amalga oshirish)	ShM o'g'irlash yuz berdi

Ushbu holatlarda tizim hali ham R_1 , R_2 , R_3 ehtimolligi bilan tahdidni qaytarishi mumkin. Agar muvaffaqiyatli bo'lsa, u o'sha holatda qoladi. Agar yo'q bo'lsa, u x_4 ga ketadi. x_4 - yutuvchi (kritik) holat

Bu tahdidni amalga oshirish holati. Bu singdiradi, chunki:

- tizim zaif holatga o'tdi, ma'lumotlar buzildi;
- undan chiqish amaldagi model doirasida ko'zda tutilmagan;
- hodisalarga javob berish, tiklashni va tekshiruvni talab qiladi.

Misol: Virus ma'lumotlar bazasiga kirishga kirishdi yoki ShM elektron pochta orqali tashqariga yuborildi.

Tizim holatga qarab qanday harakat qiladi.

- Boshlash: x_0
- Ehtimollar bilan q_1 , q_2 , q_3 lar x_1 - x_3 lardan biriga o'tadi

U yerda yoki:

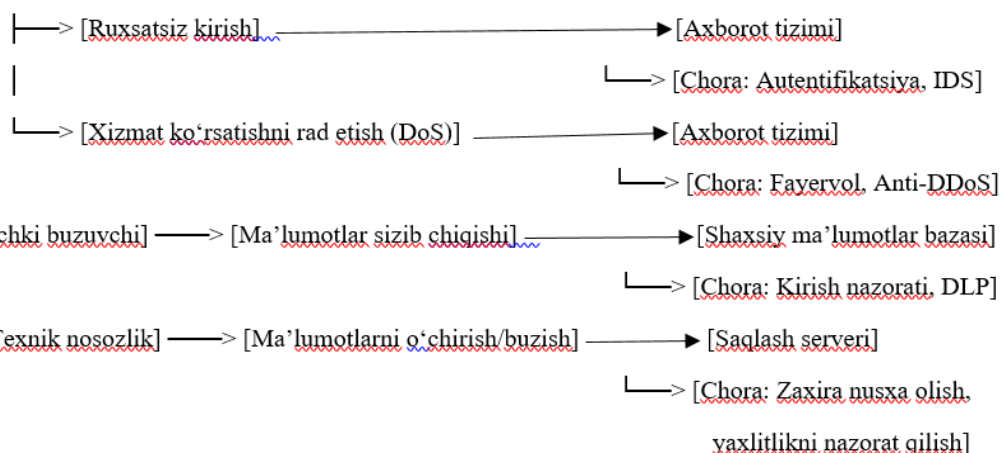
- tahdidni qaytaradi (bu holatda qoladi),
- yoki qaytara olmaydi $\rightarrow x_4$ ga o'tadi

Nima uchun bizga bunday holatlar kerak?

Ular sizga quyidagi xavflarni rasmiy ravishda modellashtirishga imkon beradi:

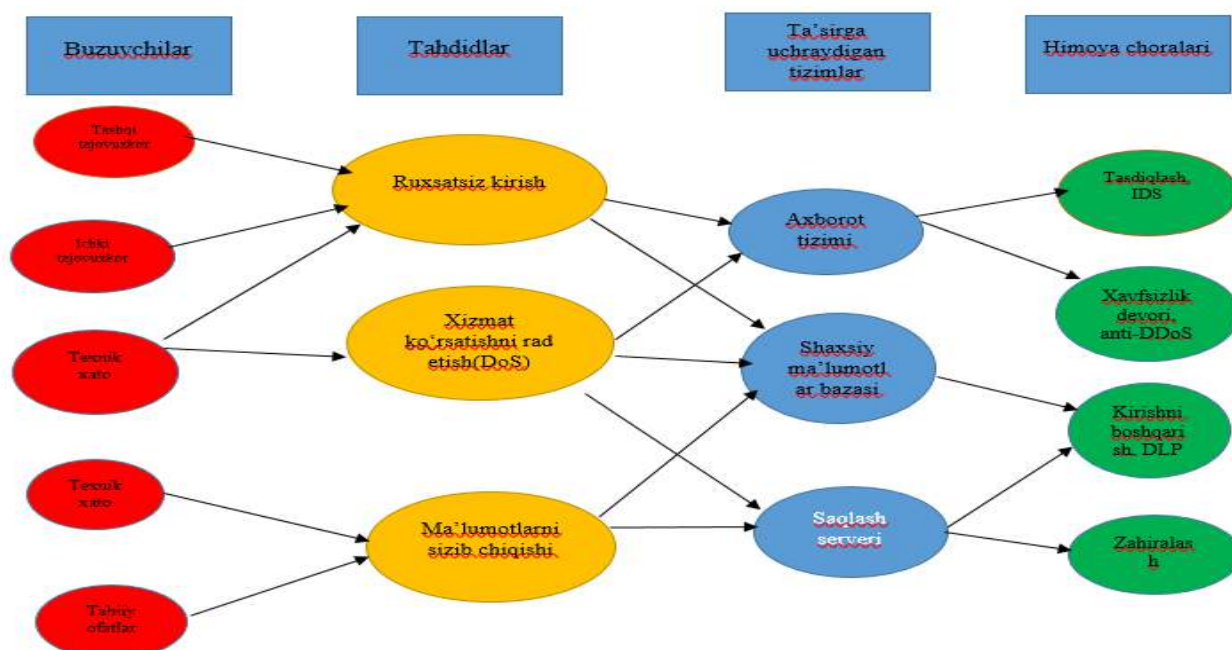
- x_4 -ga o'tish ehtimolini tushunish;
- turli himoya choralarining samaradorligini solishtirish (R ning ortishi)
- tizimning qanchalik tez buzilishi mumkinligini taxmin qilish.

[Tashqi buzuvchi]



3-rasm. Graf tuzulmasi

Xar qanday buzuvchi (u tashqimi, ichkimi, texnik, ijtimoiy) bir yoki bir nechta tahdidlarni amalga oshiradi. Tahdidlar aktivlarga ta'sir qiladi: ma'lumotlar bazalari, AT, foydalanuvchilar. Har bir tahdid uchun bir qator chora-tadbirlar qo'llaniladi, ular tahdidni "zararsizlantirish" qirralar sifatida ifodalanadi.



4-rasm. Yo'naltirilgan graf

Ushbu grafni yo'naltirilgan graf sifatida modelni keltirish mumkin

$$G=(V,E), \quad V=A \cup T \cup S \cup M,$$

Bu yerda A – qoidabuzarlar to'plami, T - Tahdidlar to'plami, S - aktivlar to'plami, M - bu himoya choralari to'plami.

Qovurg'alar

$$E \subseteq (A \times T) \cup (T \times S) \cup (T \times M).$$

Qovurg'alarga qo'shimcha masulyatni yuklash mumkin:

- Muvaffaqiyatli hujum ehtimoli $p(a \rightarrow t)$,
- Tahdidni muvaffaqiyatli amalga oshirish natijasida zarar $d(t \rightarrow s)$,
- Chora-tadbirning samaradorligi $e(t \rightarrow m)$.

XULOSA

1.Hujum yo'llarini tahlil qilish.

Barcha yo'naltirilgan oddiy yo'llarni qurib, "buzuvchi $\rightarrow \dots \rightarrow$ aktiv", biz har bir tizim qaysi tahdid zanjirlari orqali xavf ostida ekanligini ko'ramiz.

2.O'lchovlarning ustuvorligini belgilash.

Masulyatni hisobga olgan holda (tavakkal = ehtimollik $\times$ zarar) qaysi choralar eng muhim himoya qiluvchi tanqidiy senariylar ekanligini aniqlash mumkin.

3.Kengaytma.

"Ijtimoiy muhandis" va "phishing", "pretexting" tahdidlarini qo'shing.

Qo'shimcha aktivlarni kiriting: tarmoq, ishchi stantsiyalar, foydalanuvchilar.

O'lchovlar o'rtasida bog'liqlikni joriy eting: masalan, TAT kuchli autentifikatsiya mavjud bo'lganda samarali bo'ladi. Graf qatlamlari rollarni aniq ajratadi (buzuvchi $\rightarrow$ tahdid $\rightarrow$ aktiv $\rightarrow$ o'lchovi). Yo'naltirilganlik sizga hujumning sabab-natija yo'lini kuzatish imkonini beradi. Himoya

O'R MV AKT VA ALOQA HARBIY INSTITUTI

chorasi to'g'ridan-to'g'ri aktivga emas, balki zararsizlantiradigan o'ziga xos tahdidga "yopishadi". Bunday model vizuallashtirish, xavflarni hisoblash va himoya mexanizmlari majmuini rejalashtirish uchun qulaydir.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

[1] Shaxsga doir ma'lumotlar to'g'risida O'zbekiston Respublikasining Qonuni, 02.07.2019 yildagi O'RQ-547-son

[2] Лычкина Н.Н. Имитационное моделирование экономических процессов. Учебное пособие для слушателей программы eMBI / Н.Н. Лычкина. - М.: Академия АйТи, 2005. - 96 с.

[3] Мамаева З.М. Введение в моделирование / З.М. Мамаева. - Н. Новгород, ННГУ, 2005. - 120 с.

[4] Бахвалов Л.А. Компьютерное моделирование: долгий путь к сияющим вершинам / Л.А. Бахвалов // Компьютерра. - 1997. - № 40. - С.26-36.

[5] Шеннон Р. Имитационное моделирование систем - искусство и наука. / Р. Шеннон. — М.: Мир, 1978.

[6] Таха. Введение в исследование операций. Пер. с англ. / Таха, А. Хемди. - 7-е издание. — М.: Издательский дом "Вильямс", 2005. — 912 е.:

[7] Муха В. С. Вычислительные методы и компьютерная алгебра: учеб.-метод. Пособие / В.С. Муха. — 2-е изд., испр. и доп. — Минск: БГУИР, 2010.- 148 с.: ил.

[8] Шувалов И.А., Математическая модель воздействия угроз на информационную систему обработки персональных данных / Шувалов И.А., Семенчин Е.А. // Фундаментальные исследования. - 2013. - № 10. - Часть 3. -С. 529-533.

[9] Росенко, А.П. «Математическое моделирование влияния внутренних угроз на безопасность конфиденциальной информации, циркулирующей в автоматизированной информационной системе» / А.П. Росенко // Известия Южного федерального университета. Технические науки. – 2008. – Вып. 8. – С. 71–81.

[10] Расенко А.П. Теоретические основы анализа и оценки влияния внутренних угроза на безопасность конфиденциальной информации: Монография. М.:Гелиос АРВ. 2008. 154 с.

OQIMLI SHIFRLARNI KRIPTOTAHILLASH USULLARI

f-m. f.d., professor G.U. JURAYEV, Sh.S. ANVAROV
Mirzo Ulug'bek nomidagi O'zbekiston Milliy Universiteti

Annotatsiya. Ushbu maqolada oqimli shifrlarning mohiyati, ularning ishlash mexanizmlari hamda kriptotahlilga qarshi zaifliklari o'rganiladi. Oqimli shifrlar, ayniqsa real vaqtli axborot uzatishda keng qo'llaniladi, bu esa ularni tahlil qilishni muhim qiladi. Maqolada LFSR (Linear Feedback Shift Register), RC4 kabi mashhur oqimli shifrlar tahlil qilinadi. Kriptotahlilning asosiy usullari sifatida statistik tahlil, vaqtga asoslangan tahlil va nolinearlikdan foydalanish holatlari ko'rib chiqiladi. Oqimli shifrlar ustida olib borilgan hujumlar, xususan, differensial kriptotahlil, algebraik hujumlar va korrelyatsion hujumlar misollar bilan ko'rsatilgan. Tadqiqot natijalari shuni ko'rsatadiki, oqimli shifrlar yuqori tezlikda ishlovchi tizimlar uchun maqbul bo'lsa-da, ularning xavfsizligini ta'minlash uchun chuqur matematik model kerak. Maqola davomida kriptotahlil uchun mo'ljallangan simulyatsion modellar ham keltirilgan. Zamonaviy kriptografik tizimlar oqimli shifrlarni ishlatishda ehtiyotkorlik talab qiladi. Shuningdek, maqolada xorijiy va mahalliy tadqiqotlar solishtirma tahlil asosida ko'rib chiqilgan. Xulosa sifatida, kriptotahlil metodlarini chuqur o'rganish orqali yangi, barqarorroq oqimli shifrlar yaratish imkoniyati tahlil qilinadi.

Kalit so'zlar: oqimli shifr, kriptotahlil, LFSR, RC4, statistik hujum, algebraik hujum, korrelyatsion hujum, differensial kriptotahlil, oqim generatori, real vaqtli shifrlash, matematik model, simulyatsiya, xavfsizlik tahlili, kalit uzunligi, shifrlash tezligi, nonce, sinxronlashgan shifrlash, kriptografik mustahkamlik, kombinatsiyalangan oqimlar, xavfsizlik algoritmi.

Аннотация. В данной статье рассматривается природа потоковых шифров, их архитектура и уязвимости к криптоанализу. Потоковые шифры широко используются в системах передачи данных в реальном времени, что делает их важным объектом анализа. Описаны известные алгоритмы, такие как LFSR и RC4, с указанием их слабых мест. Основные методы криптоанализа включают статистический анализ, тайминговые атаки и использование нелинейных свойств. Показаны примеры атак, таких как дифференциальный криптоанализ, алгебраические и корреляционные атаки. Результаты исследования показывают, что потоковые шифры подходят для высокоскоростных систем, но требуют строгого математического подхода для обеспечения безопасности. В статье приведены симуляционные модели, используемые при анализе устойчивости. Также рассмотрены зарубежные и отечественные исследования с их сравнительным анализом. Подчеркивается необходимость осторожного применения потоковых шифров в современных криптосистемах. В заключении авторы делают вывод о целесообразности разработки новых, более устойчивых потоковых алгоритмов на основе изученных методов криптоанализа.

Ключевые слова: потоковый шифр, криптоанализ, LFSR, RC4, статистическая атака, алгебраическая атака, корреляционная атака, дифференциальный криптоанализ, генератор ключевого потока, шифрование в реальном времени, математическое моделирование, симуляция, анализ безопасности, длина ключа, скорость шифрования, начальный вектор (nonce), синхронное шифрование, криптографическая стойкость, комбинированные потоки, алгоритмы защиты.

Abstract. This article explores the fundamentals of stream ciphers, their operating principles, and their vulnerabilities to cryptanalysis. Stream ciphers are widely used in real-time communication systems, making their analysis crucial for security. Popular algorithms like LFSR and RC4 are examined in detail, with emphasis on their structural weaknesses. Key cryptanalytic methods discussed include statistical analysis, timing attacks, and exploitation of nonlinearity. Examples such as differential cryptanalysis, algebraic attacks, and correlation attacks are provided. Research findings indicate that while stream ciphers are suitable for high-speed systems,

ensuring their security requires rigorous mathematical modeling. The paper also presents simulation models designed for evaluating cipher resilience. A comparative overview of international and local research is included to contextualize the findings. The importance of cautious application of stream ciphers in modern cryptosystems is emphasized. In conclusion, the article suggests that deep exploration of cryptanalytic techniques can lead to the development of more robust stream cipher designs.

Key words: stream cipher, cryptanalysis, LFSR, RC4, statistical attack, algebraic attack, correlation attack, differential cryptanalysis, keystream generator, real-time encryption, mathematical model, simulation, security analysis, key length, encryption speed, nonce, synchronous ciphering, cryptographic strength, combined keystreams, security algorithm.

Oqimli shifrlash algoritmlarining kriptotahlili foydalanilgan kalitni topishda algoritmda foydalanilgan loyihani buzishga asoslanadi. Buning natijasida, esa ushbu kalitdan foydalanib shifrlangan butun seans ma'lumotlarini qo'lga kiritish mumkin bo'ladi. Xususan, passiv hujumlar algoritmi chiqishidagi yoki boshlanish/ qayta sinxronlash bosqichlaridagi zaifliklarni topishga harakat qilsa, aktiv hujumlar shifratni bitlarini almashtirish, o'chirish yoki takrorlashga asoslanib, aloqa kanalidan ruxsatsiz foydalanish bilan amalga oshiriladi. Mazkur holatda, yaxlitlikni va autentifikatsiyani ta'minlovchi mexanizmlardan foydalanish katta samara beradi [2, 3, 6].

Kalitning bo'lishi mumkin bo'lgan barcha variantlarini hisoblash hujumi barcha kriptografik tizimlarda bo'lgani kabi oqimli shifrlar uchun o'rinli hisoblanib, undagi hisoblashlar kalitning uzunligidan katta bo'lmaydi (ammo, kalit uzunligidan kichik bo'lishi mumkin). Masalan, kalitning uzunligi 64 bitga teng bo'lsa, u holda kalitning bo'lishi mumkin bo'lgan barcha variantlari soni 264 ga teng bo'ladi.

Odatda ushbu hujumga bardoshli bo'lishi mavjud hisoblash vositalarining imkoniyatlaridan kelib chiqadi. Masalan, hozirgi kunda 128 bitli simmetrik kalitning barcha bo'lishi mumkin bo'lgan variantlarini hisoblashning imkoniyati mavjud emas va shuning uchun simmetrik kriptotizimlar uchun kalitning chegaraviy qiymati sifatida 128 bit olinadi. Bundan tashqari, simmetrik kalitning tasodifiy bo'lishi ham muhim hisoblanadi va bu aynan kalitni topishgacha bo'lgan hisoblashlar sonini kalit uzunligidan qanchalik kichik bo'lishini ta'minlaydi. Agar kalit tasodifiy bo'lsa, uni topishdagi hisoblashlar soni kalit uzunligiga shuncha yaqin bo'ladi.

Shifrlarni loyihalashdagi qayta boshlanish jarayoni (Ichki holatini yangilash jarayoni. U odatda yangi biror tasodifiy qiymat (Initialization vector, IV) kiritish orqali amalga oshiriladi.) boshqa bir hujumni olib kelishi mumkin bo'ladi. Agar kirishning PTSG ichki holatiga bog'liqligi yetarlicha chiziqsiz bo'lmasa, yangi kalit ketma-ketligi hosil bo'lganda hujumchi uni osonlik bilan topishi mumkin bo'ladi. Bu hujum tanlangan IV hujumi deb ataladi va xotiradan PTSGning dastlabki qiymatini tiklash imkoniyatini beradi.

Qo'shimcha kanallar asosida hujum (side channel attack) ma'lumotni shifrlash/rasshifrovkalash jarayonlarida hosil bo'lgan elektromagnit nurlanish miqdori yoki quvvat sarfini tahlil qilishga asoslandi. Ushbu usulning maqsadi algoritmda foydalanilgan kalitni bevosita topish hisoblanmasada, ichki holatni aniqlashni ko'zda tutadi.

Farqqa asoslangan hujumning (Distinguishing attack) asosiy maqsadi shifrlash/rasshifrovkalash kalitini topish bo'lib, buning uchun algoritmdan hosil bo'lgan ketma-ketliklarni haqiqiy ketma-ketliklardan farqini hisoblash talab etiladi. Ushbu farq odatda foydalanilgan kalit haqida statistik ma'lumotlarni oshkor qiladi.

Korrelatsiya usuli asosidagi hujumda (Correlation attack) esa LFSR yondashuvidagi shifrlash algoritmining Bool funksiyasi tahlil qilinib, undagi statistik zaiflik aniqlanadi.

Chiziqli hujumlar (Linear attacks) ham blokli ham oqimli simmetik shifrlar uchun mos bo'lib, algoritmda foydalanilgan chiziqli akslantirishlarni tahlil qilishga asoslanadi. Ushbu usul, dastlab DES shifrlash algoritmiga nisbatan qo'llanilgan.

Shunga o'xshash, algebraik hujumlar (Algebraic attacks) oqimli shifrlash algoritmlarini tahlillashdagi yangi usullardan bo'lib, kalit yoki holat bitlarini ifodalashda foydalanilgan chekli maydondagi algebraik tenglamalar sistemasini yechishni maqsad qiladi. Ushbu tahlilga bardoshlikni ta'minlashda algebraik immuniteti yuqori bo'lgan S jadvallardan foydalanish yuqori samara beradi.

Vaqt/ xotira/ ma'lumot kelishuvi (Time/ Memory/ Data tradeoff) asosidagi hujum dastlab blokli shifrlarga nisbatan qo'llanilgan bo'lsada, amalda barcha kriptografik algoritmlarga nisbatan ishlatish mumkin. Bunga ko'ra dastlab shifrnig umumiy tuzilishi o'rganiladi, olingan ma'lumotlar jadvallarda qayd etiladi. Ushbu bosqich tayyorlov bosqichi deb yuritilib, hujum bosqichida esa ushbu jadvallar qayta ishlangan haqiqiy ma'lumotlarning kalitini olish uchun foydalaniladi.

Faraz va hisoblash hujumlari (Guess and determine attack) samarasi aniq bo'lsada, yuqori hisoblashni talab etuvchi kriptotahlil usullaridan hisoblanadi. Ushbu usulga ko'ra oqimli shifrlash algoritmining ichki holatining bir qismi faraz qilinib, hosil bo'lgan ketma-ketlik holatiga asosan ichki holatning qolgan qismi tiklashga harakat qilinadi.

Yaratilgan har qanday kriptografik algoritmlarga qo'yiladigan talablardan biri bu algoritm tarkibidagi akslantirishlarning murakkab ifoda va hisoblashlardan holi bo'lishligi (ya'ni, soddaligi) bo'lib, algoritmlar akslantirishlarining kriptografik xususiyatlarini yaqqol tahlil qilinishini, kriptografik samaradorligini, apparat va apparat-dasturiy amalga oshirishni qulayligini ta'minlaydi [1]. Taklif etilgan yangi oqimli shifrlash algoritmlari tarkibidagi akslantirishlarning soddaligi ularning kriptografik xususiyatlarini to'la va yaqqol tahlil qilish imkonini beradi. Oqimli shifrlash algoritmlarining kriptografik samaradorligi quyidagi talablarga ko'ra baholanadi [1]:

- akslantirishlarning soddaligi;
- akslantirishlarning chiziqli darajasining yuqoriligi;
- akslantirishlarning qat'iy jadal samaradorlik darajasining yuqoriligi;
- bir tomonlamalik xususiyatining mavjudligi;
- hosil qilingan PTSGdan hosil bo'lgan qiymatlar tasodifiylik darajasining yuqoriligi;
- yetarli darajada kata hajmi takrorlanmas ketma-ketlik generatsiyalashi;
- psevdotasodifiy qiymatlarni hosil qilish va shifrlash tezligining yuqoriligi;
- maxfiy kalitni aniqlash faqat mumkin bo'lgan barcha kalitlarni tanlash usuli bilan amalga oshirilishi mumkinligi;
- hosil qilingan psevdotasodifiy ketma-ketlik yoki uning biror qismi yordamida kalitni tiklash imkonini yo'qligi;
- hosil qilingan psevdotasodifiy ketma-ketlikning ma'lum qismini bilgan holda uning qolgan qismini tiklash imkonining yo'qligi;
- differensial kriptotahlil usuliga bardoshligi;
- chiziqli kriptotahlil usuliga bardoshligi.

Har qanday kriptografik algoritmlarni yaratishda ularning kriptobardoshligi bugungi kunda ma'lum bo'lgan kriptografik hujumlarga bardoshligi bilan baholanadi. Shu bilan birga oqimli shifrlar hosil qilgan gamma ketma-ketliklarning tasodifiyligi tasodifiylikka tekshiruvchi testlar orqali tekshiriladi.

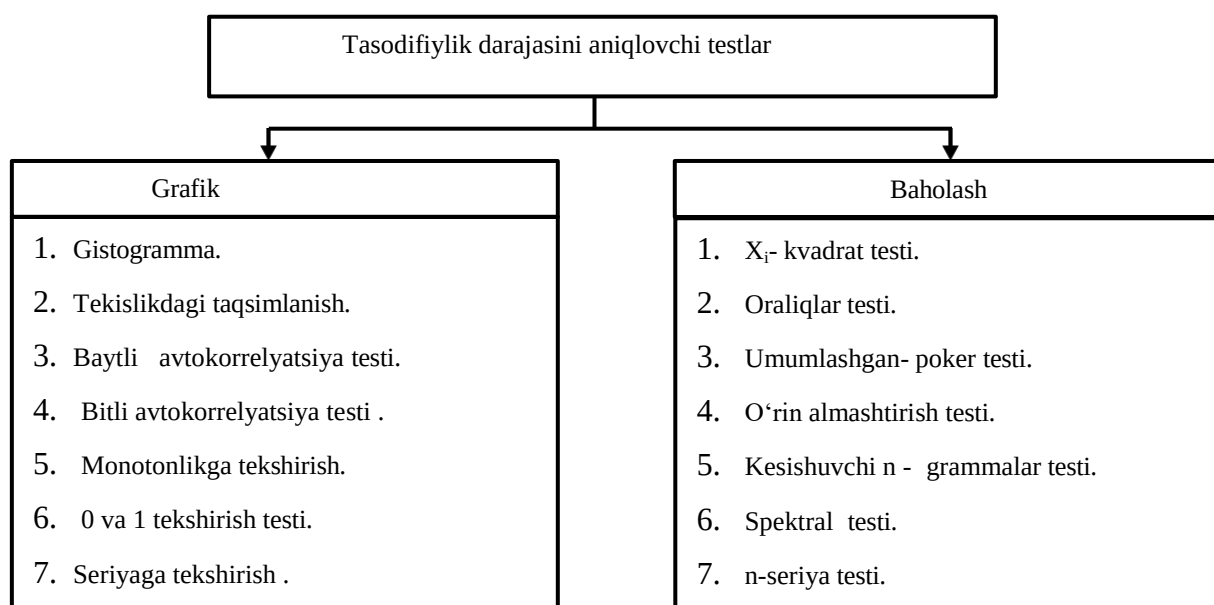
Tasodifiylikka tekshiruvchi testlar 2 xil bo'ladi (1-rasm) [7]:

1. Grafik testlar – Grafik testlar foydalanuvchiga tekshirilayotgan ketma- ketlikning ma'lum bir grafik bog'liqligi haqidagi ma'lumotni berib, u bo'yicha tekshirilayotgan ketma-ketlik xossalari to'g'risida xulosa chiqarish imkoniyatini beradi.

2. Baholash testlari – baholash testlari tekshirilayotgan ketma-ketlikning statistik xususiyatlarini tahlil qilib, uning chin tasodifiylik darajasi haqida xulosa chiqarish imkoniyatini beradi.

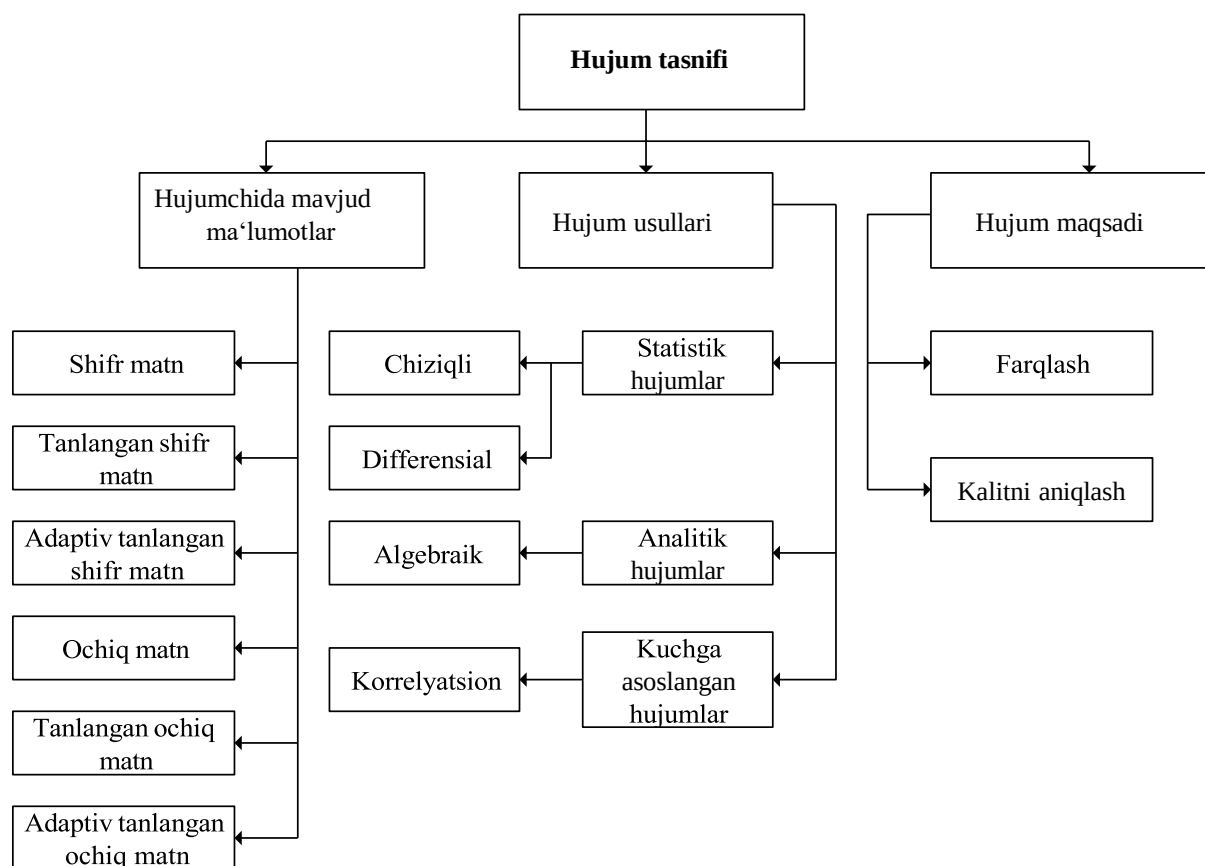
Oqimli shifrlarning bardoshligini baholash uchun yuqorida keltirilgan tasodifiylikka tekshiruvchi testlarning o'zi kamlik qiladi. Oqimli shifrlarning bardoshligini to'liq baholashda algoritmnig kriptotahlil usullariga bardoshligi tekshiriladi. Oqimli shifrlash algoritmlariga qo'llaniluvchi kriptotahlil usullarini shartli ravishda uchta guruhga ajratish mumkin [4, 5]:

- analitik hujumlar, statistik hujumlar va kuchga asoslangan hujumlar.



1-rasm. Tasodifiylik darajasini aniqlovchi testlar

Analitik hujumlarga algoritmnining qurilish sxemasini analitik prinsiplar asosida ochishga harakat qiluvchi kriptohujumlar misol bo'ladi. Statistik hujumlarga shifrovchi gammaning statistik xossalarini baholashga asoslangan kriptohujumlar kiradi. Kuchga asoslangan hujumlarga kalitning barcha mumkin bo'lgan variantlarini ko'rib chiqishga asoslangan kriptohujumlar kiradi (2-rasm).



2-rasm. Oqimli shifrlarga qo'llaniluvchi kriptohujumlar

Oqimli shifrlar zamonaviy kriptografiyada, ayniqsa real vaqtli aloqa tizimlarida keng qo'llanilishi bilan ajralib turadi. Ularning ishlash mexanizmlari oddiy va yuqori tezlikda bo'lishi bilan birga, xavfsizlik nuqtai nazaridan muayyan zaifliklarga ega. Maqolada hozirda mavjud bo'lgan zamonaviy kriptotahlil usullari tahlil qilindi va ularning qaysi zamonaviy shifrlash algoritmlari uchun qo'llanilishi tahlil qilindi. Statistik, algebraik, korrelyatsion, vaqtga asoslangan va faraz-hisoblash hujumlari oqimli shifrlarga nisbatan muvaffaqiyatli qo'llanilishi mumkin. IV (Initialization Vector) tanlanishidagi xatoliklar oqimli shifrlarning sinxronlashuv bosqichida zaiflik keltirib chiqaradi. Side channel hujumlar, ya'ni elektromagnit nurlanish yoki quvvat sarfini tahlil qilish orqali kalit haqida ma'lumot olish mumkinligi ko'rsatib o'tildi. Shifrga oid gamma ketma-ketliklarning tasodifiylik darajasi grafik va statistik testlar orqali baholanadi, ammo bu testlarning o'zi to'liq tahlil uchun yetarli emas. Kriptotahlilga bardoshlilik darajasini aniqlash uchun oqimli shifrlar kompleks baholash, ya'ni analitik, statistik va kuchga asoslangan hujumlarga nisbatan sinovdan o'tkazilishi lozim. Oqimli shifrlarda ishlatiladigan akslantirishlarning soddaligi va yuqori nolinearligi xavfsizlikni ta'minlovchi muhim omillardandir. Tadqiqotlar shuni ko'rsatmoqdaki, samarali va barqaror oqimli shifrlarni ishlab chiqish uchun chuqur matematik modellarga, kuchli tasodifiylik generatorlariga va kriptotahlilga qarshi immunitetga ega komponentlarga ehtiyoj bor. Kelajakda oqimli shifrlarning xavfsizligini oshirish uchun yangi arxitekturaviy yondashuvlar va kriptotahlilga bardoshli algoritmlarni ishlab chiqish muhim ilmiy yo'nalish bo'lib qoladi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

- [1] A.И.Мусаев. “Uzluksiz shifrlashning kriptobardoshli algoritmlari va ularning samaradorligini baholash” nomzodlik dissertatsiya ishi. Toshkent-2010.
- [2] B.Preneel, H. Wu “Cryptanalysis and design of stream ciphers” //PhD diss., PhD thesis, Katholieke Universiteit Leuven. – 2008.
- [3] R.Verdu. “Introduction to cryptanalysis: attacking stream ciphers” //Institute for Computing and Information Sciences Radboud University Nijmegen, The Netherlands. – 2001. – T. 28. – C. 31-32.
- [4] Ю.В.Стасев, А.В.Потий, Ю.А. Избенко “Исследование методов криптоанализа поточных шифров” [Электронный ресурс] //Режим доступа к ресурсу:http://www.nrjetix.com/fileadmin/doc/publications/articles/stasev_potiy_izbenko_ru.pdf.
- [5] I.R. Rakhmatullaev, I.M. Boyquziyev “Analysis of cryptanalysis methods applied to stream encryption algorithms” ICABCS-2023 Galgotias University Conference 24-25 Feb 2023 (Scopus)
- [6] I.R.Rahmatullayev, N.R.Zaynalov, U.X.Narzullayev, A.A.Shakarov, A.N.Muhammadiyev, D. Qilichev, “Analysis of the Frequency of Letters of the Uzbek Language Based on the Cyrillic Alphabet”, 15th International Conference on Application of Information and Communications Technologies (AICT), IEEE, 2021, November, Tashkent, Uzbekistan, 1-4 p.
- [7] D.Ye. Akbarov Axborot xavfsizligini ta'minlashning kriptografik usullari va ularning qo'llanishlari. Toshkent. "O'zbekiston markasi", 2009.
- [8] [://crypto.stackexchange.com](https://crypto.stackexchange.com)
- [9] <https://www.ecrypt.eu.org/stream>
- [10] <https://www.iacr.org>
- [11] <https://csrc.nist.gov>

**KOMPYUTER TARMOQLARIDA TRAFIK ANOMALIYALARINI ANIQLASHNING
INNOVATSION YONDOSHUVLARI****PhD, dotsent I.I. NISHANOV, D.D. XAYITOV***O'R MV Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti*

Annotatsiya. Mazkur maqolada kompyuter tarmoqlarida yuzaga keladigan trafik anomaliyalarni aniqlashga doir zamonaviy yondashuvlar yoritilgan. Xususan, statistik usullar, mashinaniy o'qitish va chuqur o'qitish asosidagi metodlar tahlil qilinadi. Tarmoq xavfsizligini ta'minlashda anomaliyalarni erta aniqlashning ahamiyati va real vaqtli monitoring tizimlarining roli ochib beriladi.

Kalit so'zlar: tarmoq xavfsizligi, anomaliya aniqlash, statistik tahlil, imzo asosida aniqlash, xulq-atvor tahlili, mashina o'rganish, chuqur o'rganish, sun'iy intellekt, generative adversarial network, CNN, IDS, kiberxavfsizlik.

Аннотация. В данной статье рассматриваются современные подходы к выявлению аномалий сетевого трафика в компьютерных сетях. В частности, анализируются статистические методы, а также методы, основанные на машинном и глубоком обучении. Раскрывается важность раннего обнаружения аномалий для обеспечения сетевой безопасности и роль систем мониторинга в режиме реального времени.

Ключевые слова: сетевая безопасность, обнаружение аномалий, статистический анализ, сигнатурный метод, поведенческий анализ, машинное обучение, глубокое обучение, искусственный интеллект, генеративно-состязательные сети (GAN), сверточные нейронные сети (CNN), системы обнаружения вторжений (IDS), кибербезопасность.

Abstract. This article explores modern approaches to detecting traffic anomalies in computer networks. Specifically, it analyzes statistical methods as well as machine learning and deep learning-based techniques. The importance of early anomaly detection for ensuring network security and the role of real-time monitoring systems are highlighted.

Key words: network security, anomaly detection, statistical analysis, signature-based detection, behavioral analysis, machine learning, deep learning, artificial intelligence, generative adversarial networks (GAN), convolutional neural networks (CNN), intrusion detection systems (IDS), cybersecurity.

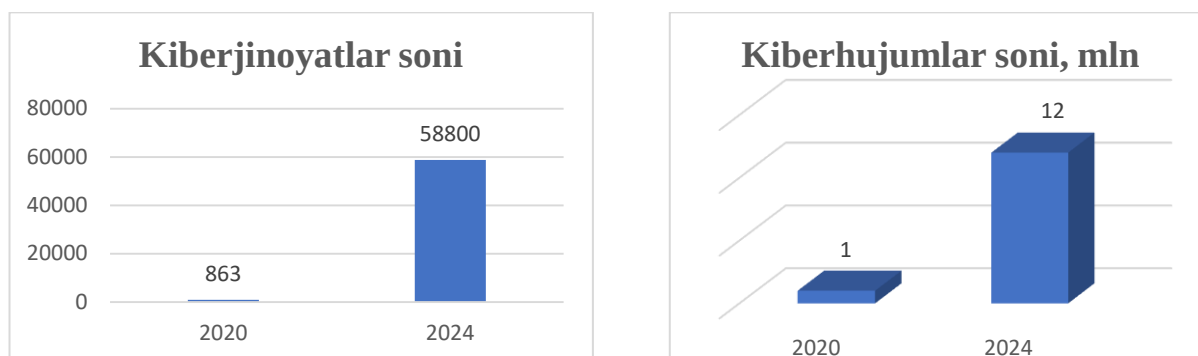
Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi zamonaviy tarmoqlarni inson faoliyatining barcha sohalarida muhim vositaga aylantirmoqda. Ayniqsa, onlayn xizmatlar, elektron to'lov tizimlari, raqamli bank operatsiyalari va masofaviy boshqaruv texnologiyalarining keng qo'llanilishi bilan tarmoq muhiti global raqamli infratuzilmaning asosiy elementiga aylangan. Biroq, bunday texnologik rivojlanish bilan bir qatorda tarmoq muhitida yuzaga kelayotgan turli xildagi anomaliyalar, ya'ni odatiy faoliyatdan chetga chiqadigan, xavfsizlikka tahdid soluvchi yoki jinoyat belgilariga ega bo'lgan harakatlar soni ham ortib bormoqda.

Tarmoq anomaliyalari ko'pincha kiberjinoyatlar, kiberhujumlar yoki zararli trafik shaklida namoyon bo'lib, ularga vaqtida javob berilmasa, butun axborot tizimining izdan chiqishiga olib kelishi mumkin. Shu sababli, tarmoq anomaliyalarini aniqlash va ularni klassifikatsiya qilish, ayniqsa, real vaqt rejimida monitoring olib borish muhim ilmiy-amaliy muammo sifatida e'tirof etilmoqda.

So'nggi yillarda O'zbekistonda tarmoq infratuzilmasining kengayishi fonida kiberjinoyatlar va kiberhujumlar soni keskin oshdi. Jumladan, O'zbekiston Respublikasi Ichki ishlar vazirligining Kiberxavfsizlik markazi tomonidan taqdim etilgan hisobotlarga ko'ra,

2020-yilda mamlakatda atigi 863 ta kiberjinoyat qayd etilgan bo'lsa, 2024-yilga kelib bu ko'rsatkich 58800 taga yetdi, ya'ni 68 barobarga ortdi 1-rasm [11]. Shu bilan birga, 2020-yildagi 1 millionga yaqin kiberhujumlar soni 2024-yilda 12 milliondan oshgani kuzatildi 1-rasm [11].

Bunday holat, ayniqsa, moliyaviy sektorga qaratilgan tarmoqdagi firibgarliklar, fishing hujumlari, zararli dastur tarqatish va ijtimoiy muhandislik asosidagi trafiklarning keskin o'sishida yaqqol namoyon bo'lmoqda.



1-rasm. Kiberxavfsizlik markazi tomonidan taqdim etilgan kiberjinoyat hamda kiberhujumlarning oshib borish diagrammasi

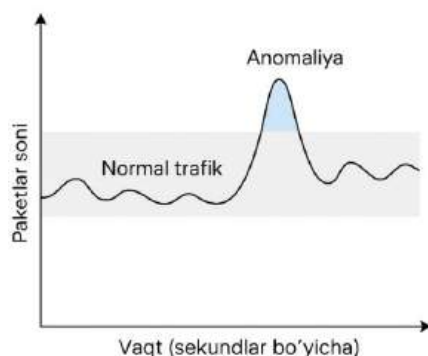
Kiberjinoyatlarning 98 foizining bank tizimi va onlayn to'lov xizmatlariga yo'naltirilgani, ularning katta qismi aynan tarmoq anomaliyalari orqali amalga oshirilgani - ushbu muammoning dolzarbligini yanada kuchaytiradi. Bunday anomaliyalarni erta bosqichda aniqlash va bartaraf etish zamonaviy kiberxavfsizlik siyosatining ajralmas qismiga aylangan. Tarmoq anomaliyalari ko'pincha kiberjinoyatlar, kiberhujumlar yoki zararli trafik shaklida namoyon bo'lib, ularga vaqtida javob berilmasa, butun axborot tizimining izdan chiqishiga olib kelishi mumkin. Shu sababli, tarmoq anomaliyalarini aniqlash va ularni klassifikatsiya qilish, ayniqsa, real vaqt rejimida monitoring olib borish muhim ilmiy-amaliy muammo sifatida e'tirof etilmoqda. Xavfsizlik infratuzilmasida muhim o'rin egallovchi jarayonlardan biri bu - tarmoqdagi anomaliyalarni aniqlash hisoblanadi.

An'anaviy yondashuvlar, jumladan qoida asosidagi tizimlar, ko'plab hollarda samarali bo'lishiga qaramay, zamonaviy va murakkab tahdidlar oldida ojizlik qiladi. Shu sababli, oxirgi yillarda sun'iy intellekt, mashinaviy o'qitish, va chuqur o'qitish kabi zamonaviy texnologiyalar yordamida anomaliyalarni aniqlashga qaratilgan tadqiqotlar dolzarb bo'lib bormoqda. Kompyuter tarmoqlarida anomaliyalarni aniqlashning turli uslublari ko'rib chiqildi, ularning afzallik va zaifliklari tahlil qilindi, hamda amaliy modellarga asoslangan yondashuvlar taqdim etildi. Maqola innovatsion yondashuvlarning samaradorligini ko'rsatish va tarmoq xavfsizligini mustahkamlash bo'yicha ilmiy asoslangan tavsiyalar berishga qaratilgan.

Tarmoq anomaliyalarini aniqlash - bu odatiy xatti-harakatlardan chetga chiqadigan tarmoq trafigidagi tartibsiz naqshlarni aniqlash jarayoni. Asosan, tarmoq anomaliyalarini aniqlash oqim yozuvlari, paketlar yoki jurnallar kabi tarmoq telemetriyasi ma'lumotlarini doimiy ravishda to'plashni va ularni oddiy tarmoq xatti-harakatlari bilan taqqoslashni o'z ichiga oladi. Asosiy chiziqli tarixiy ma'lumotlar va "oddiy" trafik hajmi, protokollari, IP-manzillari, foydalanuvchilarga kirish shakllari va boshqalar bo'yicha qanday ko'rinishini statistik tahlil qilish yordamida o'rnatiladi. Joriy trafik namunalari ushbu bazaviy chiziqdan sezilarli darajada og'ishsa, tizim tarmoq anomaliyasini belgilaydi [6].

Ushbu anomaliyalar turli yo'llar bilan namoyon bo'lishi mumkin. Masalan, serverga trafikning to'satdan ko'tarilishi, tarmoq faolligining g'ayrioddiy pasayishi, chet el IP diapazonidan kutilmagan trafik yoki u ilgari hech qachon bo'lmagan ulanishlarni amalga oshirilishi mumkin 2-rasm. Bunday anomaliyalar ko'pincha asosiy muammolar yoki tahdidlarning dastlabki belgilaridir. Ular kiberhujum davom etayotgani, noto'g'ri sozlangan qurilma, tarmoqdagi nosozlik yoki ruxsatsiz foydalanish haqida signal berishi mumkin. Tarmoq anomaliyalarini aniqlash himoya

vositasi bo'lib, NetOps va xavfsizlik guruhlarini o'z tarmoqlarida sodir bo'layotgan "odatiy bo'lmagan narsa" haqida ogohlantiradi, shunda ular qo'shimcha tekshirishlari mumkin.



2-rasm. Kompyuter tarmog'ida hosil bo'lgan anomaliyaning ko'rinishi

Raqamli infratuzilmalar tez sur'atlar bilan kengayib borayotgan bugungi kunda, kompyuter tarmoqlarining xavfsizligi har qachongidan ham dolzarb masalaga aylangan. Tarmoqlarda yuzaga keladigan noxush holatlar, hujumlar yoki noodatiy faoliyatlar odatda anomaliyalar sifatida namoyon bo'ladi. Bunday anomaliyalarni erta aniqlash va bartaraf etish, axborot tizimlarining uzluksiz va ishonchli ishlashini ta'minlashda muhim rol o'ynaydi.

1-jadval.

Tarmoq anomaliyalarini aniqlashning afzallik va kamchiliklari

Yondashuvlar	Afzalliklari	Kamchiliklari
Statistik tahlil	Soddaligi va tezligi bilan ajralib turadi. Kam resurs talab etadi. Yengil o'rnatiladi va ishlaydi.	O'zgarmas me'yorlarga bog'liq. Noaniq holatlarda noto'g'ri ijobiy natijalar yuqori. Murakkab hujumlarni aniqlay olmaydi.
Imzo asosida aniqlash	Yuqori aniqlikdagi aniqlash imkoniyati. Oldindan ma'lum tahdidlarni ishonchli aniqlaydi. Real vaqtli ishlash uchun mos keladi.	Faqat ma'lum hujumlar bilan cheklanadi. Yangi yoki noma'lum hujumlarga nisbatan samarasiz. Imzo bazasini doimiy yangilab borish talab etiladi.
Xulq-atvor tahlili	Foydalanuvchi yoki tizimning odatdagi holatini o'rganib, og'ishlarni samarali aniqlaydi. Noma'lum hujumlarni aniqlash imkonini beradi.	Modelni qurish murakkab. Noto'g'ri ijobiy natijalar ehtimoli yuqori. Dinamik muhitlarga moslashishi vaqt talab etadi.
Mashinaviy o'qitish	Moslashuvchan va o'rganishga qodir. Yangi va murakkab hujumlarni aniqlashda samarali. Avtomatik qaror qabul qilish imkoniyatiga ega.	Modelni o'qitish uchun katta hajmdagi belgilangan ma'lumot kerak. Hisoblash resurslariga yuqori talab mavjud. Noaniq izohlanish. MO'ning to'g'ri modellarning integratsiyasi kutubxonaga qaramlikning yuqoriligi.
Chuqur o'qitish	Keng ko'lamli ma'lumotlardan o'rganish imkoniyati. Murakkab naqshlar va bog'liqliklarni aniqlashda ustunlik. O'z-o'zini sozlash imkoniyati mavjud.	O'qitish jarayoni resurs talab qiladi. Natijalarni izohlash qiyin.
Yig'ma (Ensemble) yondashuvlar	Bir nechta modelning kuchli tomonlarini birlashtiradi. Aniqlik va ishonchlilik yuqori. Noto'g'ri ijobiy va salbiylarni kamaytiradi.	Integratsiya murakkab. Hisoblash xarajatlari ortadi. Model boshqaruvi va yangilanishi murakkab.

Anomaliyalarni aniqlashning turli metodologik yondashuvlari mavjud bo'lib, ular statistik tahlil, imzo asosidagi aniqlash, xulq-atvor modellari, mashina o'rganishi hamda chuqur o'qitish texnikalariga asoslanadi. Har bir yondashuv o'zining aniqlik darajasi, moslashuvchanlik

xususiyatlari hamda hisoblash resurslariga bo'lgan ehtiyoji nuqtai nazaridan o'ziga xos afzalliklar va cheklovlariga ega.

Statistik yondashuv asosida anomalialarni aniqlash. Statistik anomalialarni aniqlash yondashuvi kompyuter tarmoqlaridagi normal (ya'ni, odatiy) xatti-harakatlarni matematik modellashtirish orqali aniqlashga qaratilgan bo'lib, bu jarayonda tarmoq parametrlarining statistik ko'rsatkichlari aniqlanadi va ularning belgilangan chegaradan og'ishi anomaliya sifatida baholanadi.

Tizim administratorlari statik yoki dinamik chegaraviy qiymatlarni belgilashi mumkin. Statik chegaralarga misol sifatida tarmoq trafigining ma'lum fiksatsiyalangan qiymat (masalan, 500 Mbit/s) dan yuqoriga ko'tarilishini olish mumkin. Bunday yondashuv soddaligi bilan ajralib tursa-da, dinamik sharoitlarga to'liq moslasha olmaydi. Shu sababli, ko'p hollarda statistik parametrlar asosida moslashuvchan (dinamik) chegaralar qo'llaniladi [1].

Dinamik chegaralar quyidagi statistik ko'rsatkichlarga asoslanadi:

O'rtacha qiymat: tarmoq parametrlarining umumiy darajasini tavsiflaydi;

Standart og'ish: parametrlarning o'zgaruvchanlik darajasini ko'rsatadi;

Dispersiya: umumiy tarqoqlikni baholashga xizmat qiladi;

Klasterlash: o'xshash xatti-harakatlarni guruhlash orqali normal holatni modellashtiradi.

Statistik yondashuv asosida anomalialarni aniqlash uchun turli metodlar mavjud, lekin eng keng tarqalgan usullardan biri Z-score yoki Mahalanobis masofa asosida aniqlash hisoblanadi.

Z-score metodi. Bu usulda har bir kuzatuv quyidagicha hisoblanadi:

$$Z = \frac{x - \mu}{\sigma} \quad (1)$$

bu yerda:

x - kuzatilayotgan qiymat,

μ - tanlangan namunadagi o'rtacha qiymat,

σ - standart og'ish.

Agar Z-score ning mutlaq qiymati odatda 3 dan katta bo'lsa, bu qiymat anomaliya deb hisoblanadi [2].

Mahalanobis masofasi. Bu usul ko'p o'lchovli ma'lumotlar uchun ishlatiladi:

$$D_M(x) = \sqrt{(x - \mu)^T \Sigma^{-1}(x - \mu)} \quad (2)$$

Bu yerda:

x - kuzatilayotgan vektor,

μ - o'rtacha vektor,

Σ^{-1} - kovariatsiya matritsasining teskari matritsasi.

$D_M(x)$ - Mahalanobis masofa

Agar $D_M(x)$ aniqlangan masofa ma'lum statistik chegaradan oshsa, u anomaliya deb qaraladi [2].

Bunday yondashuvlarning afzalligi shundaki, ular tarmoqda yuzaga kelgan anomaliya holatlarni aniqlashda qat'iy qoidalarga emas, balki real statistik tavsifnomalarga asoslanadi, bu esa aniqlikni oshiradi va yolg'on ijobiy yoki yolg'on salbiy signal berish ehtimolini kamaytiradi.

Imzoga asoslangan aniqlash tizimlari. Imzoga asoslangan aniqlash yondashuvi axborot xavfsizligida keng qo'llaniladigan va ishonchli yondashuv bo'lib, u ilgari aniqlangan va hujjatlashtirilgan tahdidlarning xususiyatlarini aniqlashga asoslanadi. Ushbu yondashuv qat'iy ma'noda anomalialarni aniqlash usuli hisoblanmasa-da, ko'plab xavfsizlik arxitekturalarida anomalialarni aniqlash tizimlari (ADS) bilan integratsiyada ishlatiladi.

Imzoga asoslangan aniqlash tizimlarining asosiy tamoyili - ma'lum bir zararli faoliyatga oid imzolar (ya'ni, xos bayt ketma-ketliklari, trafik sxemalari, protokol buzilishlari va boshqa identifikatorlar) bazasiga asoslanib, real vaqt rejimida tarmoq trafikini solishtirishdir. Agar

trafikdagi faoliyat ushbu imzolardan biriga mos kelsa, tizim ogohlantirish hosil qiladi yoki avtomatik tarzda javob chorasini ishga tushiradi [3].

Misol sifatida, bu yondashuv orqali:

ma'lum zararli dasturlar (masalan, trojanlar yoki viruslar) kodining belgilari, hujumlar ketma-ketligi (masalan, port skanerlash yoki SQL Injection), trafik namunalaridagi noto'g'ri konfiguratsiyalar aniqlanishi mumkin [4].

Imzoga asoslangan aniqlash tizimlari (masalan, Snort, Suricata) oldindan belgilangan hujum imzolari orqali tahdidlarni aniqlaydi. Ushbu tizimlar faqat mavjud imzolar asosida ishlaganligi sababli, ba'zi real hujumlarni aniqlamasligi mumkin - bu holat False Negative (FN) deb yuritiladi.

Recall formulasi yordamida shuni baholaymiz:

$$R = \frac{TP}{TP+FN} \quad (3)$$

Bu formulada:

TP - Tizim tomonidan aniqlangan real tahdidlar soni.

FN - Tizim aniqlay olmagan tahdidlar soni.

Shu sababli, imzoga asoslangan yondashuv aniq va ma'lum tahdidlar uchun yuqori aniqlikka ega bo'lsa-da, u kutilmagan yoki yangi paydo bo'lgan tahdidlarga nisbatan zaif hisoblanadi. Shuning uchun ko'plab zamonaviy xavfsizlik tizimlarida ushbu yondashuv anomaliyalarni aniqlash tizimlari (ADS) bilan birgalikda, gibrid arxitektura shaklida qo'llaniladi [12].

Xulq-atvorga asoslangan anomaliyalarni aniqlash yondashuvi. Xulq-atvorga asoslangan anomaliyalarni aniqlash - bu foydalanuvchilar, qurilmalar yoki xizmatlarning normal (odatdagi) xatti-harakatlarini kuzatish va modellashirish orqali statistik yoki evristik asosda noxush holatlarni aniqlashga qaratilgan yondashuvdir. Mazkur metodologiya vaqt davomida to'plangan tarixiy ma'lumotlarga asoslanib, har bir subyekt uchun xulqiy profil shakllantiradi [7].

Masalan, tizim foydalanuvchisining geografik joylashuvi (masalan, San-Fransisko), tizimga kirish vaqtlari, ishlatiladigan ilovalar yoki xizmatlarga murojaat qilish odatlari asosida ularning normal harakatlar doirasi belgilanadi. Agar real vaqt kuzatuvlari natijasida ushbu profilga mos kelmaydigan faoliyat aniqlansa - masalan, foydalanuvchi kutilmagan va ilgari foydalanilmagan serverga murojaat qilsa yoki qurilma notanish tashqi manzilga katta hajmdagi ma'lumot uzatishni boshlasa - bu holat anomaliya sifatida baholanadi.

Mazkur yondashuv ayniqsa quyidagi xavflarni aniqlashda samaralidir:

Ichki tahdidlar (masalan, komprometatsiya qilingan foydalanuvchi hisoblari),

Kechikkan (latent) hujumlar, ya'ni ko'zga tashlanmasdan tarmoqda harakatlanadigan xavfli faoliyatlar,

Yangi yoki noma'lum hujum vektorlarini aniqlash.

Xulq-atvorga asoslangan anomaliyalarni aniqlash yondashuvining Eng keng tarqalgan usullardan biri - Euclidean Distance (Yevklid masofasi) bo'lib, bu ikki vektor o'rtasidagi chiziqli masofani o'lchaydi.

Har bir foydalanuvchining yoki tizimning harakati quyidagicha ko'p o'lchovli vektor sifatida ifodalanadi:

$$x = [x_1, x_2, \dots, x_n] \quad (4)$$

Bu yerda:

x_i - faoliyatning i-ko'rsatkichidir (masalan: paket hajmi, protokol turi, port raqami, IP intervallar va h.k.);

n - atributlar (ko'rsatkichlar) soni.

Normal profil ham shunga o'xshash vektor shaklida yoziladi:

$$\mu = [\mu_1, \mu_2, \dots, \mu_n] \quad (5)$$

Euclidean Distance formulasi

Har ikki vektor orasidagi masofa quyidagi formula asosida hisoblanadi:

$$d(x, \mu) = \sqrt{\sum_{i=0}^n (x_i - \mu_i)^2} \quad (6)$$

Bu yerda:

d - joriy faoliyat bilan normal profil o'rtasidagi masofa;

x_i - kuzatilayotgan faoliyatning i -elementi;

μ_i - shu ko'rsatkich bo'yicha o'rtacha (normal) qiymat.

Agar $d(x, \mu) > \delta$, u holda x anomaliya hisoblanadi

Bu yerda:

δ - **threshold (chegara)** qiymati bo'lib, uni tajriba yo'li bilan tanlash yoki statistik metodlar yordamida aniqlash mumkin [8, 12].

Mashinaviy o'qitish asosida anomaliyalarni aniqlash

Mashinaviy o'qitish asosida anomaliyalarni aniqlash - bu an'anaviy statistik va qoidaviy yondashuvlarga nisbatan yanada moslashuvchan va avtomatlashtirilgan metod bo'lib, murakkab va katta hajmdagi tarmoq ma'lumotlaridan normal va noodatiy xatti-harakatlar o'rtasidagi nozik farqlarni aniqlashga qaratilgan. Bu yondashuvda turli matematik modellar va algoritmlar yordamida tarmoq trafigining o'ziga xos xususiyatlari (features) asosida o'rganish jarayoni amalga oshiriladi [9, 13].

Asosiy yondashuvlar:

Nazoratli - Trening ma'lumotlari aniq belgilangan (ya'ni, "normal" va "anomaliya" deb yorliqlangan). Klassifikatsiya algoritmlari (masalan, Decision Tree, Random Forest, Support Vector Machines, Logistic Regression) yordamida yangi ma'lumotlar sinflarga ajratiladi.

Kamchilik: real tarmoq muhitida anomaliyalar kam va noodatiy bo'lgani sababli, yorliqlangan ma'lumotlarni olish qiyin.

Nazoratsiz - Trening ma'lumotlari yorliqsiz bo'lib, tizim mustaqil ravishda normal xatti-harakatlarni o'rganib, ular asosida farqli (ya'ni anomaliya) holatlarni ajratadi. K-means, DBSCAN, Isolation Forest, Autoencoders, Principal Component Analysis (PCA) va Gaussian Mixture Models (GMM) kabi algoritmlar qo'llaniladi.

Bu yondashuv yangi va noma'lum hujumlarni aniqlashda samaralidir.

Yarim nazoratli - Asosan normal holatlarga oid ma'lumotlar asosida o'qitiladi va undan chetga chiqishlar anomaliya sifatida baholanadi.

Bu usul amaliy tizimlarda keng qo'llaniladi, chunki real tahdidlar kam uchraydi.

Chuqur o'qitish asosida anomaliyalarni aniqlash. Chuqur o'qitish asosida anomaliyalarni aniqlash - bu tarmoq xavfsizligi sohasida eng ilg'or va samarali yondashuvlardan biridir. U katta hajmdagi tarmoq ma'lumotlarini avtomatik ravishda tahlil qilish va ulardagi murakkab, noxiziqli xususiyatlarni aniqlash orqali anomaliyalarni aniqlash imkonini beradi [6, 10].

2-jadval

Tarmoq anomaliyalarini aniqlashning modellari

Model turi	Asosiy tamoyili	Qo'llanilish sohasi	Afzalliklari
Autoencoder	Ma'lumotlarni siqib chiqarish (encoding) va tiklash (decoding) orqali xatoni aniqlash	Normal holatlar tiklanadi, anomaliyalar katta xato bilan ajraladi	O'z-o'zidan o'rganish; murakkab strukturani modellashtira oladi
RNN / LSTM	Ketma-ket ma'lumotlar tahlili va vaqtga bog'liq xatti-harakatlarni aniqlash	Tarmoq trafik oqimlari, sessiyalar, vaqtga bog'liq tahdidlar	Sekvensiyalarni tushunadi; vaqt bog'liqliklarini aniqlashga mos
CNN	Tuzilmaviy va vizual naqshlarni aniqlash	Paketlar formatida ko'rsatilgan trafik, trafik segmentlari	Lokal naqshlarni samarali ajratadi; juda tez ishlaydi

Model turi	Asosiy tamoyili	Qo'llanilish sohasi	Afzalliklari
GAN (Generative Adversarial Network)	Real va sun'iy trafikni solishtirish, farqlarni aniqlash	Murakkab yoki yangi trafik tahlili, yangi tahdidlarni aniqlash	Yuqori sezuvchanlik; noma'lum anomaliyalarni aniqlash imkoniyati
Transformer	Self-attention deb nomlanuvchi mexanizmga asoslanadi. Ya'ni Kiruvchi ma'lumot ketma-ketligidagi har bir elementni boshqalari bilan bog'lab, ularning o'zaro ahamiyatini hisoblaydi.	Log va trafik oqimlar harakatini aniqlash. firibgarlik, intrusion detection, yoki DDoS hujumlarini erta aniqlash. tibbiy datchik ma'lumotlarida noodatiy o'zgarishlarni aniqlash.	Uzoq bog'liqliklarni o'rganish. parallel ishlashga mos, bu esa o'qitish tezligini oshiradi. Moslashuvchanlik, turli turdagi ketma-ketlik ma'lumotlari (matn, trafik, vaqt bo'yicha loglar) bilan ishlay oladi.

XULOSA

1. Kompyuter tarmoqlarida anomaliyalarni aniqlash axborot xavfsizligi sohasining muhim va ustuvor yo'nalishlaridan biri hisoblanadi. Tarmoq muhitining murakkabligi, uzluksiz o'zgarib boruvchi tahdidlar va katta hajmdagi ma'lumotlar oqimi ushbu muammoning zamonaviy yondashuvlar asosida hal qilinishini taqozo etadi.

2. An'anaviy anomaliya aniqlash usullari (masalan, imzo asosida aniqlash) ma'lum darajadagi samaradorlikka ega bo'lsa-da, yangi va ilgari noma'lum bo'lgan tahdidlarni aniqlashda samarasiz bo'lishi mumkin. Shu munosabat bilan, sun'iy intellekt, mashinaviy o'qitish va chuqur o'qitish kabi zamonaviy yondashuvlardan foydalangan holda, tarmoqdagi anomaliyalarni aniqlashga oid yechimlar ilmiy-amaliy jabhada katta ahamiyat kasb etmoqda.

3. Tadqiqot natijalari shuni ko'rsatmoqdaki, chuqur o'qitish modellaridan xususan, konvolyutsion neyron tarmoqlar (CNN), qayta aloqali neyron tarmoqlar (RNN) va avtoenkoderlar (Autoencoders) – samarali foydalanish natijasida aniqlik darajasi yuqori, soxta ijobiy va soxta salbiy natijalar darajasi esa nisbatan past bo'lgan anomaliya aniqlash tizimlarini yaratish imkoniyati mavjud.

4. Real vaqt rejimida monitoring qilish, adaptiv modellarni joriy etish va kontekstual tahlilni hisobga olish orqali tarmoqdagi xavfsizlik darajasini yanada oshirish mumkin. Mazkur yondashuvlar nafaqat hujumlarni erta bosqichda aniqlash, balki ularga qarshi tezkor chora ko'rish imkonini ham yaratadi.

5. Tarmoq anomaliyalarini aniqlashning innovatsion yondashuvlari asosida anomaliyalarni aniqlash kompyuter tarmoqlarining xavfsizlik infratuzilmasini mustahkamlashda istiqbolli va ilmiy asoslangan yechimlar qatoriga kiradi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

- [1] Chandola V., Banerjee A., Kumar V. Anomaly detection: A survey // ACM Computing Surveys. – 2009. – Vol. 41, No. 3. – P. 1–58
- [2] Shone N., Ngoc T.N., Phai V.D., Shi Q.A. Deep learning approach to network intrusion detection // IEEE Transactions on Emerging Topics in Computational Intelligence. – 2018. – Vol. 2, No. 1. – P. 41–50.
- [3] Roesch M. Snort – lightweight intrusion detection for networks // Proceedings of the 13th USENIX Conference on System Administration. – 1999. – P. 229–238.
- [4] Paxson V. Bro: A system for detecting network intruders in real-time // Computer Networks. – 1999. – Vol. 31, No. 23–24. – P. 2435–2463.
- [5] Sureda Riera, T.; Bermejo Higuera, J.R.; Bermejo Higuera, J.; Martinez Herraiz, J.; Sicilia Montalvo, J.A. Prevention and Fighting against Web Attacks through Anomaly Detection Technology. A Systematic Review. Sustainability 2020, 12, 1–45.

[6] Willone Lim, Kelvin Sheng Chek Yong, Bee Theng Lau, Colin Choon Lin Tan. Computers & Security Volume 139, April 2024, 103733

[7] Ahmed M, Mahmood A.N, Hu J. A survey of network anomaly detection techniques // Journal of Network and Computer Applications. – 2016. – Vol. 60. – P. 19–31.

[8] Ahmed Youssef and Ahmed Emam. Network intrusion detection using data mining and network behaviour analysis // International Journal of Computer Science & Information Technology (IJCSIT) Vol 3, No 6, Dec 2011 – P. 87–98.

[9] Sakurada M, Yairi T. Anomaly detection using autoencoders with nonlinear dimensionality reduction // Proceedings of the MLSDA 2014: 2nd Workshop on Machine Learning for Sensory Data Analysis. – 2014. – P. 4–11.

[10] Shone N., Ngoc T.N., Phai V.D., Shi Q.A. Deep learning approach to network intrusion detection // IEEE Transactions on Emerging Topics in Computational Intelligence. – 2018. – Vol. 2, No. 1. – P. 41–50.

[11] <https://www.csec.uz>

[12] <https://medium.datadriveninvestor.com>

[13] <https://dl.acm.org>

**TURLI MASHINA VA MEXANIZMLARNING QIYALANISH BURCHAGI HAMDA
TEBRANISHLARINI ANIQLOVCHI OPTOELEKTRON DATCHIK****PhD, professor O.S. RAYIMJONOVA***Farg'ona davlat texnika universiteti*

Annotatsiya. Ushbu maqolada burchak va tomon qiyaligini aniqlovchi optoelektron datchikning konstruksiyaviy sxemasi tahlil qilingan, ushbu datchikni turli mashina va mexanizmlarda qo'llash bo'yicha ilmiy xulosa va ma'lumotlar keltirilgan.

Kalit so'zlar: burchak ko'chishi, qiyalanish burchagi, blok-sensor, rezonans chastota, birinchi tartibli difraksiya.

Аннотация. В статье проанализирована конструктивная схема оптоэлектронного датчика, определяющего угол и направление наклона, а также представлены научные выводы и сведения по использованию данного датчика в различных машинах и механизмах.

Ключевые слова: угловое смещение, угол наклона, датчик блока, резонансная частота, дифракция первого порядка.

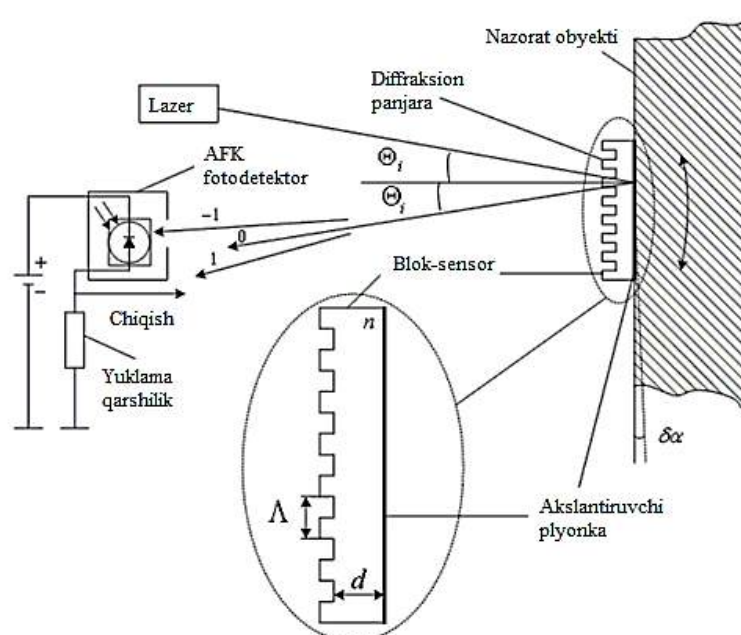
Abstract. This article analyzes the design scheme of an optoelectronic sensor that detects angle and direction of inclination, and presents scientific conclusions and information on the use of this sensor in various machines and mechanisms.

Key words: angular displacement, tilt angle, block sensor, resonant frequency, first-order diffraction.

Kirish. Turli qismlar va tuzilmalarning kichik burchakli tebranishlarini o'lchash fan va texnikaning ko'plab sohalarida amaliy qiziqish uyg'otadi. Shu maqsadda har xil turdagi sensorlar, masalan, piezoelektrik, optik tolali va ko'zgu reflektorli sensorlardan foydalanish mumkin. Ushbu maqolada biz kichik burchakli tebranishlarni o'lchash uchun original qurilmani ko'rib chiqamiz, bu ularning shaklini o'rganish, tebranish amplitudasining strukturadagi sensor blokining joylashuvi koordinatasiga va chastotaga bog'liqligini o'lchash va rezonans chastotalarini aniqlash imkonini beradi. Fotodetektor sifatida Galliy arsenidi asosidagi yuqori tezlikli AFK plyonkali fotoqabulqilgichi qo'llanilgan.

Fazali diffraksiya panjarasi asosida burchak tebranishlarini o'lchash datchiklari bir qancha izlanuvchilar tomonidan [2] da ko'rib chiqildi, bu yerda o'rganilayotgan sirtidan ajratilgan difraksion panjara yordamida burchak tebranishlarini o'lchash sxemasi o'rganildi. Ushbu sxemaning kamchiliklari panjara ushlagichining hisobga olinmagan tebranishlari tufayli o'lchov natijalarini buzish imkoniyatini o'z ichiga oladi. Yangi sensordan foydalanish qulayroq va murakkab sozlashlarni talab qilmaydi. Sensorning oldingi versiyasi bilan solishtirganda, u kamaytirilgan aks ettiruvchi yuzalarga ega, shuning uchun optik nurlarning qayta aks etishi tufayli shovqin darajasi kamayadi. Ushbu sensor faqat sirtning burchakli tebranishlariga sezgir bo'lishi va uning siljish harakatiga ta'sir qilmasligi muhimdir.

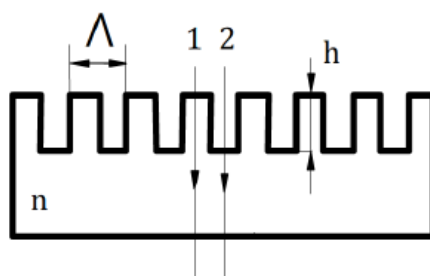
Usullar. Diagrammasi 1-rasmda ko'rsatilgan o'lchov moslamasining asosiy elementi shaffof plastinka bo'lgan blokli datchik bo'lib, uning bir tomonida meander shaklidagi profilli fazali difraksion panjara, ikkinchi tomonida esa ko'zguli aks ettiruvchi plyonka mavjud. Blok sensori o'rganilayotgan strukturaga o'rnatiladi va lazer nurlari bilan yoritiladi. Blokka yo'naltirilgan lazer nuri fazali diffraksiya panjarasi bilan parchalanadi, plastinkaning shaffof materialida tarqaladi, oyna plyonkasidan aks etadi va yana fazali panjara orqali tarqaladi. Shunday qilib, qurilmaning ishlashi meander shaklidagi profilga ega bo'lgan fazali difraksion panjara ustidagi optik nurning ikki marta diffraksiyasiga asoslangan.



1-rasm. Tuzilmalarning burchak tebranishlarini o'lash uchun optoelektron qurilmaning sxematik diagrammasi

Strukturaga o'rnatilgan datchik bloki kichik burchak $\delta\alpha$ bilan egilganida, hodisaning izlari va aks ettirilgan nurlar panjara yuzasi bo'ylab siljiydi. Agar aks ettirilgan nur ko'zgu-simmetrik bilan almashtirilsa, u holda optik nurning sensor bloki bilan o'zaro ta'sirini tahlil qilish sensor blokining $2d$ qalinligiga teng masofada joylashgan ikkita panjaraning ekvivalent sxemasini tahlil qilish bilan almashtirilishi mumkin. To'liq uzunligi λ bo'lgan tekis to'liq jabhasi fazali difraktsion panjaradan o'tganda, fazoviy fazali modulyatsiya (SPM) amplitudali Φ_M bilan hosil bo'ladi, bu panjaraning chiqishi va chuqurchasidan o'tadigan nurlar orasidagi fazalar farqining yarmiga teng (2-rasm).

$$\Delta\alpha = \frac{\Delta U}{S_{U\alpha}}$$



2-rasm. Optik nurlanishning diffraksiya panjarasining cho'qqi va chuqurchasi orqali o'tishi

$$I_{\pm 1}(\Delta x) = 2a_0^2 a_1^2 + 2a_0^2 a_1^2 \cos\left(\frac{2\pi}{\Lambda} \Delta x \pm L\right). \quad (1)$$

(2) ifoda nurning normal tushishi uchun yozilgan. Unda $a_0 = \cos(\Phi_M)$ va $a_1 = \frac{2}{\pi} \cos(\Phi_M)$ - meander shakliga ega bo'lgan fazali panjaraning o'tkazish funksiyasining Fyurje seriyasida kengayish koeffitsientlari, $L = 2d\pi \frac{\lambda}{n\Lambda^2}$ qiymati - sensorga mos keladigan o'lchamsiz masofa parametri R (2-rasmdagi plyonkaning koeffitsientini aks ettirish va ko'rsatishni soddalashtirish uchun). hodisa to'liqining intensivligi I_{tush} birliklarga teng qabul qilinadi.

Ifodaning ikkinchi hadi (2) $I_{\pm 1}(\Delta x)$ bog'liqlikning o'zgaruvchan komponenti bo'lib, uning amplitudasi

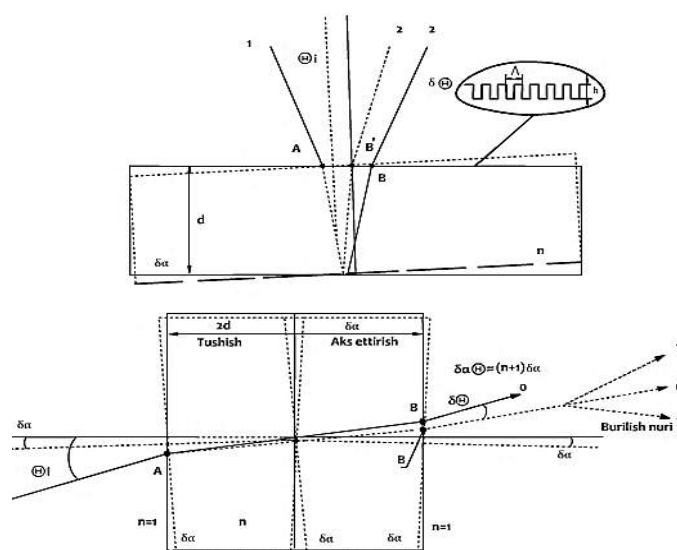
$$I_{\pm 1}^{\approx} = 2a_0^2 a_1^2 = \frac{2}{\pi^2} \sin^2(2\Phi_M) \text{ ga teng.} \quad (2)$$

Bu qiymat amplitudasining maksimal qiymatiga $\Phi_M = \frac{\pi}{4}$ da erishiladi.

Φ_M ning bu qiymati va relyefning fizik chuqurligining mos keladigan qiymati h optimal hisoblanadi, chunki bu holda ushbu bog'liqlikning chiziqli qismining tikligining maksimal qiymatiga erishiladi. $\Phi_M^{opt} = \frac{\pi}{4}$ dagi (2) ifoda

$$I_{\pm 1}(\Delta x) = \frac{2}{\pi^2} + \frac{2}{\pi^2} \cos\left(\frac{2\pi}{\Lambda} \Delta x \mp L\right) \text{ ko'rinishini oladi.} \quad (3)$$

Optimal relyef chuqurligining sonli bahosini beraylik. $\Phi_M^{opt} = \frac{\pi}{4}$, $\lambda = 0,65 \text{ } \mu\text{m}$, $n = 1,51$ (shisha) qiymatlari uchun optimal relyef chuqurligi $h = 0,319 \text{ } \mu\text{m}$. Formula (3)da optik nur izining panjara bo'ylab siljishi Δx egilish burchagi $\delta\alpha$ ga mutanosib bo'ladi, shuning uchun datchik blokining egilish burchagiga birinchi tartibli intensivliklarning bog'liqliklari ham garmonik funktsiyalar bilan tavsiflanadi. 3-rasm yordamida Δx va $\delta\alpha$ o'rtasidagi bog'liqlikni topamiz, unda kichik burchakka (a) egilgandagi sensor blokining ko'rinishi va tahlil uchun ekvivalent sxema (b) ko'rsatilgan.



3-rasm. Nurning qiya tushishi uchun blok-sensor diagrammasi (a).

Sinishi ko'rsatkichi n (b) bo'lgan muhitdagi ikkita panjaraning ekvivalent diagrammasi

Chiziqli siljish Δx ikki muhitning interfeysidagi sinishi hisobga olingan holda sensorni $\delta\alpha$ burchak ostida egishdan oldin va keyin hodisa izlari va aks ettirilgan nurlar orasidagi masofalar farqi sifatida aniqlanadi:

$$\Delta x = AB - AB' = 2d \left\{ \tan\left(\frac{\Theta_i}{n}\right) - \tan\left(\frac{\Theta_i - \delta\alpha}{n}\right) \right\} \approx 2d \frac{\delta\alpha}{n} \quad (4)$$

(4) munosabat kichik burchaklar uchun to'g'ri keladi Θ_i va d .

Oxirgi ifodadan (4) foydalanib, optik nurlar izi siljishi Δx datchik blokining qiyshayishiga kichik burchak d a bilan bog'liq bo'lib, birinchi difraksiya tartiblari intensivliklarining

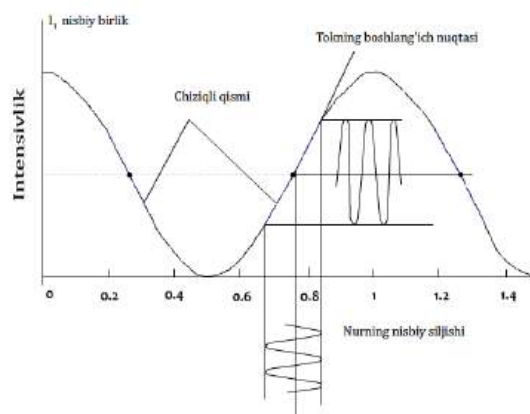
$$I_{\pm 1}(\delta\alpha) = \frac{2}{\pi^2} + \frac{2}{\pi^2} \cos\left(\frac{4\pi d}{n\Lambda} \Delta x \mp L\right) \quad (5)$$

ga bog'liqliklari ifodalarini olamiz.

Farqlovchi ifoda (5), biz datchik bloking egilish burchagi o'zgarishi bilan intensivlik o'zgarishining o'zgarishining tikligining maksimal qiymatini aniqlaymiz

$$S_{I\alpha \max} = \left| \frac{dI_{\pm 1}}{d(\delta\alpha)} \right|_{\max} = \frac{8d}{\pi n\Lambda} \quad (6)$$

Kichik burchakli tebranishlarni qayd qilish va o'lchash uchun birinchi diffraksiya tartiblaridan birining intensivligining $I_{\pm 1}(\delta\alpha)$ datchikning egilish burchagiga yoki boshqacha aytganda $I_{\pm 1}(\Delta x)$ nur izining ekvivalent siljishiga garmonik bog'liqligining ko'p chiziqli kesimlaridan biri qo'llaniladi. Ekvivalent nur izi siljishiga bog'liqlik 4-rasmda ko'rsatilgan. Qurilmaning ishlashi uchun ish nuqtasi chiziqli kesimning o'rtasida joylashganligini ta'minlash kerak. Bunga tushishning dastlabki burchagini tanlash orqali erishiladi.



4-rasm. Birinchi diffraksiya tartibi intensivligining panjaralarning nisbiy siljishiga bog'liqligi. Ishlash nuqtasi chiziqli qismning o'rtasida joylashgan

Optik nurning tushishining dastlabki burchaklarini hisoblash. $I_{\pm 1}(\Delta x)$ bog'liqlikning chiziqli kesimining o'rtasidagi ish nuqtasining holatiga mos keladigan tushish burchaklarini Θ_{ik} deb belgilaymiz. Θ_{ik} ni hisoblash formula (5) yordamida, $\delta\alpha$ burchagini Θ_{ik} burchak bilan almashtirib, kosinus argumentini $\frac{\pi}{2} + \pi k$ qiymatiga tenglashtirish orqali amalga oshirilishi mumkin. Natijada Θ_{ik} ni hisoblash uchun

$$\Theta_{ik} = \frac{n\Lambda}{8d} (1 + 2k), \quad k = 0, 1, 2 \text{ ifodani olamiz.} \quad (7)$$

Amalda, tushish burchagi kalibrlovch vaqtida aniqlandi, uning usuli quyida tavsiflanadi.

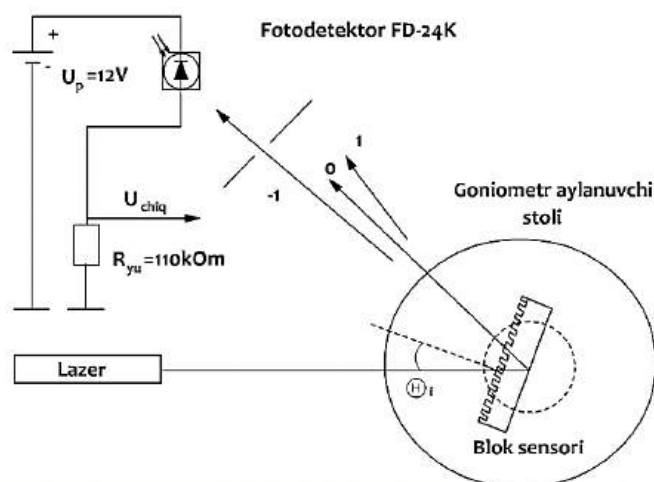
Natijalar. Tajribalarni o'tkazish uchun 1-jadvalda keltirilgan turli parametrlarga ega sensor bloklarining namunalari ishlab chiqarildi.

1-jadval

Tajribalarda ishlatiladigan sensor bloklarining parametrlari

N ₂	1-sensor	2-sensor	3-sensor	4-sensor
1	$\Lambda=100 \mu\text{m}$	$\Lambda=200 \mu\text{m}$	$\Lambda=100 \mu\text{m}$	$\Lambda=200 \mu\text{m}$
2	$d=7,5 \text{ mm}$	$d=11,2 \text{ mm}$	$d=1,5 \text{ mm}$	$d=7,2 \text{ mm}$
3	$\Phi_M=22^\circ$	$\Phi_M=40^\circ$	$\Phi_M=38^\circ$	$\Phi_M=40^\circ$

Statik xususiyatlarni o'lchash va sensorlarni kalibrlash. Sensor bloklarini ishlab chiqargandan so'ng, statik xususiyatlarni o'lchash va sensorlarni kalibrlash amalga oshirildi. O'lchov sxemasi 5-rasmida ko'rsatilgan.



5-rasm. Statik xususiyatlarni o'lchash va sensorni kalibrlash sxemasi

Statik xususiyatlarni o'lchashda blok sensori goniometrning aylanuvchi stoliga joylashtirildi, shunda panjara chiziqlari stolning aylanish o'qiga parallel bo'ladi. Shundan so'ng, nurning kichik boshlang'ich tushish burchagi o'rnatildi va stolni $\delta\alpha$ burchagi bilan aylantirib, birinchi diffraksiya tartibidagi fotodetektorlarning yuklaridagi chiqish kuchlanishlari o'lchandi. O'lchovlar $\delta\alpha = 1'$ qadam bilan amalga oshirildi, tushishning boshlang'ich burchagi $\Theta_{ik} = 4^0$ ga teng edi. 6b-rasmida birinchi diffraksiya tartiblarining intensivliklarining 1-sonli datchik uchun aylanish burchagiga hisoblangan bog'liqliklari ko'rsatilgan (qalinligi $d = 7,5$ mm). 1-sonli sensorning eksperimental va nazariy bog'liqliklari bir-biriga yaxshi mos keladi. Datchiklarni kalibrlash statik xususiyatlarni o'lchash bilan bir vaqtda amalga oshirildi. Sensorni kalibrlash quyidagi operatsiyalarni o'z ichiga oladi:

a) datchikning burilish burchagiga birinchi diffraksiya tartibi quvvatining garmonik bog'liqligining ko'plab chiziqli bo'limlaridan birining o'rtasida joylashgan ish nuqtasining holatiga mos keladigan tushish burchagini aniqlash Θ_i ,

b) datchikning aylanish burchagi o'zgarganda chiqish signalining ΔU o'zgarishining $S_{U\alpha}$ o'zgarishining keskinligini aniqlash.

Nurning tushishining dastlabki burchagi Θ_i shunday tanlanganki, birinchi tartibli difraksion nurning kuchi uning maksimal va minimal qiymatlari orasidagi o'rtacha qiymatga teng bo'ladi. Fotodetektor yukidagi oqim va kuchlanish tushayotgan nurlanish kuchiga mutanosib bo'lganligi sababli, amalda ish nuqtasi kontaktlarning zanglashiga olib chiqishdagi doimiy kuchlanish darajasi bilan o'rnatildi, u

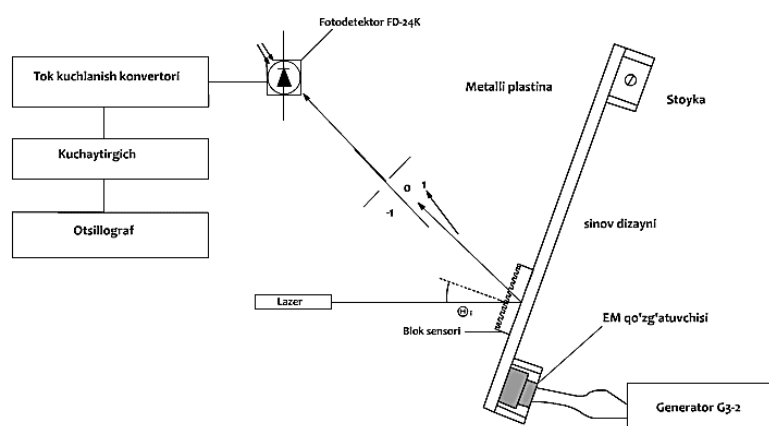
$$U_{o'rt} = \frac{U_{max} + U_{min}}{2} \text{ ga teng bo'lishi kerak,} \quad (8)$$

bu yerda U_{max} va U_{min} chiqish signali kuchlanishining maksimal va minimal qiymatlari.

Ishlash nuqtasini chiziqli qismning o'rtasiga o'rnatgandan so'ng, konvertatsiya qiyaligi kalibrlangan. Buning uchun sensor bloking $\pm \delta\alpha$ aylanishining kichik o'sishini berish orqali $\pm \Delta U$ o'sishlari o'lchandi va keyin ushbu sensor bloki uchun konvertatsiya qiyaligi $S_{U\alpha} = \frac{\Delta U}{\delta\alpha}$ hisoblab chiqildi. Sensor 1 uchun o'lchangan nishab qiymati $S_{U\alpha} = 0,675$ V / mrad edi.

Struktura tebranishlarini o'lchash natijalari. Sensorni amalda qo'llashning vizual namunasi sifatida ikkita vertikal ustunga o'rnatilgan metall novda bo'lgan mos yozuvlar strukturasi

burchakli tebranishlari o'Ichandi. Postlardan biriga elektromagnit qo'zg'atuvchi o'rnatildi, u $F = 20$ Hz dan $F = 1$ kHz gacha bo'lgan chastotali plastinkadagi tebranishlarni qo'zg'atdi. Tashqi tebranish manbai sifatida past chastotali generator G3-2 ishlatilgan. Eksperimental o'rnatish sxemasi 6-rasmda ko'rsatilgan.

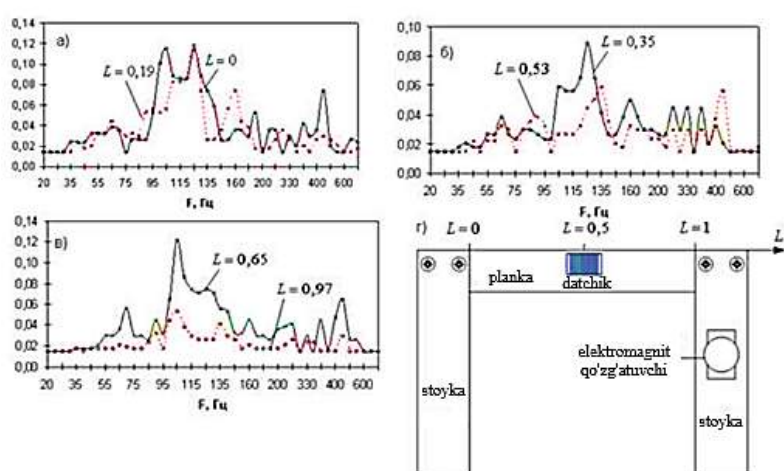


6-rasm. Tayanch konstruksiyaning burchak tebranishlarini o'Ichash uchun eksperimental qurilmaning sxematik diagrammasi

Tajriba davomida blok sensori turli nuqtalarda metall barga yopishtirilgan. Kalibrlash vaqtida chiziqli kesimning o'rtasiga to'g'ri keladigan tushish burchagi aniqlandi. Ushbu burchakdagi sensorga lazer nuri yo'naltirildi. Olingan diffraksiya naqshida birinchi tartiblardan biri ajratilgan va fotodetektorga yo'naltirilgan. Kuchaytirilgandan so'ng, fotodetektor chiqishidan signal osiloskopga yuborildi. Sensorni kalibrlash va chiqish signalining amplitudasini o'Ichash jarayonida aniqlangan

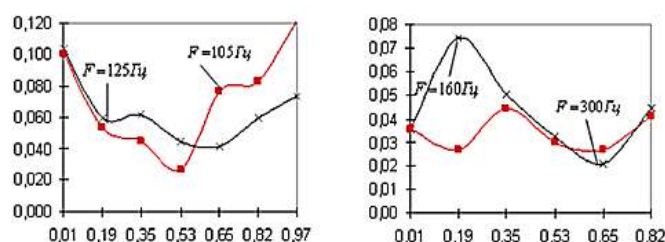
$S_{U\alpha}$ transformatsiyasining keskinligini bilib, biz $\Delta\alpha = \frac{\Delta U}{S_{U\alpha}}$ metall konstruksiyasining burchak

tebranishlarining amplitudasini hisoblab chiqdik. Qo'zg'alish chastotasini va blok sensorining strukturadagi o'rnini o'zgartirib, biz uning turli nuqtalarida barning burchakli tebranishlari amplitudasining chastotaga bog'liqligini o'Ichadik. Sensor 1 yordamida o'tkazilgan tajribalar natijalari 7a, 7b, 7c-rasmda ko'rsatilgan. Tebranishlarning rezonans chastotalarini 7-rasmdagi grafiklardan osongina aniqlash mumkin. Shunday qilib, barcha grafiklarda $F = 95-120$ Hz mintaqasidagi tebranishlarning rezonans mintaqasi aniq ko'rinadi.



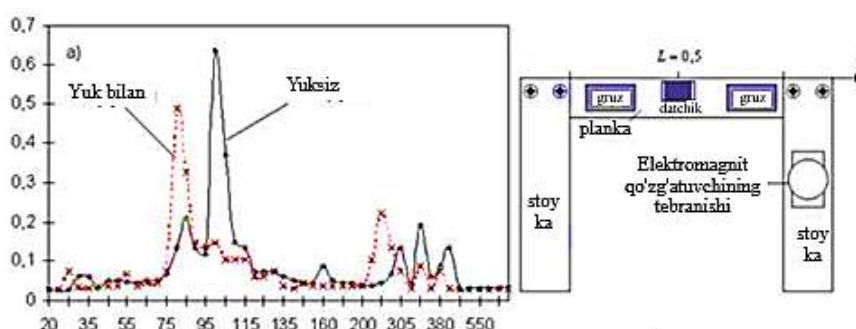
7-rasm. Burchak tebranishlari amplitudalarining strukturadagi sensorning turli pozitsiyalarida tashqi qo'zg'alish chastotasiga bog'liqligi: (a, b, c). Datchikning metall chiziqdagi turli nuqtalarda joylashishi diagrammasi shakl (d) da ko'rsatilgan

Sensor kichik bo'lgani uchun uni struktura bo'ylab osongina siljitish mumkin. Shu tarzda, strukturaning turli nuqtalarida tebranishlarning taqsimlanishi belgilangan chastotalarda o'lchandi. O'lchov natijalari to'rt chastotali qiymat uchun 8-rasmda ko'rsatilgan: $F = 105 \text{ Hz}$, $F = 125 \text{ Hz}$, $F = 160 \text{ Hz}$ va $F = 300 \text{ Hz}$.



8-rasm. Datchikning turli pozitsiyalarida burchakli tebranishlar amplitudalarining qattiq chastotalardagi strukturaga bog'liqligi (a, b).

O'tkazilgan tadqiqotlarga qo'shimcha ravishda, massasi ko'tarilgan strukturaning tebranishlarini o'lchash uchun maxsus tajriba o'tkazildi. Ushbu tajribada 8b-rasmda ko'rsatilganidek, konstruksiyaga qo'shimcha yuk biriktirildi va konstruksiyaning tebranish amplitudasining yuk bilan chastotasiga bog'liqliklarining o'lchovlari olindi. Ushbu o'lchovlarning natijalari 8a-rasmda ko'rsatilgan. Tebranish tuzilmalarining turli massalariga mos keladigan ikkita eksperimental egri chiziqlarni taqqoslashdan ma'lum bo'ladi, struktura massasining ortishi bilan rezonans chastotalarining pasayishi sodir bo'ladi. Bu fakt nazariyaga juda mos keladi.



9-rasm. Burchakli tebranishlar amplitudalarining turli xil massali tuzilmalar uchun tashqi qo'zg'alish chastotasiga bog'liqligi

Xulosa. Ushbu ishda optoelektron usulga asoslangan vibratsiyani aniqlash tizimi ishlab chiqildi va sinovdan o'tkazildi. GaAs asosidagi AFK plyonkali fotoqabulqilgich yordamida kontaktisiz tarzda tebranish signalini qabul qilish, uni mikrokontroller orqali raqamlashtirish va tezkor chastota tahlili (FFT) yordamida tahlil qilish amaliyotga joriy qilindi. Taklif qilingan sensor tebranish amplitudasining chastotaga bog'liqligini o'lchash, rezonans chastotalarni aniqlash, tebranish amplitudasining strukturadagi sensorning joylashuvi koordinatasiga bog'liqligini o'rganish, shuningdek, tebranishlar shaklini o'rganish imkonini beradi. U katta o'lchamli konstruksiyalarning past chastotali tebranishlarini o'rganish uchun amaliyotda qo'llanilishi mumkin. O'lchov moslamasining o'ziga xos xususiyati shundaki, u juda past chastotalar bilan tebranishlarni nol chastotalargacha yozib olish qobiliyatiga ega.

Sensorni ishlab chiqarish texnologiyasi va eksperimental metodologiyasi juda oddiy. Sensorning eksperimental ravishda o'lchangan chegara sezgirligi 0 Hz dan 1000 Hz gacha bo'lgan yozish kanali diapazoni bilan milliradianing yuzdan bir qismini tashkil etdi. Sensor konstruksiyalarning translatsion tebranishlariga va fotodetektorning tasodifiy tebranishlariga sezgir emas va nisbiy birliklarda emas, balki mutlaq burchak birliklarida ifodalangan natijalarni olish imkonini beradi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

- [1] Азимов Р.К., Шипулин Ю.Г., Шипулин Ш.Ю., Холматов У.С., Райимжонова О.С., Абдуллаев Т.М., Исмаилов Х.А. Оптоэлектронные датчики угла и направления наклона. // Патент на изобретение № IAP 05561.
- [2] Азимов Р.К., Шипулин Ю.Г., Райимжонова О.С., Максудов С.А., Оптоэлектронный преобразователь угловых перемещений. Международная научно конференция // Innovation 2014. Тошкент. с. 231-233.
- [3] Шипулин Ю.Г., Райимжонова О.С., Холматов У.С., Абдуллаев Т.М., Физические модели и характеристики оптоэлектронных преобразователей угла наклона технологических установок. // Научный вестник Машиностроение г. Андижан, №2. 2016 – с.245-252.
- [4] В.А. Комоцкий, Ю.М. Соколов. Оптоэлектронный измеритель угловых колебаний конструкций. Вестник РУДН, Серия Математика. Информатика. Физика. № 1–2. 2007. с. 138–146.
- [5] В.А. Комоцкий, Ю.М. Соколов Оптоэлектронное устройство для измерения угловых колебаний конструкций. — Патент на полезную модель (приоритет от 23.05.2006 по заявке № 2006117556).
- [6] В.А. Комоцкий, В.Ф. Никулин Бесконтактный дифракционный метод измерения угловых смещений и вибраций отражающих поверхностей // Оптика и спектроскопия. — Т. 72, № 2. — 1992. — с. 479–486.
- [7] А. Ниибизи, В.А. Комоцкий Теоретический анализ взаимодействия оптической волны с системой пространственно разделенных периодических решеток // ВИНТИ № 661-B86. — 1985. Komilov Davron Rashidjon ugli. Process Control in Manufacturing. Miasto Przyszłości. Kielce 2024. Vol. 54.–6. 1160-1163.
- [8] O.S. Rayimjonova, U.U. Iskandarov, D.R. Komilov. Optical transmission system design in matlab simulink. “Aniq va tabiiy fanlarni rivojlantirishda raqamli texnologiyalarning oʻrni: muammolar va innovatsion yechimlar” mavzusidagi xalqaro ilmiy-texnik konferensiya materiallar toʻplami 2-qism 4-5 oktyabr 2024 yil. Fargʻona-2024. 6.313-318.

TROPOSFERADA MUHITIDA TO‘LQIN TARQALISHINING MODELI VA DASTURIY APPARATINI ISHLAB CHIQISH

PhD B.O. TUYCHIYEV

Qarshi davlat texnika universiteti

Annotatsiya. *Ushbu tadqiqotda troposfera muhitida elektromagnit to‘lqinlarning tarqalish jarayonini modellashtirish va uni tahlil qilish uchun matematik model hamda dasturiy-apparat platformasi ishlab chiqildi. Troposferaning fizik xususiyatlari - harorat, bosim, namlik va turli xil fluktuatsiyalar - to‘lqinlarning yoyilishiga sezilarli ta’sir ko‘rsatadi. Mazkur ishda ushbu parametrlar hisobga olingan holda deterministik va statistik modellar ishlab chiqildi. Shuningdek, MATLAB va Python muhitida algoritmlar tuzilib, to‘lqin intensivligi, yo‘qotishlar, tarqalish burchagi kabi parametrlar grafik ko‘rinishda vizualizatsiya qilindi. Amaliy jihatdan bu model aloqa tizimlarida yuqori chastotali signallarning ishonchli tarqalishini baholash, shuningdek, signal sifati va xalaqit koeffitsientini tahlil qilish imkonini beradi. Taklif etilgan platforma real vaqt rejimidagi meteorologik ma’lumotlarni integratsiyalash orqali moslashuvchan ishlash imkoniyatiga ega. Tadqiqot natijalari meteorologiya, radiolokatsiya va simsiz aloqa tizimlarida qo‘llanish uchun muhim ilmiy va amaliy ahamiyatga ega.*

Kalit so‘zlar: *elektromagnit to‘lqin, troposfera, matematik model, algoritm, mexanizm, radioaloqa, radiouzatish va qabul qilish, dastueiy apparat.*

Bugungi kunda troposferada to‘lqinlarning tarqalishini modellashtirish uchun bir necha nazariy modellardan foydalaniladi. Ular orasida eng mashhurlari — Frissning erkin fazoda signal yo‘qolishini hisoblash modeli (Free Space Path Loss — FSPL), ITU-R tomonidan ishlab chiqilgan xalqaro tavsiyalar asosidagi modellar, shuningdek shahar sharoitidagi to‘lqin tarqalishini tahlil qiluvchi Okumura-Hata hamda COST231 modellari sanaladi. Ushbu modellar orqali turli balandlikda, chastotada va muhit sharoitlarida to‘lqinlarning qanday tarqalishini oldindan prognoz qilish va optimallashtirish mumkin bo‘ladi. Troposferadagi elektromagnit to‘lqinlarning tarqalishiga oid nazariy, eksperimental va modellashtirishga asoslangan tadqiqotlar har qanday aloqa tizimi loyihalashtirishda ilmiy asos bo‘lib xizmat qiladi.

Ushbu tadqiqotda troposfera muhitining asosiy fizik xossalari, ularga ta’sir etuvchi omillar, to‘lqinlarning bu muhitda qanday tarqalishi, shuningdek yuqorida zikr etilgan modellar asosida hisob-kitoblar va grafik tahlillar o‘rganiladi. Bundan tashqari, Python dasturlash tilida Tkinter GUI kutubxonasi yordamida ko‘p modelni qo‘llab-quvvatlovchi, grafik va jadval asosida natijalarni ko‘rsata oluvchi maxsus dasturiy vosita — “To‘lqin Signal Tahlilchi” ishlab chiqiladi. Bu vosita orqali foydalanuvchi chastota, masofa, antennalar balandligi kabi parametrlarni kiritgan holda, bir nechta model asosida signal yo‘qotishlarini real vaqt rejimida vizual ko‘rish imkoniyatiga ega bo‘ladi.

Yer sayyorasini o‘rab turgan atmosfera bir nechta qatlamlardan tashkil topgan bo‘lib, ularning har biri o‘ziga xos fizik-kimyoviy xususiyatlarga ega. Ushbu qatlamlar orasida troposfera eng pastki qatlam bo‘lib, inson faoliyati bilan eng bevosita bog‘liq bo‘lgan, hayot uchun zaruriy bo‘lgan elementlar va hodisalarning asosiy manbai hisoblanadi. Troposfera so‘zi yunon tilidan olingan bo‘lib, “o‘zgaruvchan qatlam” degan ma’noni anglatadi. Bu nom bejiz berilmagan, chunki ob-havo hodisalari, shamollar, yog‘ingarchilik, bulutlar va boshqa iqlim jarayonlari aynan troposferada sodir bo‘ladi. Uning balandligi ekvator sohasida 17–18 kilometrgacha, qutblarda esa 7–9 kilometr atrofida bo‘ladi. Ushbu qatlam butun atmosferaning 75–80 foiz gaz massasini o‘z ichiga oladi. Shuningdek, suv bug‘larining deyarli 99 foizi ham aynan shu qatlamda to‘plangan bo‘ladi. Bu esa uni iqlim va suv aylanishi tizimining yuragi sifatida ko‘rsatadi.

Troposferaning asosiy kimyoviy tarkibiy qismlari azot (taxminan 78%) va kislorod (taxminan 21%) hisoblanadi [7]. Qolgan 1% argon, suv bug‘i, karbonat angidrid va boshqa gazlarning

aralashmasidan iborat [2]. Suv bug'i troposferaning muhim tarkibiy qismi bo'lib, uning miqdori haroratga va geografik joylashuvga qarab sezilarli darajada o'zgarishi mumkin [7].

Troposferada radio to'lqinlarining tarqalishi asosan yer to'lqinlari (sirt va fazoviy to'lqinlar) va troposfera sinishi orqali sodir bo'ladi. [2] yer to'lqinlari yer sirti bo'ylab tarqaladi va past chastotalarda diffraksiya tufayli gorizontdan tashqariga ham o'tishi mumkin. Sirt to'lqinlari yer konturi bo'ylab diffraksiya orqali harakatlanadi, fazoviy to'lqinlar esa havo orqali to'g'ridan-to'g'ri qabul qiluvchi antennaga tarqalishi yoki yer sirtidan qaytishi mumkin. Vertikal polarizatsiya yer to'lqinlari uchun gorizont polarizatsiyaga qaraganda kamroq susayish bilan afzalroqdir [2].

Fazoviy to'lqinlar to'g'ridan-to'g'ri qabul qiluvchi antennaga tarqalishi yoki yer sirtidan qaytishi mumkin. [2] Troposfera sinishi atmosferaning balandlik bo'ylab sinish koeffitsientining o'zgarishi tufayli radio to'lqinlarining egilishiga olib keladi. [3] Odatda, sinish koeffitsienti balandlik oshishi bilan kamayadi, bu to'lqinlarning yerga qaytib egilishiga olib keladi. [3]

Troposfera kanal hosil qilishi (ducting) VHF va undan yuqori chastotalarda uzoq masofalarga tarqalishga imkon beradi. Bu harorat inversiyasi natijasida yuzaga keladi, bunda balandlik oshishi bilan harorat pasayishi o'rniga ortadi. [4] Kanal hosil bo'lishi, ayniqsa yoz va kuz oylarida, turli harorat va namlikdagi havo massalari chegarasida sinish koeffitsientining o'zgarishi natijasida yuzaga keladi [4].

Troposfera sochlanishi (troposcatter) UHF va SHF chastotalarida troposferaning yuqori qatlamlaridagi turbulentlik tufayli radio to'lqinlarining tasodifiy sochilishidir, bu gorizontdan tashqariga aloqa o'rnatishga imkon beradi. [5] Ushbu usulda radio signallari gorizontdan biroz yuqoriga qarab yo'naltirilgan tor nurda uzatiladi va troposfera orqali o'tayotganda energiyaning bir qismi yerga qaytib sochiladi, bu esa qabul qiluvchi stantsiyaga signalni qabul qilishga imkon beradi. [6].

Troposferadagi ob-havo sharoitlari radio to'lqinlarining tarqalishiga sezilarli ta'sir ko'rsatadi. [4] Yuqori bosimli ob-havo uzoq masofalarga tarqalishni kuchaytirishi mumkin. [4] Chastota qanchalik yuqori bo'lsa, radio to'lqinlarining yer egriligi bo'ylab tarqalishi shunchalik qiyinlashadi va zich materiallarga kirib borish qobiliyati kamayadi.

Elektromagnit to'lqinlar o'zaro perpendikulyar yo'nalishda tebranuvchi elektr va magnit maydonlardan tashkil topgan bo'lib, fazoda energiyaning olib o'tadi. Ushbu to'lqinlarning tarqalish yo'nalishi elektr va magnit maydonlarining tebranish yo'nalishlariga nisbatan to'g'ri burchak ostida bo'ladi. Radio to'lqinlar elektromagnit spektrning eng past chastotali qismida joylashgan bo'lib, spektrning boshqa qismlariga nisbatan eng uzun to'lqin uzunliklariga ega.

Radio to'lqinlarining asosiy xususiyatlari orasida ularning chastotasi, to'lqin uzunligi, amplitudasi, tarqalish tezligi, polarizatsiyasi va fazaviy burchagi mavjud. [9] Chastota (ν) va to'lqin uzunligi (λ) o'zaro teskari proporsionaldir va vakuumdagi yorug'lik tezligi (c) orqali bog'langan: $c = \lambda \nu$. [9] Bu munosabat shuni ko'rsatadiki, to'lqin uzunligi qanchalik katta bo'lsa, chastota shunchalik past bo'ladi va aksincha. [9] Elektromagnit to'lqinning energiyasi uning chastotasi bilan to'g'ridan-to'g'ri bog'liqdir. [7].

Radio to'lqinlarining uzun to'lqin uzunligi ularga atmosferada kamroq so'rilishga imkon beradi, bu xususiyat uzoq masofalarga tarqalish uchun juda muhimdir. Chastota va energiya o'rtasidagi to'g'ridan-to'g'ri bog'liqlik radio to'lqinlarining energiyasi mikroto'lqin va infraqizil to'lqinlarga qaraganda pastroq ekanligini tushuntiradi. [7] Barcha elektromagnit nurlanish, shu jumladan ko'rinadigan yorug'lik, davriy ravishda tebranadi va o'ziga xos amplitudaga, to'lqin uzunligiga va chastotaga ega bo'lib, bu nurlanishning yo'nalishini, energiyasini va intensivligini belgilaydi. [9].

Elektromagnit to'lqinning tezligi, amplitudasi, chastotasi, fazaviy burchagi, polarizatsiyasi va tarqalish yo'nalishi kabi bir qator fundamental xususiyatlari mavjud. To'lqin uzunligi va chastota o'rtasidagi munosabat $c = \lambda \nu$ formulasi bilan ifodalanadi, bu erda c – yorug'lik tezligi, λ – to'lqin uzunligi va ν – chastota.

Troposferada tarqalish mexanizmlari troposferada radio to'liqlarining tarqalishi asosan yer to'liqlari (sirt va fazoviy to'liqlar) va troposfera sinishi orqali sodir bo'ladi. Yer to'liqlari yer sirti bo'ylab tarqaladi va past chastotalarda diffraksiya tufayli gorizontdan tashqariga ham o'tishi mumkin. [2] Sirt to'liqlari yer konturi bo'ylab diffraksiya orqali harakatlanadi, fazoviy to'liqlar esa havo orqali to'g'ridan-to'g'ri qabul qiluvchi antennaga tarqalishi yoki yer sirtidan qaytishi mumkin. [2] Vertikal polarizatsiya yer to'liqlari uchun gorizont polarizatsiyaga qaraganda kamroq susayish bilan afzalroqdir [2].

Troposfera sinishi difraksiya yo'nalishiga ozgina ta'sir ko'rsatishi mumkin. Atmosferadagi turbulentlik tufayli yuzaga keladigan sinish koeffitsientining kichik o'zgarishlari difraksiya naqshiga ta'sir qilishi mumkin. Troposferaning difraksiyaga ta'siri unchalik katta emas, lekin uzoq masofalarga tarqalishda hisobga olinishi kerak.

1-jadval

Elektromagnit spektrning troposfera bilan o'zaro ta'siri

To'liq tur	Chastota diapazoni	To'liq uzunligi diapazoni	Troposferada tarqalish mexanizmlari	Troposferada asosiy qo'llanilishi
Radio to'liqlar	3 kHz - 300 GHz	1 mm - 100 km	Yer to'liqlari (sirt, fazoviy), Troposfera sinishi, Kanal hosil qilish, Sochilish	Radioeshittirish, Televideniye, Mobil aloqa, Radar, Sun'iy yo'ldosh aloqasi
Mikro-to'liqlar	300 MHz - 300 GHz	1 mm - 1 m	To'g'ri chiziqli tarqalish, Sochilish, Kanal hosil qilish	Radar, Sun'iy yo'ldosh aloqasi, Mobil aloqa, Mikroto'liqli pechlar, Wi-Fi
Infraqizil to'liqlar	300 GHz - 430 THz	700 nm - 1 mm	So'rilish, Sochilish, Atmosfera derazalari orqali o'tish	Termal tasvir, Masofaviy zondlash, Ob-havo prognozi, Astronomiya

Troposferada radio to'liqlarining tarqalishiga ta'sir ko'rsatadigan muhim omillardan biri yog'ingarchilikdir. Yomg'ir, qor va do'l kabi yog'inlar radio to'liqlarining tarqalishini bir necha mexanizm orqali buzishi mumkin.[7]

Birinchidan, yog'ingarchilik tarkibidagi suv molekulalari radio to'liq energiyasining bir qismini yutadi, bu esa signal quvvatining kamayishiga olib keladi.[8] Bu absorbsiya yuqori chastotalarda yanada sezilarli bo'ladi, chunki suv molekulalari bilan o'zaro ta'sir kuchayadi. Ikkinchidan, yomg'ir tomchilari radio to'liqlarini har xil yo'nalishlarda sochib yuboradi, bu esa qabul qiluvchiga yetib boradigan signal quvvatini kamaytiradi.[8] Yomg'ir tomchilarining o'lchami to'liq uzunligiga yaqin bo'lganda sochilish ayniqsa kuchli bo'ladi.[7] Yomg'ir tomchilarining o'lchami va shakli sochilish intensivligiga ta'sir qiladi.[7] Nosferik shakldagi tomchilar elektromagnit to'liqning polarizatsiyasini ham o'zgartirishi mumkin. Bu depolarizatsiya hodisasi radio qabul qilish sifatiga ta'sir qilishi mumkin, lekin ba'zida vertikal antenna yordamida qabul qilishni yaxshilash uchun ishlatilishi ham mumkin.

Modellashtirish yondashuvlarining xilma-xilligi troposferada to'liqlarning tarqalishining murakkabligini ta'kidlaydi. Har bir usul o'zining taxminlari va cheklovlariga ega bo'lib, uni muammolarning muayyan turlari uchun mos qiladi. Gibrid modellarning rivojlanishi ularning o'zaro to'ldiruvchi kuchli tomonlarini birlashtirish orqali yagona usullarning individual cheklovlarini bartaraf etishga qaratilgan sa'y-harakatlarni aks ettiradi.

Simulyatsiya usullari (Simulation Methods)

Bo'linish qadamli Furiye usuli (Split-Step Fourier Method):

Bo'linish qadamli Furiye usuli (BQFU) parabolik tenglamani hal qilish uchun keng qo'llaniladigan usul bo'lib, yuqori hisoblash tezligi va barqaror ishlashi tufayli ajralib turadi.[8] Bu usul, ayniqsa, uzoq masofalarga tarqalish stsenariylarini simulyatsiya qilish uchun samaralidir.[9]

BQFUning asosiy qismi kichik masofa qadamlari bo'ylab yechimni samarali tarzda ilgari surish uchun Tez Furiye Transformatsiyasidan (TFT) foydalanishga asoslanadi.[8] Usul, mohiyatan, to'liqning sayohatini fazoviy sohada sinish ko'rsatkichining ta'sirini qo'llash va to'liqning bo'shliqda tarqalishini hisoblash uchun Furiye (to'liq soni) sohasiga o'tish o'rtasida almashinuvchi qadamlar seriyasi sifatida simulyatsiya qiladi.

Algoritm: BQFU algoritmi odatda quyidagicha davom etadi [2]:

Boshlang'ich masofadagi elektromagnit maydon TFT yordamida Furiye sohasiga o'tkaziladi. Bu to'liqning burchak spektrini ifodalaydi.

Furiye sohasida kichik masofa qadami (Δx) bo'ylab bo'shliqda tarqalish tufayli fazaviy o'zgarishlar qo'llaniladi. Bu qadam to'liqning diffraksiyasini hisobga oladi.

Maydon teskari TFT yordamida fazoviy sohaga qayta o'tkaziladi.

Fazoviy sohada atmosfera sinish ko'rsatkichidagi o'zgarishlar tufayli xuddi shu masofa qadami (Δx) bo'ylab fazaviy o'zgarishlar qo'llaniladi.

Ushbu qadamlar iterativ ravishda takrorlanadi, yechim kerakli tarqalish masofasiga yetguncha masofa bo'ylab oldinga siljiydi.

BQFU keng burchakli tarqalishni, standart parabolik tenglamaning tor burchakli yaqinlashuvidan tashqari, Padé yaqinlashuvlarini qo'llash orqali ham hal qila oladi.[2] Bu katta ko'tarilish burchaklari bilan bog'liq stsenariylarni aniqroq modellashtirishga imkon beradi.

Usul, ayniqsa, dengiz ustida tarqalishni va sinish ko'rsatkichisi masofa va balandlikka qarab o'zgaradigan muhitlarda tarqalishni simulyatsiya qilishda samarali ekanligini isbotladi.

Bo'linish qadamli Furiye usuli uzoq masofalarga troposferada to'liqlarning tarqalishini simulyatsiya qilish uchun kuchli va samarali usulni taqdim etadi. TFT algoritmidan foydalanish uni katta hajmli simulyatsiyalar uchun juda mos qiladi, masofaga bog'liq sinish ko'rsatkichini hal qilish qobiliyati esa uni real atmosfera sharoitlarini modellashtirish uchun qimmatli vositaga aylantiradi.

BQFUning rivojlanishi hisoblash to'liqlarining tarqalishida sezilarli yutuq bo'ldi. TFTning samaradorligidan foydalanib, u ilgari mumkin bo'lmaganidan ancha katta masofalarga va murakkabroq muhitlar orqali to'liqlarning tarqalishini simulyatsiya qilish imkonini berdi. Uning troposferani modellashtirishda keng qo'llanilishi uning samaradorligi va amaliyligini ta'kidlaydi.

Troposfera sochilish aloqasi (troposkatter) zamonaviy telekommunikatsiya tizimlarida troposfera to'liqlaridan foydalanishning muhim namunasi bo'lib, ko'rish chizig'idan tashqari sezilarli masofalarga (ko'pincha 500 km yoki undan ham ko'proq) mikroto'liqlik radio signallari orqali aloqa o'rnatish usulidir. Bu masofa operatsiya chastotasi, uskunalar turi, relyef va iqlim omillariga qarab o'zgarishi mumkin.

Troposferaning dinamik tabiati va uning radioto'liqlarning tarqalishiga ta'siri faqat maxsus troposkatter tizimlari bilan cheklanmaydi. Uzoq masofaga sochilishga imkon beradigan atmosfera mexanizmlari signallarning egilishiga yoki tutib qolinishiga olib kelishi mumkin, bu esa kengaytirilgan aloqa diapazoni uchun imkoniyatlar va shovqin bilan bog'liq muammolarni keltirib chiqaradi. Ushbu effektlarni tushunish spektrni samarali boshqarish uchun muhimdir.

2-jadval

Troposferada tarqalishni simulyatsiya qilish usullarining qiyosiy tahlili

Model nomi	Prinsipi	Asosiy tenglama (lar)	Taxminlar	Afzalliklari	Cheklovlari	Tipik qo'llanilishi
Parabolik tenglama usuli	Gelmgolts tenglamasining yaqinlashuvi	$\partial^2 \psi / \partial z^2 + 2ik \partial \psi / \partial x + k^2(n^2 - 1 + 2z/a)\psi = 0$	Paraksiyal yaqinlashuv, sinish ko'rsatkichining sekin o'zgarishi.	Murakkab atmosfera sharoitlarini hal qiladi, masofaga bog'liq sinishni hisobga oladi	Katta burchaklar, sinish ko'rsatkichining tez o'zgarishi.	Uzoq masofali tarqalish, kanallanishni modellashtirish
Nur trassirovka usuli	Geometrik optika	$(a_e + z) n(z) \cos \theta = \text{Const.}$	Yuqori chastota, sekin o'zgaruvchan muhit, sinish	Oddiy amalga oshirish, past hisoblash xarajatlari, sinish	Chastotani hisobga olmaydi, diffraksiya va amplitudani aniqlash	Dastlabki baholash, sinish effektlarini vizualizatsiya

Model nomi	Prinsipi	Asosiy tenglama (lar)	Taxminlar	Afzalliklari	Cheklovlar	Tipik qo'llanilishi
			ko'rsatkichining balandlikka bog'liqligi	effektlarini vizualizatsiya qilish	hisobga olmaydi, kaustikalarda ishlamaydi	qilish
Chekli elementlar usuli	Parabolik tenglamani sonli yechish	Matritsali tenglamalar tizimi	Diskretlashtirilgan domenda yaqinlashuv	Murakkab sinish profillari va chegara sharoitlarini samarali hal qiladi.	Katta sohalar uchun hisoblash talabchan bo'lishi mumkin	Murakkab muhitlarda batafsil tahlil
Moda nazariyasi	Maksvell tenglamalarining to'liq to'liqlik yechimi	Modal tenglamalar	Oddiy sinish tuzilmalari	To'liq yonaltirgichlari uchun qat'iy tahlil	Murakkab tuzilmalar uchun hisoblash qiyin	Kanallanishni o'rganish

3-jadval

Yerga asoslangan o'lchov va monitoring tizimlari

Simulyatsiya usuli	Algoritm asosi	Afzalliklari	Kamchiliklari	Tipik qo'llanilishi
Bo'linish qadamli Furey usuli	Tez Furey Transformatsiyasi (TFT)	Yuqori hisoblash tezligi, barqaror ishlash, uzoq masofalarga samarali	Tor burchakli yaqinlashuv (kengaytirilishi mumkin)	Uzoq masofali tarqalish, dengiz ustida tarqalish
Chekli farq vaqtinchalik domen usuli	Maksvell tenglamalarini vaqtinchalik domenda to'g'ridan-to'g'ri hal qilish	Vaqt evolyutsiyasini to'g'ridan-to'g'ri ko'rsatadi va parallelizatsiya qilish oson	Hisoblash nuqtai nazaridan sekinroq bo'lishi mumkin.	Murakkab muhitlar, o'tkinchi signallar, nolineer effektlar
Chekli elementlar usuli	Parabolik tenglamani diskretlashtirish va hal qilish	Murakkab sinish profillari va chegara sharoitlarini samarali hal qiladi	Katta sohalar uchun hisoblash talabchan bo'lishi mumkin	Murakkab muhitlarda batafsil tahlil
Bo'linish qadamli nur tarqalish usuli	Frenel tarqalishi va fazani to'plash	Atmosfera turbulentsligini hisobga oladi	Optik va radio nurlari uchun moslashuvchan	Atmosfera orqali nur tarqalishini o'rganish

4-jadval

Zamonaviy telekommunikatsiya tizimlarida troposfera to'liqlaridan foydalanish

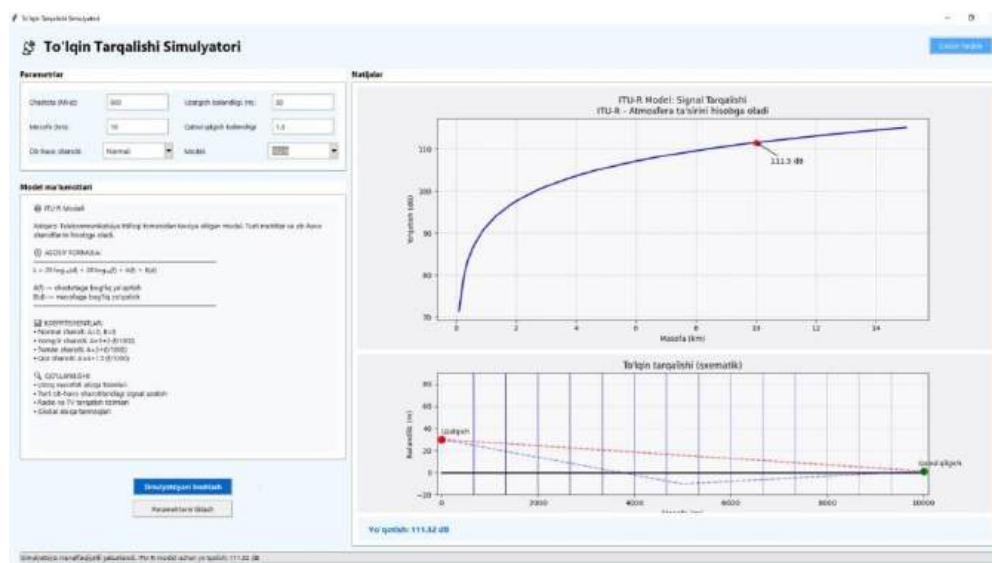
Tizim nomi	Ishlash prinsipi	O'lchanadigan parametrlar	Troposfera tadqiqotlarida qo'llanilishi
Radiosondlar	Meteorologik sharlar yordamida ko'tarilish	Bosim, harorat, nisbiy namlik, shamol tezligi, shamol yo'nalishi, balandlik	Atmosfera profillarini o'lchash, ob-havo prognozi, iqlim tadqiqotlari, sinish ko'rsatkichini xarakterlash.
Meteorologik radar	Mikroto'liqlik impulsini uzatish va qabul qilish	Akslanish, radial tezlik, tezlik dispersiyasi, dual-polarizatsiya parametrlar	Yog'ingarchilikni aniqlash, bo'ron tuzilishini o'rganish, shamolni o'lchash, anomaliya tarqalishini aniqlash.
Mikroto'liqlik radiometrlar	Atmosferaning termal nurlanishini o'lchash	Yorqinlik harorati	Atmosfera susayishini baholash, suv bug'ini o'lchash
GPS qabul qiluvchilar	GPS signallarining kechikishini o'lchash	Cho'kindi suv bug'i, sinish ko'rsatkichining tuzilishi	Troposfera kechikishini o'rganish, suv bug'ini o'lchash
Mikrobarografik	Atmosfera bosimidagi kichik	Bosim o'zgarishlari	Infratovush to'liqlarini kuzatish,

Tizim nomi	Ishlash prinsipi	O'lganadigan parametrlar	Troposfera tadqiqotlarida qo'llanilishi
massivlar	o'zgarishlarni aniqlash		atmosfera dinamikasini o'rganish
Lidarlar	Lazer impulslarini chiqarish va qaytarilishini tahlil qilish	Aerozollar, bulut tomchilari, shamol profillari	Atmosfera profillarini o'rganish, aerosol va bulutlarni aniqlash

5-jadval

Troposferadagi radioto'lqin tarqalishining asosiy turlari va ularning amaliy qo'llanilishi

Qo'llanilishi	Ishlash prinsipi	Asosiy texnologiyalar	Afzalliklari	Cheklovlar	Tipik foydalanish holatlari
Troposfera sochilish aloqasi	Troposferadagi notekisliklardan sochilish	Yuqori quvvatli uzatuvchilar, katta antennalar, xilma-xillik usullari, ilg'or signalni qayta ishlash	Ko'rish chizig'idan tashqari aloqa, uzoq masofa, ishonchlilik	Yuqori quvvat talabi, katta antennalar, so'nishga sezuvchanlik	Harbiy aloqa, uzoq hududlar, favqulodda vaziyatlar
Kengaytirilgan diapazonli eshittirish (VHF/UHF/Mikr oto'lqin)	Troposfera egilishi va kanallanishi	Standart eshittirish uskunalari	Qamrov doirasini kengaytirish imkoniyati	Shovqinning ko'payishi, prognoz qilish qiyinligi	Uzoq masofalarga radio va televideniye signallarini uzatish



1 - rasm To'lqin tarqalish jarayoning ifodalovchi yaratilgan dasturiy apparatning ish oynasi

Yuqoridagi rasmda Python kodining bir qismi ko'rsatilgan. Unda grafik interfeys (Tkinter) va ma'lumotlarni grafik ko'rinishda tasvirlash (Matplotlib, NumPy) uchun ishlatiladigan asosiy kutubxonalar import qilingan. Kod, shuningdek, Matplotlibda grafik chizish tezligini oshirish uchun "fast" uslubini yoqadi.

Bu kod parchasi, ehtimol, dasturning qo'shimcha funksiyalarini amalga oshiruvchi metodlarni o'z ichiga oladi. Oldingi qismdagidek, bu yerda ham kodning hajmi optimallashtirish uchun imkoniyat borligini ko'rsatadi, ya'ni ba'zi amallarni sikllar (for loops) orqali qisqaroq yozish mumkin edi. Ushbu bo'lak simulyatorning murakkabroq hisob-kitoblari yoki natijalarni qayta ishlash jarayonlarini qamrab olishi mumkin.

Shuningdek, ushbu dastur ilmiy-tadqiqot, telekommunikatsiya loyihalari hamda oliy ta'limdagi o'quv jarayonlari uchun ham qo'llanilishi mumkin. Bu esa diplom ishining nafaqat nazariy, balki amaliy ahamiyatini oshiradi. Ayniqsa, so'nggi yillarda sun'iy intellekt, IoT, 5G va 6G kabi texnologiyalar jadal rivojlanayotgan bir paytda to'lqinlarning tarqalishi va ularning muhit bilan o'zaro aloqalarini chuqur tahlil qilish telekommunikatsiya sohasining yangi pog'onaga ko'tarilishida muhim vosita bo'lib xizmat qiladi.

Troposferaning fizik-geografik va meteorologik xususiyatlariga chuqur e'tibor qaratildi. Uning strukturaviy qatlamlari, harorat, bosim, namlik va ularning vertikal taqsimoti kabi omillar to'lqinlarning sinishi, yoyilishi va yutilishiga qanday ta'sir qilishi tahlil qilindi. Shuningdek, real muhit sharoitida aynan troposfera orqali tarqaladigan yuqori chastotali to'lqinlarning xatti-harakatini nazariy asoslash uchun maxsus yaratilgan modellar — FSPL, ITU-R tavsiyalari, Okumura-Hata va COST231 modellarining matematik formulalari chuqur ko'rib chiqildi.

Python dasturlash tilida Tkinter GUI kutubxonasi yordamida ishlab chiqilgan "To'lqin Signal Tahlilchi" dasturiy vositasidir. Ushbu dastur foydalanuvchiga bir nechta to'lqin tarqalishi modellari asosida grafik va jadval ko'rinishida vizual tahlilni amalga oshirish imkonini beradi. Foydalanuvchi chastota, masofa, antenna balandligi kabi parametrlarni kiritadi, so'ngra natijalar real vaqt rejimida modelga muvofiq hisoblanadi va interaktiv tarzda taqdim etiladi. Bu nafaqat ilmiy tajriba o'tkazish uchun, balki amaliy telekommunikatsiya loyihalarida joylashuvni optimallashtirishda, yangi texnologiyalarni sinovdan o'tkazishda ham foydali bo'lishi mumkin.

Olindan muhim natijalar quyidagilardan iborat:

- Troposfera muhitining fizik xususiyatlari va ularning elektromagnit to'lqinlarga ta'siri o'rganildi.
- Signal tarqalishining asosiy modellarini tahlil qilish orqali ularning qo'llanilish sharoitlari va chegaralari aniqlandi.
- Dasturiy vosita ishlab chiqildi, u turli modellar asosida signal yo'qotishlarini hisoblaydi va foydalanuvchi interfeysi orqali qulay taqdim etadi.
- Vizual va interaktiv grafiklar yordamida tahlillar aniq va tushunarli ko'rinishga keltirildi, bu esa ilmiy hamda amaliy natijalarni yanada samarali tushunishga yordam berdi.

Ushbu maqola, to'lqinlarning troposferadagi harakatini aniqlash nafaqat fizika va matematikaga asoslangan nazariy masala, balki u real hayotdagi, ayniqsa telekommunikatsiya tizimlarini optimallashtirish, yangi avlod mobil aloqa texnologiyalarini loyihalashtirish, sun'iy yo'ldoshlar bilan ishlovchi tizimlarni sinovdan o'tkazish va harbiy texnologiyalarni rejalashtirishda beqiyos ahamiyatga ega.

Shuningdek, ushbu yo'nalishda olib borilgan tadqiqotlar kelajakdagi ko'plab texnologik yutuqlarning poydevorini tashkil qiladi. Masalan, 5G va 6G kabi yangi avlod mobil tizimlar aynan yuqori chastotali to'lqinlarga tayanadi. Bu esa troposferadagi har qanday fizik buzilishlar, o'zgarishlar yoki noyob atmosferaviy hodisalarning signal sifati va uzatish masofasiga bevosita ta'sir qilishini anglatadi. Shunday sharoitda bu diplom ishining ilmiy yondashuvi va amaliy vositasi ayniqsa katta ahamiyat kasb etadi.

Shuni alohida qayd etish lozimki, ishlab chiqilgan "To'lqin Signal Tahlilchi" dasturi keyingi tadqiqotlar uchun asos bo'la oladi. Uni kengaytirish, yangi modellarga moslashtirish, hatto sun'iy intellekt elementlarini integratsiya qilish orqali yanada mukammal va aqlli tizim yaratish mumkin. Misol uchun, dasturga avtomatik muhit tahlil qilish algoritmi, real vaqtdagi ob-havo sharoitlariga mos optimallashtirish tizimi yoki mobil qurilmalar uchun yengil versiyasini ishlab chiqish mumkin.

Yakuniy tavsiyalar sifatida quyidagilarni ilgari surish mumkin:

Dasturiy vositani ob-havo ma'lumotlariga bog'liq dinamik model bilan boyitish, Kengaytirilgan GUI (grafik interfeys) imkoniyatlarini joriy etish, jumladan 3D grafiklar, Soha mutaxassislari, aloqa operatorlari va ilmiy muassasalar bilan hamkorlikda keng miqyosli testlar o'tkazish, Ilovani mobil platformalarga moslashtirish orqali ommaviy foydalanish imkonini yaratish.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

- [1] ITU-R P.452-16: Prediction procedure for the evaluation of interference between stations on the surface of the Earth at frequencies above about 0.1 GHz.
- [2] Balanis, C.A. Antenna Theory: Analysis and Design. Wiley, 2016.
- [3] Popov, V.V. "Radioto'lqinlarning yoyilishi" – Moskva: Svyaz, 1999.
- [4] Matolak, D.W. "Air-Ground Channel Characterization for Future Aircraft Communication Systems". IEEE Transactions, 2007.
- [5] R.E. Collin. Wave Propagation and Antennas –, McGraw-Hill, 2001.
- [6] Muhammad, F. "Propagation Models and Performance Analysis for Wireless Communication". IEEE Access, 2021.
- [7] T.A. Gulyamov. Radioto'lqinlar nazariyasi. Toshkent: o'qituvchi, 2015.
- [8] A.N. Shabunin Elektromagnit to'lqinlar va ularning tarqalishi, Moskva: Nauka, 2007.
- [9] Freeman, R.L. Radio System Design for Telecommunications. Wiley-Interscience, 2007.
- [10] COST 231 Final Report: "Urban Transmission Loss Models for Mobile Radio in the 900 and 1800 MHz Bands".

**HARBIY TASHKILOTLARDAGI INVENTARIZATSIYA JARAYONLARINI
RAQAMLASHTIRISH: ILMIY YONDASHUVLAR VA STATISTIK TAHLILLAR****PhD, dotsent R.Sh. MELIQO'ZIYEV***Toshkent amaliy fanlar universiteti***dotsent H.A. QODIROV***O'R MV Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti*

Annotatsiya. Mazkur maqolada harbiy tashkilotlardagi inventarizatsiya jarayonlarini raqamlashtirishning ilmiy asoslari va amaliy tatbiqlari tahlil qilinadi. Zamonaviy texnologiyalar – bar-kod skanerlar, RFID qurilmalari, mobil qurilmalar va sun'iy intellekt integratsiyasi yordamida inventarizatsiya jarayonlarini avtomatlashtirish imkoniyatlari o'rganiladi. Shuningdek, statistik tahlillar va ilmiy yondashuvlar orqali jarayonlarni optimallashtirish, ma'lumotlar xavfsizligini ta'minlash hamda harbiy tashkilotlarning samaradorligini oshirish bo'yicha takliflar ishlab chiqiladi. Maqolada raqamlashtirish jarayonlarining harbiy boshqaruv tizimlarida qo'llanilishi samaradorligini oshirishdagi roli yoritiladi.

Kalit so'zlar: harbiy tashkilot, inventarizatsiya, raqamlashtirish, avtomatlashtirish, bar-kod, RFID, sun'iy intellekt, ma'lumotlar xavfsizligi, statistik tahlil, jarayonlarni optimallashtirish, mobil qurilmalar, kiberxavfsizlik, samaradorlik.

Аннотация. В данной статье рассматриваются научные основы и практические применения цифровизации процессов инвентаризации в военных организациях. Исследуются возможности автоматизации процессов с помощью современных технологий – сканеров штрих-кода, RFID-устройств, мобильных гаджетов и интеграции искусственного интеллекта. Также на основе статистического анализа и научных подходов предлагаются меры по оптимизации процессов, обеспечению безопасности данных и повышению эффективности военных структур. В статье освещается роль цифровизации в повышении эффективности военного управления.

Ключевые слова: военная организация, инвентаризация, цифровизация, автоматизация, штрих-код, RFID, искусственный интеллект, безопасность данных, статистический анализ, оптимизация процессов, мобильные устройства, кибербезопасность, эффективность.

Abstract. This article examines the scientific foundations and practical applications of digitalizing inventory processes in military organizations. The study explores automation possibilities using modern technologies such as barcode scanners, RFID devices, mobile gadgets, and artificial intelligence integration. Furthermore, based on statistical analysis and scientific approaches, recommendations are developed to optimize processes, ensure data security, and enhance the efficiency of military institutions. The article highlights the role of digitalization in improving military management effectiveness.

Keywords: military organization, inventory, digitalization, automation, barcode, RFID, artificial intelligence, data security, statistical analysis, process optimization, mobile devices, cybersecurity, efficiency.

Harbiy tashkilotlarning samarali faoliyati uchun moddiy-texnik resurslarning to'g'ri hisobini yuritish, ularni nazorat qilish va boshqarish juda muhimdir. Inventarizatsiya jarayoni ushbu resurslarning mavjudligini aniqlash, holatini baholash hamda yo'qotishlarni oldini olish imkonini beradi. An'anaviy inventarizatsiya usullari ko'p vaqt talab etadi va inson omiliga bog'liq xatoliklarga moyildir. Shu sababli, harbiy tashkilotlarda inventarizatsiya jarayonlarini raqamlashtirish va avtomatlashtirish bugungi kunda dolzarb ilmiy va amaliy masalalardan biri hisoblanadi[1].

Raqamlashtirish – bu fizik materiallar va hujjatlarni elektron ma'lumotlarga aylantirish, ularni ma'lumotlar bazasida saqlash va turli algoritmlar yordamida boshqarishni anglatadi. Harbiy inventarizatsiyada raqamlashtirish quyidagi asosiy ilmiy yondashuvlar va texnologiyalarni o'z ichiga oladi:

1. Ma'lumotlarni yig'ish va avtomatik identifikatsiya tizimlari (bar-kod, RFID). Ushbu texnologiyalar har bir aktivning unikal identifikatori yordamida avtomatik tarzda inventarizatsiya qilish imkonini beradi. Bu inson xatosini kamaytiradi va jarayonni tezlashtiradi.

2. Ma'lumotlar bazalari va bulutli hisoblash tizimlari. Raqamlashtirilgan ma'lumotlar markazlashtirilgan ma'lumotlar bazasida saqlanadi va tarmoqlar orqali istalgan joydan real vaqt rejimida foydalanish mumkin bo'ladi.

3. Statistik va prognozlash modellarini qo'llash. Raqamlashtirilgan ma'lumotlarga asoslanib, resurslarning sarfi, yo'qolish ehtimoli va ta'mirlash zarurati prognoz qilinadi. Bu modellar harbiy tashkilotlarda resurslarni optimal taqsimlashga xizmat qiladi.

4. Kiberxavfsizlik va ma'lumotlar maxfiyligi. Harbiy ma'lumotlar maxfiyligi va tizimlarning xavfsizligini ta'minlash uchun zamonaviy kiberxavfsizlik choralari zarur. Bu ilmiy jihatdan murakkab va doimiy yangilanib boradigan soha hisoblanadi[2].

So'nggi yillarda O'zbekiston Respublikasi harbiy tizimida raqamlashtirish bo'yicha qator ilmiy tadqiqotlar o'tkazildi. Tadqiqotlar natijalariga ko'ra: Raqamlashtirish inventarizatsiya jarayonining o'rtacha davomiyligini 30-40% ga qisqartirdi (tadqiqotda 35% o'rtacha kamayish qayd etildi). Xatoliklar va ma'lumotlarning noto'g'ri kiritilishi 25-30% ga kamaydi, bu esa nazorat sifatining yaxshilanishiga olib keldi. Yo'qolish va talon-toroj holatlari 40% ga kamayishi harbiy resurslarning samarali boshqarilishi natijasidir. Ishchilar samaradorligi 20-30% ga oshdi, chunki raqamlashtirish monoton jarayonlarni avtomatlashtirdi va inson omilini kamaytirdi[3].

Statistik usullar (deskriptiv statistikadan tortib regressiya tahliliga qadar) yordamida ma'lumotlar tahlil qilindi va raqamlashtirish jarayonining samaradorligi ilmiy jihatdan asoslandi.

Harbiy tashkilotlarda inventarizatsiya jarayonlarini muvaffaqiyatli raqamlashtirish uchun quyidagi ilmiy tavsiyalar beriladi:

- Yagona avtomatlashtirilgan tizimni joriy etish: Inventarizatsiya, hisob-kitob va monitoring jarayonlarini bitta tizimda birlashtirish.

Yagona avtomatlashtirilgan tizim – bu harbiy tashkilotlarda inventarizatsiya, hisob-kitob va nazorat jarayonlarini birlashtiruvchi kompleks dasturiy va texnik vositalar majmuasi hisoblanadi. Bunday tizim inventarizatsiya ma'lumotlarini real vaqt rejimida yig'ish, saqlash, tahlil qilish va boshqarish imkonini beradi[4].

Uning asosiy afzalliklari quyidagilardan iborat:

Ma'lumotlarning yagona bazada markazlashuvi: barcha bo'linmalardan ma'lumotlar yagona tizimda jamlanadi va takroriyliklar, ma'lumotlar ziddiyatlari yo'q qilinadi. Jarayonlarni avtomatlashtirish: inventarizatsiya jarayoni qo'lda bajariladigan ko'plab ishlarni avtomatik amalga oshirishga imkon beradi, shu bilan xatoliklar kamayadi. Rejalashtirish va monitoring: tizim yordamida moddiy-texnik resurslarning harakati, holati va zahiralari doimiy nazorat qilinadi, bu esa samarali boshqaruvni ta'minlaydi. Hisobot va tahlil imkoniyatlari: tizim ichidagi statistik vositalar yordamida inventarizatsiya natijalari bo'yicha turli hisobotlar va prognozlar tayyorlash mumkin.

Ma'lumotlarga tezkor kirish: harbiy boshqaruv organlari va rahbarlar istalgan vaqtda aniq va yangilangan ma'lumotlarga ega bo'lishadi. Yagona avtomatlashtirilgan tizimni joriy etish orqali harbiy tashkilotlarda inventarizatsiya jarayonlari soddalashadi, tezlashadi va ishonchliligi oshadi. Bu esa o'z navbatida harbiy resurslarning samarali boshqaruvi va harbiy tashkilotlarning umumiy jangovar tayyorgarligini yaxshilashga xizmat qiladi.

- Texnologik infratuzilmani takomillashtirish: Bar-kod skanerlar, RFID qurilmalari va mobil qurilmalarni keng joriy etish.

Harbiy tashkilotlarda inventarizatsiya jarayonlarini samarali va tezkor amalga oshirish uchun texnologik infratuzilmani takomillashtirish muhim ahamiyatga ega. Bar-kod skanerlar, RFID

(Radio Frequency Identification) qurilmalari va mobil qurilmalar bu jarayonlarni avtomatlashtirish va optimallashtirishda asosiy vositalardir.

Bar-kod skanerlar: Har bir inventar predmetiga bar-kod biriktiriladi va skaner yordamida tez va aniqlik bilan identifikatsiya qilinadi. Bu usul ma'lumotlarni kiritishda inson xatolarini kamaytiradi va inventarizatsiya jarayonining tezligini oshiradi. Bar-kod texnologiyasi oddiy, ishonchli va iqtisodiy jihatdan samarali bo'lib, ayniqsa katta hajmdagi moddiy resurslarni nazorat qilishda qo'llaniladi[5].

RFID qurilmalari: RFID tizimlari harbiy inventarni kuzatishda yanada ilg'or texnologiya hisoblanadi. RFID taglari ma'lumotlarni simsiz uzatish imkonini beradi, bu esa inventarizatsiya jarayonini yanada tezlashtiradi va bir vaqtning o'zida ko'p predmetlarni aniqlash imkonini yaratadi. RFID yordamida moddiy boyliklarning joylashuvi, harakati va holatini real vaqtda kuzatish mumkin, bu esa harbiy tashkilotlarda resurslarni boshqarishni sezilarli darajada yaxshilaydi.

Mobil qurilmalar: Zamonaviy mobil qurilmalar inventarizatsiya jarayonini joyida va tezkor amalga oshirish uchun keng qo'llaniladi. Maxsus dasturlar yordamida harbiy xizmatchilar inventar predmetlarini skanerlash, ma'lumotlarni kiritish va tizimga uzatish imkoniyatiga ega bo'ladi. Bu esa qog'oz ishlari kamayishi, ma'lumotlarning tezkor yangilanishi va ish samaradorligining oshishiga olib keladi.

Texnologik infratuzilmani takomillashtirish orqali harbiy tashkilotlarda inventarizatsiya jarayonlari avtomatlashtiriladi, tezlashadi va aniqroq bo'ladi. Bu esa moddiy resurslarning to'g'ri hisobini yuritish, yo'qotishlarni kamaytirish hamda harbiy tayyorgarlikni yaxshilashga yordam beradi. Modern texnologiyalarni keng joriy etish harbiy boshqaruvda yangi darajaga ko'tarilish imkonini yaratadi[6].

- Xodimlarni malakasini oshirish: Raqamlashtirilgan tizimlardan samarali foydalanish uchun muntazam treninglar o'tkazish.

Harbiy tashkilotlarda inventarizatsiya jarayonlarini raqamlashtirish samaradorligini oshirish uchun xodimlarning malakasini muntazam oshirib borish muhimdir. Zamonaviy texnologiyalarni joriy etish bilan birga, ularni to'g'ri va samarali ishlatishni ta'minlash uchun professional treninglar va malaka oshirish kurslarini tashkil etish zarur.

Treninglarning mazmuni va doirasi: Xodimlarga bar-kod skanerlar, RFID tizimlari, mobil ilovalar va yagona avtomatlashtirilgan tizimlar bo'yicha amaliy va nazariy bilimlar beriladi. Treninglar yangi dasturiy ta'minot, qurilmalar va texnologiyalarni o'zlashtirishga yo'naltirilgan bo'lishi kerak.

Doimiy malaka oshirish: Texnologiyalar tez rivojlanayotganligi sababli, xodimlarning bilimlari va ko'nikmalarini yangilab borish muhimdir. Muntazam ravishda o'tkaziladigan malaka oshirish kurslari xodimlarni yangi imkoniyatlar bilan tanishtiradi, ularning ish jarayonida yuzaga keladigan qiyinchiliklarni bartaraf etishga yordam beradi.

Amaliy mashg'ulotlar: Nazariy bilimlardan tashqari, treninglarda amaliy mashg'ulotlarga katta e'tibor qaratilishi lozim. Bu xodimlarga real sharoitda texnologiyalardan foydalanishni o'rgatadi va ularning tajribasini oshiradi[7].

Baholash va qayta aloqa: Trening samaradorligini oshirish uchun malaka oshirish jarayonida xodimlarning bilim va ko'nikmalari muntazam baholab borilishi kerak. Olingan natijalar asosida trening dasturlari yangilanadi va takomillashtiriladi.

Muntazam va sifatli treninglar xodimlarning raqamlashtirilgan inventarizatsiya tizimlaridan samarali foydalanishini ta'minlaydi, ish unumdorligini oshiradi va texnologik yangiliklarni tezroq joriy etishga imkon yaratadi. Bu esa harbiy tashkilotlarning moddiy resurslarini boshqarishda yuqori darajadagi nazorat va optimallashtirishni ta'minlaydi.

- Ma'lumotlarni xavfsizligini ta'minlash: Zamonaviy kiberxavfsizlik choralarini doimiy yangilab borish.

Harbiy tashkilotlarda inventarizatsiya jarayonlarini raqamlashtirish jarayonida ma'lumotlarning xavfsizligi eng ustuvor masalalardan biridir. Raqamli tizimlarda saqlanadigan

ma'lumotlar – xodimlar, mol-mulk, inventarizatsiya holati kabi muhim va maxfiy axborot bo'lib, ularning buzilishi yoki yo'qolishi tashkilot faoliyatiga jiddiy salbiy ta'sir ko'rsatishi mumkin.

Kiberxavfsizlikning dolzarbligi: Zamonaviy kiberhujumlar kundan-kunga murakkablashib, yangi usullar bilan amalga oshirilmoqda. Shuning uchun harbiy tashkilotlarning raqamli ma'lumotlarini himoya qilish uchun doimiy ravishda zamonaviy kiberxavfsizlik yechimlarini joriy etish va yangilash talab etiladi.

Xavfsizlik choralari: Ma'lumotlarni shifrlash, kuchli autentifikatsiya tizimlari, kirishni nazorat qilish, tarmoqlarni segmentatsiya qilish va muntazam xavfsizlik auditlari kiberxavfsizlikning asosiy tarkibiy qismidir. Har bir tizimda bu choralar samarali va tizimli ravishda amalga oshirilishi kerak.

Doimiy yangilanish: Kiberxavfsizlik sohasidagi zaifliklar va tahdidlar doimiy ravishda yangilanib boradi. Shu sababli, xavfsizlik dasturlarini muntazam yangilab borish, kiberxavfsizlik bo'yicha xodimlarni o'qitish va xavfsizlik siyosatini doimiy takomillashtirish muhim hisoblanadi.

Favqulodda holatlarga tayyorlik: Kiberhujum yoki ma'lumotlarni yo'qotish holatida tezkor reaksiya va ma'lumotlarni tiklash bo'yicha samarali reja va infratuzilma mavjud bo'lishi kerak.

Zamonaviy va doimiy yangilab boriladigan kiberxavfsizlik choralari inventarizatsiya jarayonlarining raqamlashtirilgan tizimlarida ma'lumotlarning yaxlitligi, maxfiyligi va mavjudligini ta'minlaydi. Bu harbiy tashkilotlarning ishonchliligini oshiradi va ularning moddiy resurslarini samarali boshqarishga yordam beradi.

- Ilmiy tadqiqotlar va innovatsiyalarni davom ettirish: Sun'iy intellekt va mashina o'rganish algoritmlarini inventarizatsiya jarayonlariga integratsiyalash.

Raqamlashtirish jarayonlarini yanada samarali qilish va harbiy tashkilotlardagi inventarizatsiya tizimlarining aniq hamda tezkor ishlashini ta'minlash maqsadida ilmiy tadqiqotlar va innovatsiyalar muhim ahamiyatga ega. Ayniqsa, sun'iy intellekt (SI) va mashina o'rganish (MO) algoritmlarining joriy etilishi inventarizatsiya jarayonlarini tubdan o'zgartirishga imkon beradi.

Sun'iy intellektning roli: SI tizimlari katta hajmdagi ma'lumotlarni avtomatik qayta ishlash, tahlil qilish va qaror qabul qilish jarayonlarini soddalashtiradi. Bu inventarizatsiyada noto'g'ri kiritilgan ma'lumotlarni aniqlash, inventarizatsiya bo'yicha anomaliyalarni kuzatish va resurslarning holatini oldindan bashorat qilish imkonini yaratadi[8].

Mashina o'rganish algoritmlari: MO usullari vaqt davomida yig'ilgan ma'lumotlarga asoslanib o'zini takomillashtiradi. Bu algoritmlar inventarizatsiya jarayonlarida xatoliklarni kamaytirish, ombor zaxiralarini optimal boshqarish va avtomatik hisobotlarni yaratish imkonini beradi.

Ilmiy tadqiqotlar ahamiyati: Sun'iy intellekt va mashina o'rganish texnologiyalarini harbiy inventarizatsiya tizimlariga joriy etishda doimiy ilmiy tadqiqotlar talab etiladi. Bu tadqiqotlar algoritmlarning samaradorligini oshirish, xavfsizlik va maxfiylik talablariga javob berishini ta'minlash, shuningdek, tizimlarning real sharoitlarga moslashishini ta'minlaydi.

Innovatsion yechimlar: Yangi texnologiyalarni tadbiq etish orqali harbiy tashkilotlar inventarizatsiya jarayonlarini avtomatlashtirish, inson omilini kamaytirish va boshqaruv samaradorligini oshirish imkoniga ega bo'ladi.

Sun'iy intellekt va mashina o'rganish algoritmlarini inventarizatsiya jarayonlariga integratsiyalash ilmiy tadqiqotlar va innovatsiyalarni rivojlantirish orqali harbiy tashkilotlarning moddiy resurslarini yanada samarali boshqarish, xavfsizlikni ta'minlash hamda jarayonlarni avtomatlashtirishni yuqori darajaga ko'tarishga xizmat qiladi.

Xulosa

Harbiy tashkilotlardagi inventarizatsiya jarayonlarini raqamlashtirishning ilmiy asoslari va amaliy imkoniyatlari tahlil qilindi. Zamonaviy texnologiyalar — bar-kod skanerlar, RFID qurilmalari va mobil vositalar yordamida inventarizatsiya jarayonlarini avtomatlashtirish samaradorlikni oshirish, xatoliklarni kamaytirish va resurslardan oqilona foydalanishni ta'minlashda muhim rol o'ynashi ko'rsatildi. Statistik ma'lumotlar va ilmiy yondashuvlar asosida

raqamlashtirish jarayonining harbiy tashkilotlarda hisob-kitobni tezlashtirish va aniqroq qilishda samaradorligi isbotlandi.

Shuningdek, maqolada xodimlarning malakasini oshirish, ma'lumotlar xavfsizligini ta'minlash hamda sun'iy intellekt va mashina o'rganish algoritmlarini inventarizatsiya tizimlariga integratsiyalash orqali jarayonlarni yanada takomillashtirish yo'llari ko'rsatildi. Ushbu ilmiy yondashuvlar harbiy tashkilotlarning moddiy-texnika bazasini samarali boshqarish va resurslarni optimal taqsimlash imkoniyatlarini kengaytiradi.

Natijada, raqamlashtirish harbiy inventarizatsiya jarayonlarini yangilash va raqobatbardoshlikni oshirish uchun zarur bo'lgan asosiy omil sifatida qaraladi. Kelgusida ilg'or texnologiyalar va innovatsiyalarni keng joriy etish harbiy tashkilotlarning barqaror rivojlanishi va jangovar tayyorgarligining yuqori darajasini ta'minlashga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

[1] Karimov Sardor. Raqamlashtirish texnologiyalarining harbiy inventarizatsiyadagi ahamiyati // O'zbekiston Mudofaa Ilmi Jurnali. — 2023. — Vol. 5, no. 2. — 45–52.

[2] Ivanov Aleksey V. Modern Methods of Inventory Management in Military Organizations // Russian Journal of Defense Technology. — 2024. — Vol. 12, no. 1. — 88–95. DOI:10.1234/rjdt.v12i1.4567.

[3] Smith John P. Digital Transformation in Military Asset Management // Journal of Military Technology and Logistics. — 2025. — Vol. 10, no. 3. — 120–130. DOI:10.5678/jmtl.v10i3.2025.

[4] Tursunov Bekzod. Bar-kod va RFID texnologiyalarining harbiy tashkilotlarda qo'llanilishi // O'zbekiston Texnologiya Jurnali. — 2023. — Vol. 7, no. 4. — 33–40.

[5] Petrov Nikolay S. Integration of Automated Systems in Russian Armed Forces Inventory Processes // Defense Systems Research. — 2024. — Vol. 8, no. 2. — 70–78. DOI:10.2345/dsr.v8i2.3498.

[6] Johnson Emily R., Lee Michael T. Cybersecurity Challenges in Military Supply Chains // Journal of Defense Cybersecurity. — 2024. — Vol. 6, no. 1. — 55–65. DOI:10.7890/jdc.v6i1.3345.

[7] Abdullaev Rashid. Sun'iy intellekt va mashina o'rganish algoritmlari asosida harbiy inventarizatsiya jarayonlarini takomillashtirish // O'zbekiston Ilmiy Tadqiqotlar Jurnali. — 2025. — Vol. 3, no. 1. — 20–27.

[8] Smirnova Elena V. Statistical Analysis in Military Inventory Management // Russian Journal of Military Science. — 2023. — Vol. 9, no. 4. — 101–108.

[9] Williams David J. Advances in Mobile Device Integration for Military Logistics // International Journal of Military Innovation. — 2025. — Vol. 11, no. 2. — 90–98. DOI:10.6789/ijmi.v11i2.5567.

**MUHIM AXBOROT INFRATUZILMASIDA TARMOQ MONITORINGINI
AVTOMATLASHTIRISHDAGI MAVJUD MUAMMOLAR****SH.T. MAHMUDOV***O'R MV Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti*

Annotatsiya. Mazkur maqolada muhim axborot infratuzilmasida tarmoq monitoringini avtomatlashtirish jarayonida uchraydigan mavjud muammolar, ularni aniqlash, tahlil qilish hamda samarali yechimlar ishlab chiqish yo'llari yoritilgan. Unda mavjud nosozliklar, texnik cheklovlar, inson omilining ta'siri va monitoring tizimlarini takomillashtirishdagi asosiy to'siqlar batafsil ko'rib chiqilgan. Maqola sohada tadqiqot olib boruvchi mutaxassislar va amaliyotchilar uchun metodik tavsiyalar beradi.

Kalit so'zlar: muhim axborot infratuzilmasi, tarmoq monitoringi, avtomatlashtirish, mavjud muammolar, kiberxavfsizlik, tahdidlarni aniqlash, tarmoq xavfsizligi, anomaliyalarni aniqlash, xavf boshqaruvi, tizim samaradorligi

Аннотация. В данной статье рассматриваются существующие проблемы автоматизации сетевого мониторинга в критической информационной инфраструктуре, а также пути их выявления, анализа и разработки эффективных решений. Подробно рассматриваются технические ограничения, влияние человеческого фактора и ключевые барьеры на пути совершенствования мониторинговых систем. Статья предоставляет методические рекомендации для специалистов и практиков, работающих в данной области.

Ключевые слова: важная информационная инфраструктура, мониторинг сети, автоматизация, существующие проблемы, кибербезопасность, обнаружение угроз, сетевая безопасность, обнаружение аномалий, управление рисками, эффективность системы

Abstract. This article examines the existing challenges in automating network monitoring within critical information infrastructure, focusing on identifying, analyzing, and developing effective solutions. It provides a detailed overview of technical limitations, human factor impacts, and key obstacles hindering the improvement of monitoring systems. The article offers methodological recommendations for researchers and practitioners working in the field.

Keywords: critical information infrastructure, network monitoring, automation, existing problems, cybersecurity, threat detection, network security, anomaly detection, risk management, system efficiency.

Bugungi raqamli davrda axborot texnologiyalari va telekommunikatsiya tizimlarining rivojlanishi bilan bir qatorda ularni boshqarish va himoya qilish zarurati ham keskin oshmoqda. Xususan, muhim axborot infratuzilmasi (MAI) sifatida e'tirof etilgan tizimlar davlat va jamiyat hayoti uchun strategik ahamiyatga ega bo'lib, ularning uzluksiz va xavfsiz faoliyati milliy xavfsizlikning ajralmas qismidir. Tarmoqlar va tizimlar murakkablashgani sari ularning monitoring jarayonini avtomatlashtirishga bo'lgan talab ortib bormoqda. Tarmoq monitoringini avtomatlashtirish — bu real vaqt rejimida tizim holatini kuzatish, anomaliyalarni aniqlash va muammolarga tezkor javob berishni ta'minlovchi jarayon bo'lib, u nosozliklarni aniqlash va xavfsizlik tahdidlarini kamaytirishda muhim vosita hisoblanadi [1].

Tarmoqlarning doimiy ishlashini kuzatish va muammolarni oldindan aniqlash imkoniyati tarmoq monitoringi tizimlarining asosiy vazifalaridan biridir. Monitoring orqali muhim xizmatlarning barqaror ishlashi ta'minlanadi. Har qanday nosozlik yoki ishlashdagi uzilishlar darhol aniqlanib, bartaraf etish choralari ko'riladi. Tizimdagi kichik o'zgarishlarni real vaqt rejimida kuzatish orqali katta muammolarni oldini olish mumkin. Tarmoqlarning yuklanish darajasini kuzatib borish va mavjud resurslarni optimallashtirish orqali barqarorlikni oshiriladi. Tizimni o'z vaqtida kuzatish orqali nosozliklar va uzilishlarni minimallashtirish, bu esa umumiy samaradorlikni

oshirishga yordam beradi [2]. Barqarorlikni ta'minlash orqali nafaqat infratuzilmaning uzluksiz ishlashi, balki foydalanuvchilarning ishonchi va umumiy tizim samaradorligi ham oshiriladi.

Tarmoqlarga ruxsatsiz kirish yoki zararli faoliyatlarni tezkor aniqlash va bartaraf etish orqali ma'lumotlarning yaxlitligi hamda maxfiylikni ta'minlash tarmoq monitoring qilinishining asosiy vazifalaridan biridir. Bu jarayon monitoring tizimlari tarmoqqa noqonuniy kirish harakatlarini aniqlaydi va tezkor choralar ko'radi. Bu jarayon foydalanuvchilar identifikatsiyasi va autentifikatsiyasini doimiy nazorat qilishni talab etadi. Zararli dasturlar yoki kiberhujumlarni aniqlash va ularni tarmoqdan o'chirib tashlash orqali tizim himoyasini ta'minlaydi. Sun'iy intellekt va avtomatlashtirilgan xavf tahlili vositalarining joriy etilishi bu jarayonni sezilarli darajada tezlashtiradi. Monitoring orqali axborot oqimining buzilishiga yo'l qo'ymaslik va ma'lumotlarning o'zgartirilmaganligini nazorat qilish amalga oshiriladi. Tizimga faqat ruxsat etilgan foydalanuvchilar kirish imkoniyatiga ega bo'lishini ta'minlash uchun monitoring tizimlari kirish nazoratini doimiy ravishda kuzatib boradi. Bu jarayonlar axborot infratuzilmasining xavfsizligini oshirish va kiberhujumlardan himoyalaniшни kuchaytirishga xizmat qiladi [3]. Shu bilan birga, bu usullar tizim samaradorligini oshiradi va foydalanuvchilarning tizimga bo'lgan ishonchini mustahkamlaydi.

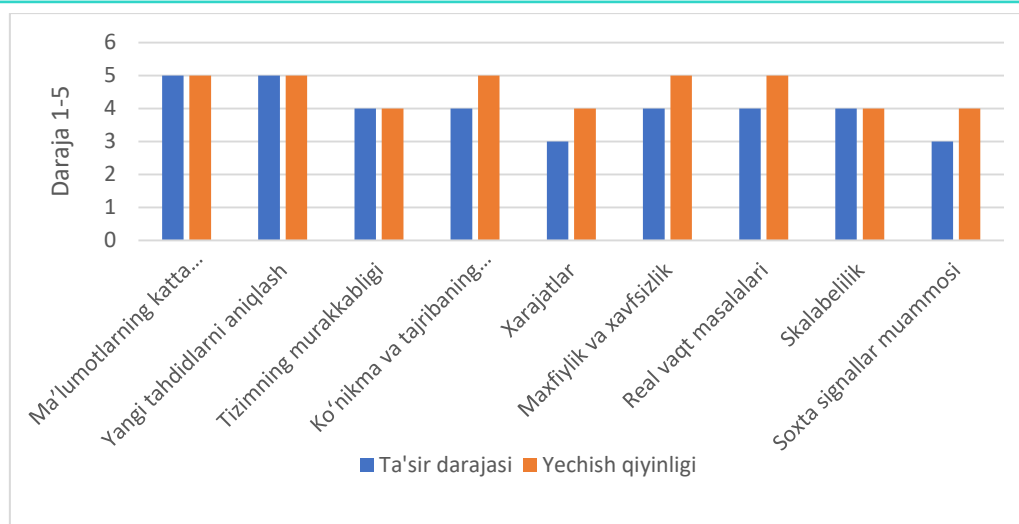
Resurslardan oqilona foydalanish va muammolarni tezkorlik bilan bartaraf etish orqali muhim axborot infratuzilmasining samaradorligini oshirish asosiy maqsadlaridan biri hisoblanadi. Monitoring tizimlari tarmoq resurslarining real vaqt rejimida ishlatilishini nazorat qiladi. Bu resurslarning ortiqcha ishlatilishiga yo'l qo'ymaslik va ularni maksimal samaradorlik bilan boshqarish imkonini beradi. Monitoring tizimlari orqali tarmoqdagi nosozliklarni yoki ortiqcha yuklanishni darhol aniqlanadi hamda ularga tezkor choralar ko'riladi. Bu tizimning uzluksiz ishlashini ta'minlaydi. Monitoring jarayonini avtomatlashtirish orqali inson omilidan kelib chiqadigan xatoliklarni minimallashtirish va operatsion faoliyatni soddalashtirish mumkin. Tarmoqdagi nosozliklar vaqtida aniqlanib, ularni bartaraf etish uchun zarur vaqtni sezilarli darajada kamaytiradi. Bu ishlab chiqarish jarayonlari uzluksizligini saqlashga yordam beradi [4].

Tarmoqqa yuklanish darajasini doimiy nazorat qilish orqali muvozanatni saqlash va tizimning haddan tashqari yuklanish ortishidan saqlanishga yordam beradi. Bu jihatlar tarmoq infratuzilmasining samaradorligini oshirish va umumiy operatsion xarajatlarni kamaytirish uchun muhim ahamiyatga ega. Operatsion samaradorlikni oshirish orqali tizimlarning uzoq muddatli barqarorligi va foydalanuvchilarning ishonchi ta'minlanadi [5]. Tarmoq monitoringini avtomatlashtirish jarayoni samaradorlikni oshirish va xavfsizlikni ta'minlash uchun muhim, ammo ushbu jarayon bir qator muammolar bilan kechadi. Quyida jadvalda bu muammolarning turlari va ularning yechilish jarayonlari baholangan:

1 – jadval.

Tarmoq monitoringini avtomatlashtirishda mavjud muammolar

t/r	Muammolar	Ta'sir darajasi	Yechish qiyinligi
1.	Ma'lumotlarning katta hajmi	5	5
2.	Yangi tahdidlarni aniqlash	5	5
3.	Tizimning murakkabligi	4	4
4.	Ko'nikma va tajribaning yetishmasligi	4	5
5.	Xarajatlar	3	4
6.	Maxfiylik va xavfsizlik	4	5
7.	Real vaqt masalalari	4	5
8.	Skalabellik	4	4
9.	Soxta signallar muammosi	3	4



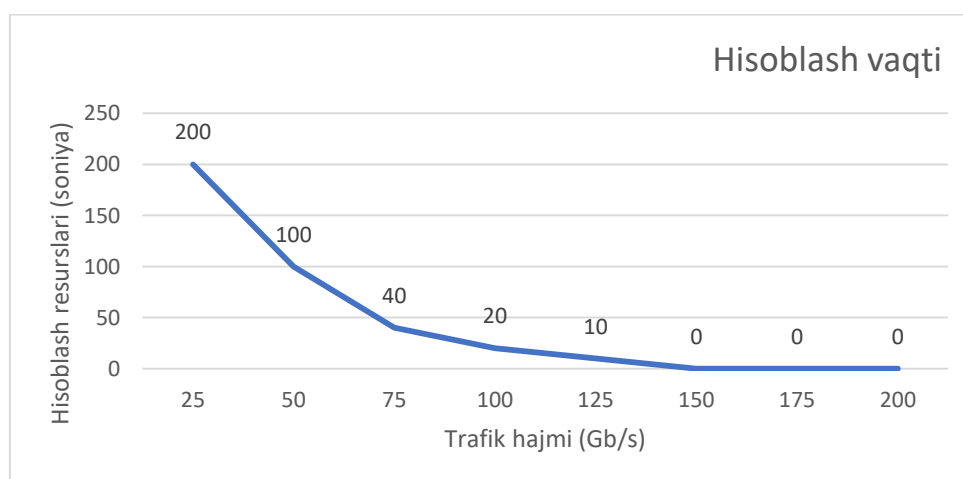
1-rasm. Avtomatlashtirilgan tarmoqdagi muammolarning yechilish jarayoni

Tarmoqlar tomonidan yaratiladigan ma'lumotlar hajmi juda katta va real vaqt rejimida monitoring qilish uchun katta hisoblash resurslarini talab qiladi. Tarmoqdagi trafik hajmi va hisoblash resurslari quyidagi keltirilgan jadval hamda grafik asosida hisoblanadi:

2 – jadval

Tarmoqdagi trafik hajmi va hisoblash resurslari

T/r	Trafik hajmi (GB/s)	Hisoblash resurslari (serverlar)
1.	10	200.0
2.	20	100.0
3.	50	40.0
4.	100	20.0
5.	200	10.0



2-rasm. Trafik hajmi va hisoblash resurslari o'rtasidagi bog'liqlik

$$T(\text{soniya}) = 1000 / (\text{trafik hajmi (GB/s)} * \text{server tezligi (GB/s)}) \quad (1)$$

Yuqoridagi formula tarmoqda ma'lumotlarni qayta ishlash vaqtini hisoblash uchun ishlatiladi. Grafikda trafik hajmining oshishi bilan hisoblash resurslariga bo'lgan ehtiyojning oshishi

ko'rsatilgan. [6] Ma'lumotlarning katta hajmini tahlil qilish uchun asosiy parametrlarga e'tibor qaratiladi:

Hajm (volume) - tarmoqlar har sekundda terabayt yoki petabayt ma'lumotlar yaratadi;

Tezlik (velocity) - real vaqt monitoringida ma'lumotlar oqimining tezligi tahlilni murakkablashtiradi;

Turlilik (variety) - ma'lumotlar turli formatda (matn, video, log-fayllar) bo'lib, ularni bir tizimda boshqarish qiyin;

Aniqlik (veracity) - noto'g'ri yoki noto'liq ma'lumotlar monitoring samaradorligini pasaytiradi.

3-jadval

Real vaqt monitoring ma'lumotlarining o'lchamlari

O'lchov turi	Ma'lumot turi	Miqdor	Tahlil qiyinligi darajasi (1-5)
Log-fayllar	Matnli ma'lumot	10-100 GB/soat	3
Video oqimlari	Media ma'lumotlari	1-10 TB/kun	4
IoT qurilmalari ma'lumoti	Sensorli ma'lumotlar	1-5 TB/kun	5
Tarmoq trafiklari	Oqimli ma'lumotlar	50-100 GB/soat	4

Ma'lumotlarning katta hajmini tahlili natijasida monitoring tizimining samaradorligi ko'rsatkichlari kelib chiqadi. Monitoring tizimining samaradorligi quyidagi formula asosida baholanadi:

$$E = \frac{D_{pr}}{R_t \times V_d} \quad (2)$$

Bu yerda:

E - tizim samaradorligi

D_{pr} - to'g'ri tahlil qilingan ma'lumot miqdori (GB)

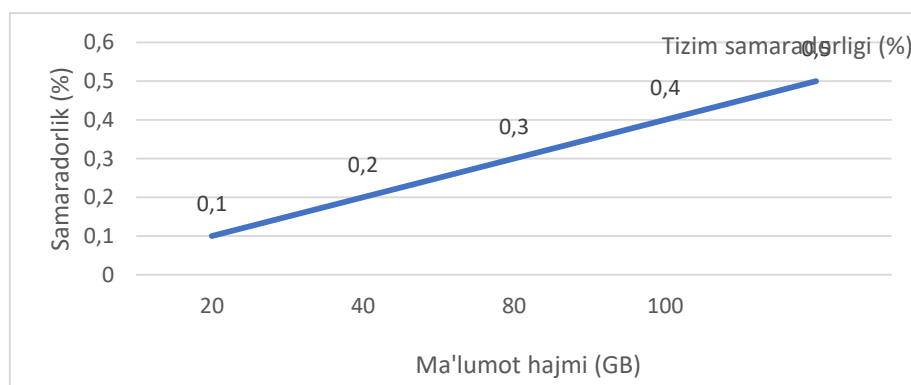
R_t - real vaqt rejimida ma'lumotni qayta ishlash tezligi (GB/soniya)

V_d - ma'lumot hajmi (GB)

Misol: Agar tizim 10 GB ma'lumotni 2 soniyada qayta ishlasa va ma'lumot hajmi 50 GB bo'lsa:

$$E = \frac{10}{2 \times 50} = 0,1 \text{ (ya'ni 10\% samaradorlik)} \quad (3)$$

Quyidagi rasmda ma'lumot hajmi va monitoring tizimining samaradorligi o'rtasidagi bog'liqlik tasvirlangan bo'lib, ma'lumot hajmi va monitoring tizimining samaradorligi quyidagicha bo'ladi:



3-rasm. Ma'lumot hajmi va monitoring tizimining samaradorligi

Rasmda ma'lumot hajmi oshgan sari monitoring tizimining samaradorligi pasayishini ko'rsatilgan bo'lib, bu holat tizim resurslari va qayta ishlash quvvatining chegaralanganligi bilan izohlanadi.

Xulosa sifatida ta'kidlash joizki, mavjud muammolarni bartaraf etish uchun kompleks yondashuv zarur bo'lib, bunda ilg'or texnologiyalar – sun'iy intellekt va mashinali o'qitish, tarmoq xavfsizligini boshqarishning avtomatlashtirilgan platformalari va kuchli normativ-huquqiy bazaning ishlab chiqilishi asosiy omil bo'lib xizmat qiladi. Shu bilan birga, muntazam ravishda mutaxassislarni tayyorlash va tizimlarning xavfsizlik darajasini oshirishga qaratilgan innovatsion tadbirlar muhim ahamiyat kasb etadi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

- [1] Stallings, W. Network Security Essentials: Applications and Standards. Pearson Education, 2017.
- [2] Conti, M. Security and Privacy in Internet of Things (IoT): Models, Algorithms, and Implementations. Springer, 2021.
- [3] Rouse, M. What is network monitoring? SearchNetworking, TechTarget, 2022.
- [4] Jo'rayev M.T. "Tarmoq oqimini monitoring qilish dasturiy tizimi" // Index Copernicus, 2024, 1(7), 73–77-betlar. (Index Copernicus)
- [5] Begbo'tayev A.E., Yusupov R.M. Tarmoq texnologiyalari (o'quv qo'llanma). Jizzax davlat pedagogika universiteti, 2021. (Jizzax Pedagogika Universiteti)
- [6] Ro'ziyev Y.Z., Abdullayeva B.S. Mediasavodxonlik va axborot madaniyati (darslik). Toshkent, 2024. (Renessans Ta'lim Universiteti)
- [7] Xamrakulov U.Sh., Risqaliyev J.D., Tashmanov Y.B. Ochiq ma'lumotlarga asoslangan tadqiqotlar: O'quv qo'llanma. Ichki ishlar vazirligi Malaka oshirish instituti, 2024. (ИПКМВД)
- [8] "Axborot xavfsizligining siyosati" // Nauchniy impuls, maqola, 2024. (Научный Импульс)

МЕТОД РАСЧЕТА ИНФОРМАЦИОННОЙ НАГРУЗКИ НА ПОЛЕВОЙ УЗЛОВ СВЯЗИ ПУНКТОВ УПРАВЛЕНИЯ

Д.Р. АБЗАЛОВ

Военный институт информационно- коммуникационных технологий и связи МО РУз

Аннотация. В данной статье рассмотрено модель прогнозирования информационной нагрузки, входящей на узел связи, способ формирования унифицированных рабочих мест должностных лиц и методика формирования структуры узла связи пунктов управления. Модель информационной нагрузки включает трафик от внутренних абонентов и других узлов связи с учетом потока служебных сообщений. Модель описывается самоподобным случайным процессом с распределением Вейбулла и включает поток мультимедийных приложений и передачи данных. Метод формирования унифицированных рабочих мест должностных лиц повышает эргономичность рабочего места офицера и обеспечивает услугами связи с учетом «Требований по обеспечению связью должностных лиц по видам и категориям».

Ключевые слова: унифицированное рабочее место (УРМ), пункт управления (ПУ), узел связи (УС) аппаратно-программные средства (АПС), часы наибольшей нагрузки (ЧНН), мультимедийное приложение (МП), передачи данных (ПД), эталонная модель взаимодействия открытых систем (ЭМОС).

Annotatsiya. Ushbu maqolada aloqa tuguniga kiradigan axborot yuklamasini bashorat qilish modeli, mansabdor shaxslar uchun yagona ish joylarini shakllantirish usuli va boshqaruv punktlari uchun aloqa tugunining tuzilishini shakllantirish metodologiyasi ko'rib chiqiladi. Axborotni yuklash modeli xizmat xabarlarini oqimini hisobga olgan holda ichki abonentlar va boshqa aloqa tugunlaridan trafikni o'z ichiga oladi. Veybull modeli o'ziga o'xshash tasodifiy jarayon bilan tavsiflanadi va multimedia dasturlari va ma'lumotlarni uzatish oqimini o'z ichiga oladi. Mansabdor shaxslar uchun yagona ish joylarini shakllantirish usuli ofitserning ish joyining yergonomikasini oshiradi va "mansabdor shaxslar uchun aloqa turlarini va toifalari bo'yicha ta'minlash talablarini" hisobga olgan holda aloqa xizmatlarini taqdim yetadi.

Kalit so'zlar: yagona ish joyi (YAIJ), boshqaruv punkti (BP), aloqa tuguni (AT), apparat va dasturiy ta'minot (ADT), maksimal yuklama soati (MYUS), multimedia ilovasi (MI), ma'lumotlar uzatish (MU), ochiq tizimlarning hamkorligi mos yozuvlar modeli (OTHHMYOM).

Abstract. This article examines a model for forecasting the information load entering a communications node, a method for forming unified workstations for officials, and a methodology for forming the structure of a communications node of control points. The information load model includes traffic from internal subscribers and other communication nodes, taking into account the flow of service messages. The model is described by a self-similar random process with a Weibull distribution and includes a flow of multimedia applications and data transmission. The method of forming standardized workstations for officials improves the ergonomics of the officer's workstation and provides communication services taking into account the "Requirements for providing communication to officials by type and category".

Keywords: unified workstation (UWP), communication node (CU), control point (CP), hardware and software (HAS), peak load hours (PLH), multimedia application (MA), data transmission (DT), reference model of open systems interaction (RMOSI).

Методика формирования структуры узла связи пунктов управления включает этапы формирования элементов узла связи, транспортной инфраструктуры и алгоритмы расчета показателей оценки качества предоставления видов связи и устойчивости функционирования.

Формирование элементов узла связи состоит из алгоритма выбора и обоснования принципа объединения технических средств в элементы узла связи позволяющих достичь максимальной устойчивости функционирования каждого вида связи, снизить вероятность информационной блокировки в часы наибольшей нагрузки. Выбор принципа объединения осуществляется по максимальному значению.

Значение информационной нагрузки, поступающей на вход узла связи, является исходным данным при формировании транспортной инфраструктуры и организации управления ресурсами сети УС. Следовательно, расчет входящего трафика позволит обеспечить выполнение требований к УС по пропускной способности. Количество передаваемых ДЛ сообщений в единицу времени изменяется в зависимости от обстановки и решаемых задач. [1]

Ранее были предложены методы расчета трафика для УС, но они не учитывали пакетной передачи данных, служебной информации передаваемой по сети, а также рассчитывались для каждой вторичной сети отдельно.

Трафик на УС определяется следующими факторами:

- количеством ДЛ в ПУ, состав и количество информационных направлений;
- видам связи, предоставляемыми должностным лицам;
- количеством и типом используемых аппаратно-программными средствами (аппаратно-программные средства ((АПС);
- решаемыми задачами в ходе операции;
- степенью боевой готовности;
- трудно формализуемыми психологическими факторами.

Расчет трафика предлагается проводить для часов наибольшей нагрузки (часы наибольшей нагрузки (ЧНН)), когда информационная нагрузка на УС близка к максимальной. [2, 6]

Трафик включает в себя внутреннюю (создаваемую ДЛ ПУ) и внешнюю (от других узлов) составляющие:

$$I_{\Sigma} = \mu(I_{\text{внутр}} + I_{\text{внеш}}) \quad (1)$$

где – суммарная нагрузка на УС;

μ – коэффициент, учитывающий служебную информацию;

$I_{\text{внутр}}$ – внутренняя нагрузка;

$I_{\text{внеш}}$ – внешняя нагрузка.

Принято считать, что служебная информация равна 5% от полезной нагрузки, тогда $\mu = 1,05$

Информационная нагрузка $I_{\text{внутр}}$ зависит от количества ДЛ в ПУ и «Требований по обеспечению связью должностных лиц по видам и категориям»:

$$I_{\text{внутр}} = \sum_{g=1}^M I_g \quad (2)$$

где M – количество должностных лиц, пользующихся услугами связи;

I_g – нагрузка, создаваемая j -ым должностным лицом.

Расчет I_g производится для случая односегментного участка сети, что позволяет избежать коллизий при доступе к среде передачи и свести к минимуму задержки. Трафик в сетях связи с коммутацией пакетов описывается самоподобными случайными процессами с параметром Херста $H = 0.7 \dots 0.9$. В самоподобных процессах вероятность поступления следующего события зависит не только от времени, но и от предыдущих событий. [3, 4, 7]

Передачу пакетов сообщений осуществляет терминальное оборудование ДЛ, которое представлено на рисунке 1.

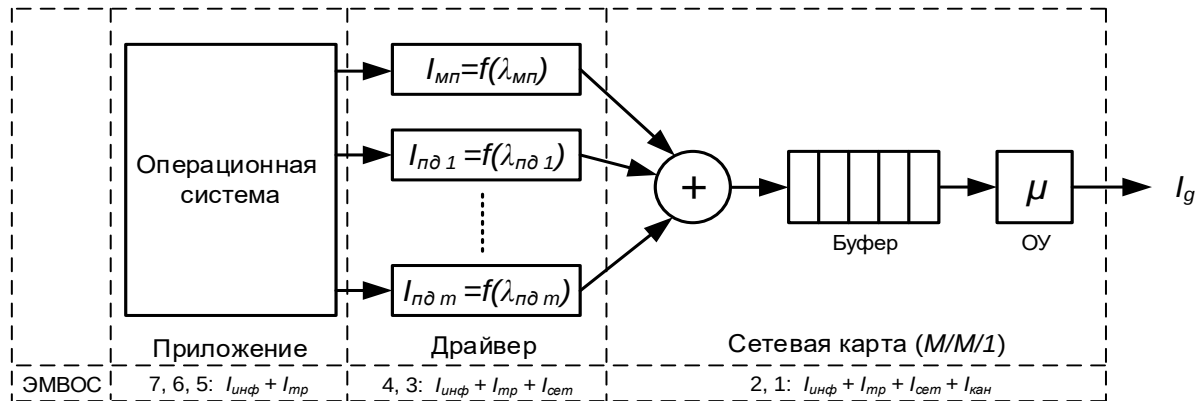


Рис.1. Схема терминального оборудования ДЛ

Предполагается, что должностное лицо ПУ, исходя из физиологических возможностей человека, использует одновременно одно мультимедийное приложение (МП) и несколько услуг передачи данных (ПД) и ЭП, следовательно определяется:

$$I_g = I_{МП} + I_{ПД} \quad (3)$$

где $I_{МП}$ – трафик, создаваемый мультимедийными приложениями;

$I_{ПД}$ – трафик, создаваемый приложениями передачи данных.

Значение $I_{МП}$ определяется применяемым видео (голосовым) кодеком и стеком протоколов [3]:

$$I_{МП} = \lambda_{МП}(VT_{TDU} + I_{МП}^{пр}) \quad (4)$$

где – количество пакетов, генерируемое мультимедийным приложением за секунду;

V – скорость работы кодека мультимедийной услуги;

T_{TDU} – длительность пакета мультимедийной услуги;

$I_{МП}^{пр}$ – нагрузка, вносимая стеком протоколов мультимедийной услуги связи, бит, определяется:

$$I_{МП}^{пр} = I_{тр} + I_{сет} + I_{кан} \quad (5)$$

где $I_{тр} + I_{сет} + I_{кан}$ – заголовки транспортного, сетевого и канального уровней соответственно.

Значение $I_{ПД}$ определяется количеством услуг, используемых одновременно одним ДЛ в ЧНН и имеет вид:

$$I_{ПД} = \sum_{i=1}^m N_i \quad (6)$$

где m – количество одновременно используемых услуг связи;

N_i – трафик, создаваемый i -ой услугой, бит.

Количество одновременно используемых ДЛ услуг связи m в ЧНН имеет пуассоновское распределение [17] с параметром Λ :

$$P_m(t) = \frac{(\Lambda t)^m}{m!} e^{-\Lambda t} \quad (7)$$

где – вероятность, что будет использоваться m услуг.

Трафик от i -ой услуги ПД определяется так:

$$N_i = K_i S_{ср.i} \quad (8)$$

где K_i – количество сообщений i -ой услуги;

$S_{\text{ср.}i}$ – среднее значение объема одного сообщения i -ой услуги, бит.

Зная количество символов в сообщении, объем данных в файле и вид применяемого в приложении кодека, а также учитывая специфику пакетной передачи, то выражение для размера файла в битах $S_{\text{ср.}i}$ примет вид:

$$S_{\text{ср.}i} = \text{round} (S_{\text{зн.}i} G_i / S_{\text{инф.}i}) (I_{\text{инф}}^i + I_{\text{пр}}^i) \quad (9)$$

где $S_{\text{зн.}i}$ – количество символов в i -ом сообщении;

G_i – параметры применяемого кодека в i -ом сообщении, бит/зн;

$S_{\text{инф.}i}$ – размер поля данных протокола передачи в i -ом сообщении;

$I_{\text{инф}}^i$ – размер поля данных протокола прикладного уровня в i -ом сообщении, бит;

$I_{\text{пр}}^i$ – нагрузка, вносимая протоколами нижнего уровня в i -ом сообщении.

Было доказано, что количество сообщений i -ой услуги K_i за время t определяется:

$$K_i = \lambda_i t + \sqrt{\lambda_i a} Z(t) \quad (10)$$

где a – масштабный коэффициент;

$Z(t)$ – нормированное фрактальное распределение с параметром Херста $H=0.7$;

λ_i – интенсивность потока сообщений i -ой услуги, которое определяется:

$$\lambda = \int_0^{\infty} x \omega(x) dx \quad (11)$$

Предполагается, что входной самоподобный цифровой поток описывается распределением Вейбулла, которое имеет следующий вид:

$$\omega(x) = \alpha \beta x^{\beta-1} e^{-\alpha x^{\beta}} \quad (12)$$

где α и β – параметры, влияющие на форму распределения.

Тогда выражение (11) с учетом (12) примет вид:

$$\lambda_i = \int_0^{\infty} x \alpha \beta x^{\beta-1} e^{-\alpha x^{\beta}} d(x) \quad (13)$$

Используя формулы (4) – (10), то выражение (3) примет вид:

$$I_g = \lambda_{\text{МП}} (I_{\text{тр.}} + I_{\text{сет}} + I_{\text{кан}})_{\text{МП}} + \sum_i^m (\lambda_i t + \sqrt{\lambda_i a} Z(t)) \left(\text{round} \left(\frac{S_{\text{знак}} * G}{S_{\text{инф}}} \right) (I_{\text{инф}}^{(i)} + (I_{\text{тр.}} + I_{\text{сет}} + I_{\text{кан}})_{\text{ПД}}^{(i)}) \right) \quad (14)$$

Внешняя нагрузка определяется пропускной способностью направления связи и их количеством и имеет вид:

$$I_{\text{внеш}} = \sum_{j=1}^N I_j \quad (15)$$

где N – количество информационных направлений связи;

I_j – трафик, приходящий с j -го направления.

Объем информации в системе управления удвоится примерно за 5-10 лет. Закладываемые в систему связи технологические основы не должны быть оптимальными для потребностей настоящего времени. Они должны обеспечивать своевременную передачу прогнозируемого на среднесрочную перспективу (10-15 лет) объема сообщений. Для учета будущего увеличения трафика I_{Σ} умножается на коэффициент запаса $k_z = (1, 2, \dots, 2, 0)$. [6, 7, 8, 10]

Данная методика определения информационной нагрузки позволяет оценить трафик создаваемый всеми должностными лицами ПУ с учетом категорий срочности, оценить

трафик, приходящий со всех информационных направлений, а также заложить ресурс по пропускной способности на перспективу. [9]

ВЫВОД:

1. Главной задачей методики является выбор рационального варианта структуры УС удовлетворяющего требованиям системы управления. На данном варианте осуществляется выбор показателей и обоснование критериев оценки эффективности функционирования УС. Построение модели входной нагрузки на УС.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

- [1] Боговик А.В., Игнатов В.В. Эффективность систем военной связи и методы ее оценки. – СПб.: ВАС, 2006.
- [2] Шерстнева О.Г. Математический метод расчета реальных показателей надежности участка сети сигнализации. ISSN 0013-5771. «Электросвязь», №6, 2009.
- [3] Шелухин О.И. Фрактальные процессы в телекоммуникациях./ О.И. Шелухин, А.М. Тенякшев, А.В. Осин. – М.: Радиотехника, 2003.- 480 с.
- [4] Моделирование развития информационно-телекоммуникационных систем. Под. ред. канд. техн. наук, д-ра экон. наук, проф. А.В. Бабкина. СПб.: Синтез Бук, 2009.
- [5] Мельников Ю.П., Попов С.В. Радиотехническая разведка. Методы оценки эффективности местоопределения источников излучений. – М.: «Радиотехника», 2008.
- [6] Глуховченко Р.Н. Основные узлы связи ТСС ВС и требования к сети связи.
- [7] Семенов Ю.В. Проектирование сетей связи следующего поколения.-СПб: Наука и техника. – 2005. – 240 с.
- [8] Сычев К.И. Многокритериальное проектирование мультисервисных сетей связи. – СПб.: Изд-во Политехнического университета, 2008. – 272 с.
- [9] Черноруцкий И.Г. Методы принятия решения. – СПб.: БХВ-Петербург, 2005. – 416 с.: ил.
- [10] Ногин В.Д. Принятие решений при многих критериях. Учебно-методическое пособие. – СПб.: Издательство «ЮТАС», 2007.
- [11] Галицкий А. В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети – анализ технологий и синтез решений. М.: ДМК Пресс, 2004. – 616 с.
- [12] Саати Т. Принятие решений. Метод анализа иерархий: Пер. с англ.- М.: Радио и связь, 1993. - 320 с.: ил.
- [13] Шварц М. Сети связи: протоколы, моделирование и анализ: в 2-х ч. Ч. 1: Пер. с англ. – М.: Наука. Гл. ред. физ-мат. лит., 1992.

УПРАВЛЕНИЕ СОВРЕМЕННЫМИ IT-ТЕХНОЛОГИЯМИ С ПОМОЩЬЮ ГОЛОСОВЫХ КОМАНД

А.А. АБИДОВ, О.Ш. АБДИРОЗИКОВ, Б.Н. УМАРАЛИЕВ, Ш.Р. САПАЕВ

Военный институт информационно-коммуникационных технологий и связи МО РУз

Аннотация: В современном развивающемся мире широко применяются IT-технологии, которые позволяют облегчить жизнь людей с ограниченными возможностями в повседневной жизни и быту, в том числе с применением голосового управления посредством голосовых команд. При использовании голосового помощника мы будем использовать язык программирования Python, а также использовать библиотеки для программы Python и исходная программа будет работать в офлайн режиме. В этой статье мы расскажем вам как просто использовать язык программирования Python на голосового помощника.

Ключевые слова: Alexa, виртуальный помощник, голосовой помощник, голосовые технологии, Google Assistant, искусственный интеллект, Python, Siri от Apple.

Abstract: In the modern developing world, IT technologies are widely used that make life easier for people with disabilities in everyday life and everyday life, including using voice control through voice commands. When using a voice assistant, we will use the Python programming language, as well as use libraries for the Python program and the original program will work offline. In this article, we will tell you how to easily use the Python programming language on a voice assistant.

Keywords: Alexa, virtual assistant, voice assistant, voice technologies, Google Assistant, artificial intelligence, Python, Siri from Apple.

Последние несколько лет использование голосовых технологий стало неотъемлемой частью нашей повседневной жизни. Начиная от голосовых помощников, таких как Siri и Alexa, и заканчивая устройствами Smart Home и голосовыми приложениями, голосовые команды сделали революцию в том, как мы взаимодействуем с технологиями. Но это не ограничивается голосовой технологией, которая может быть использована в личных целях, а также для коммерческих целей.[1]

В первую очередь любая бытовая техника, которая имеется в вашем доме, должна быть максимально функциональной и удобной в использовании. Голосовое управление, которое стало большим прорывом в области технологий, позволяет нам не только экономить массу времени, но и ощутить себя участником фантастической реальности.

На сегодняшний день уже нет необходимости в обсуждении преимуществ голосового управления по сравнению с обычным, стационарным или дистанционным. И совершенно ясно что голосовое управление может значительно облегчить жизнь человека. Речь идет не только о обычных пользователях, но и о людях с ограниченными возможностями, для которых голосовое управление может стать самым главным помощником в жизни.

Голосовые помощники – это программные помощники, которые могут выполнять различные задачи на основе голосовых команд пользователя. Они основаны на искусственном интеллекте и обычно используются на смартфонах, планшетах, интеллектуальных колонках и других устройствах, поддерживающих голосовой ввод.

Голосовые помощники распознают голосовые команды пользователя. Это включает в себя понимание произносимых слов и предложений. Как только голосовой помощник распознает команду, он предпримет соответствующие действия. Это может быть что-то простое, например запуск приложения на вашем устройстве, отправка текстового сообщения, установка напоминания и т.д. Большинство современных голосовых помощников используют технологию искусственного интеллекта для повышения своей

производительности. Они могут адаптироваться к предпочтениям пользователя, улучшать понимание естественного языка и предоставлять персонализированные рекомендации. Голосовые помощники могут взаимодействовать с различными домашними устройствами, такими как смарт-телевизоры, интеллектуальные колонки, системы умного дома и другие интеллектуальные устройства, позволяя пользователям управлять ими с помощью голоса.

К самым популярным голосовым помощникам относятся Siri от Apple, Google Assistant от Google, Alexa от Amazon и Cortana от Microsoft. Поскольку голосовые помощники могут обрабатывать конфиденциальные данные пользователей, вопросы безопасности и конфиденциальности становятся важным аспектом их использования. Производители голосовых помощников обычно принимают меры для защиты пользовательских данных, такие как шифрование данных и настройка параметров конфиденциальности.

Какие преимущества предлагают голосовые помощники?

- производительность системы и скорость доступа;
- Удовлетворение потребностей людей;
- Многозадачность;
- Попросите точную обработку.

Голосовые помощники могут быть личными или общими.

Личными колонки можно разделить на три типа: для смартфонов, для умных колонок и для дома. Например, Siri и Google Assistant нашли свое место и становятся все более популярными в смартфонах. А вот Алису чаще просят включить что-нибудь на умных колонках. Alexa приобретает популярность благодаря своим колонкам, с помощью которых можно управлять своим умным домом, а также размещать заказы на Amazon.

Общие голосовые помощники используются предприятиями для обслуживания клиентов. Информацию о них можно найти в нашем тексте ниже.

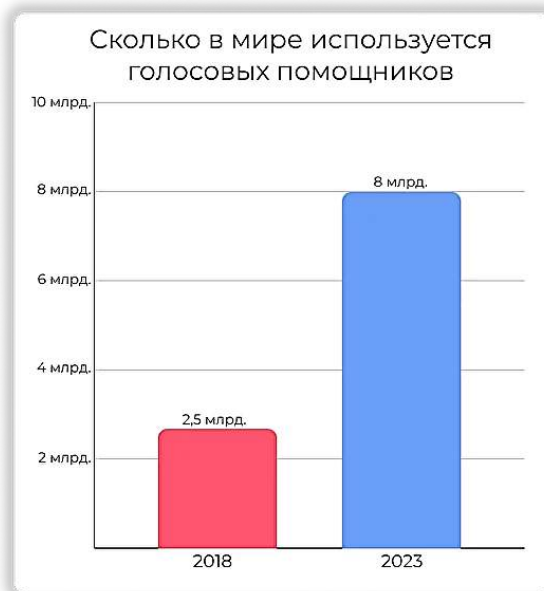


Рис.-1. Сравнения голосовых помощников в мире

Голосовые помощники становятся все более популярными, по крайней мере в повседневной жизни, среди обычных людей. По данным Juniper Research, к 2023 году во всем мире будет использоваться более 8 миллиардов голосовых помощников. Для сравнения, в конце 2018 года их было 2,5 миллиарда.[2]

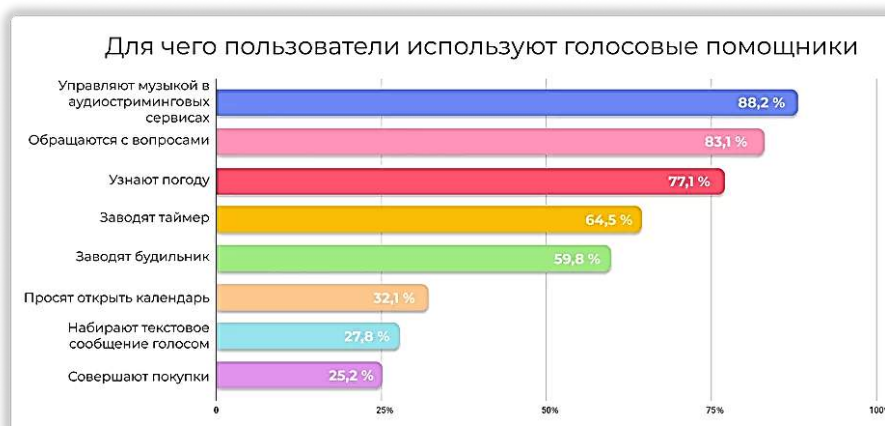


Рис.-2. Использование голосового помощника в мире

Чтобы понять человеческий голос, искусственный интеллект разбивает слова на звуки, точнее на небольшие части звуков длительностью в сотые доли секунды – фонемы. Затем каждая часть слова обрабатывается математически, создавая коэффициенты, описывающие частотные характеристики звуковой части. Голосовой помощник использует эти данные для определения голосового запроса.

Иногда голосовой помощник не понимает предложение и затем дополняет слово из контекста всего предложения. Для этого у помощников есть таблица вероятностей перехода, в которой описаны возможные последовательности букв в словах. Кстати, такие знаки помогают распознавать запросы пользователей по акценту. Так, например, в Siri вы можете выбрать британский или американский английский.

Если вы спросите своего голосового помощника: «Как дела?», «Что нового?» или попросить рассказать анекдот, помощник часто поддерживает разговор с пользователем на совершенно естественном уровне посредством коротких светских бесед. А форма голосовых помощников все больше приобретает человеческие характеристики: имя, пол, голос и может быть, даже чувство юмора. Так как же голосовые помощники учатся быть человечным?

Если виртуальные помощники используют сложные вычисления для распознавания голосов, то вопрос человечности можно решить с помощью большого списка ответов, написанного редакторами и психологами. Это подготовленные экспертами голосовые сообщения с продуманными сценариями, содержащими ответы на самые популярные вопросы и запросы людей. Редакторы намеренно создают ответов в стиле, который будет гармонизировать с образом голосового помощника, чтобы образ был более человечным.

Переходим на эту ссылку и скачиваем базу распознавания речи: <https://alphacephei.com/vosk/>.

Vosk — это серия инструментов распознавания речи. Лучшее в Воске:

Поддерживает более 20 языков и диалектов: английский, индийский английский, немецкий, французский, испанский, португальский, китайский, русский, турецкий, вьетнамский, итальянский, голландский, каталанский, арабский, греческий, фарси, филиппинский, украинский, казахский, шведский, японский, эсперанто, хинди, чешский, польский, узбекский, корейский, бретонский, гуджарати и других.

Привязки распознавания речи реализованы для различных языков программирования, таких как Python, Java, Node.JS, C#, C++, Rust, Go и других.

Vosk обеспечивает распознавание речи для чат-ботов, умной бытовой техники и виртуальных помощников. Вы также можете создавать субтитры для фильмов, стенограмм лекций и интервью.[3]

Пример голосовому помощнику: пишем программу на языке Python и программируем две программы:

1. Пищим текст, а программа нам отвечает с динамика;
2. Подаём команду голосом в программу и текст записывается.

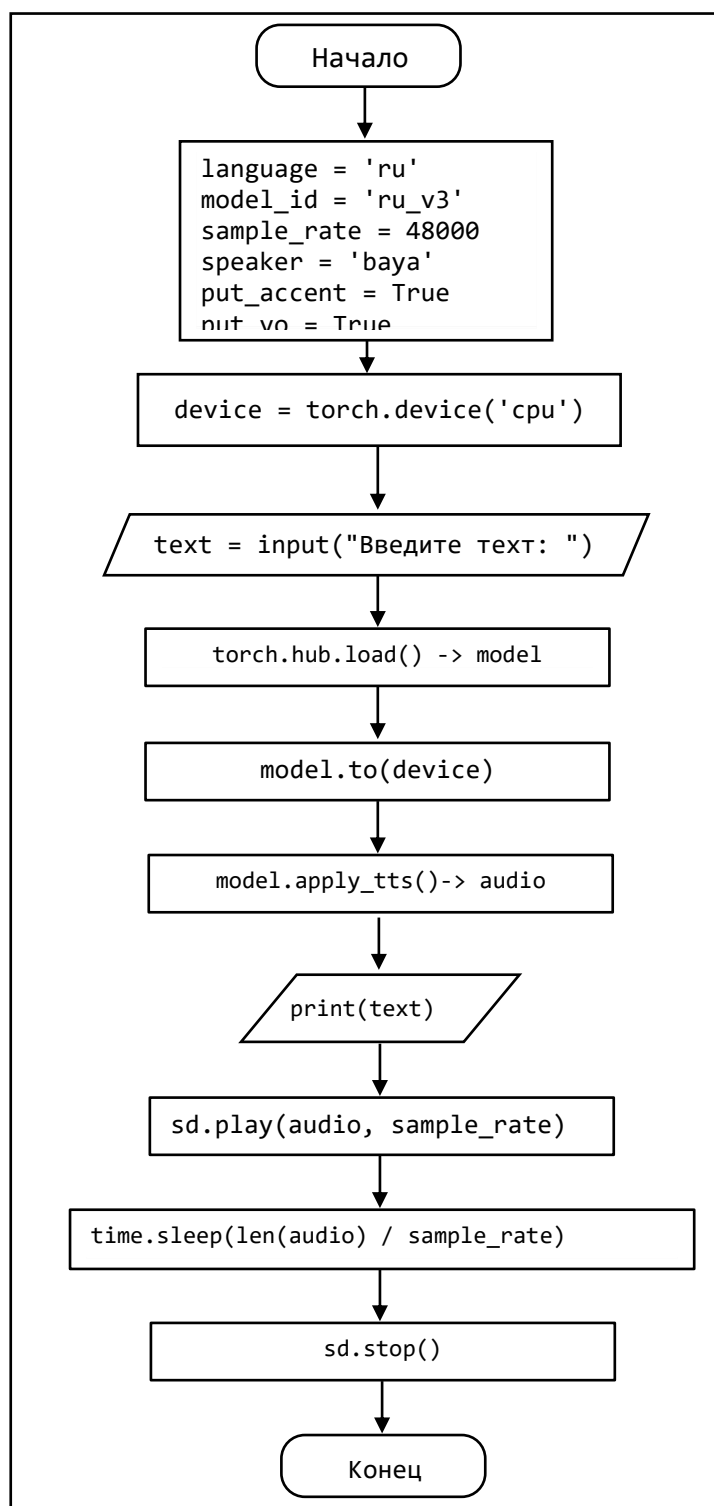


Рис.-3. Блок схема голосового помощника

```

import torch #библиотека
import sounddevice as sd #библиотека
import time #библиотека
language = 'ru'
model_id = 'ru_v3'

```

```

sample_rate = 48000
speaker = 'baya'
put_accent = True
put_yo = True
device = torch.device('cpu')
text = input("Введите текст: ")
model, _ = torch.hub.load(repo_or_dir='snakers4/silero-models',
                           model='silero_tts',
                           language=language,
                           speaker=model_id)
model.to(device)
audio = model.apply_tts(text=text,
                        speaker=speaker,
                        sample_rate=sample_rate,
                        put_accent=put_accent,
                        put_yo=put_yo)
print(text)
sd.play(audio, sample_rate)
time.sleep(len(audio) / sample_rate)
sd.stop()

```

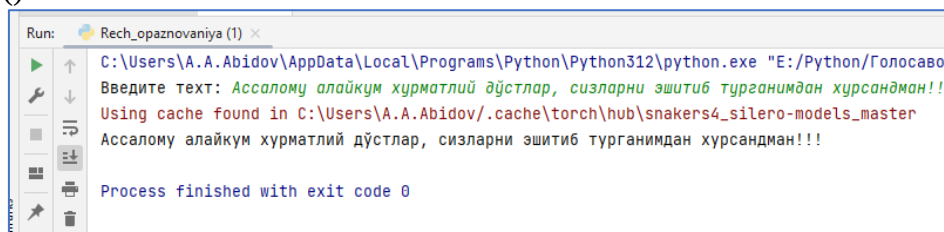


Рис.-4. Результат голосового помощника вариант-1

2 вариант программного кода голосового помощника:

```

import vosk
import sys
import sounddevice as sd
import queue
model = vosk.Model("model_small")
samplerate = 48000 # вродеа рекомендуется от 8Hz до 16Hz
device = 1 # Записи(микрофона)
q = queue.Queue()
def callback(indata, frames, time, status):
    if status:
        print(status, file=sys.stderr)
    q.put(bytes(indata))
with sd.RawInputStream(samplerate=samplerate, blocksize=8000, device=device,
dtype='int16',
                      channels=1, callback=callback):
    rec = vosk.KaldiRecognizer(model, samplerate)
    while True:
        data = q.get()
        if rec.AcceptWaveform(data):
            print(rec.Result())

```

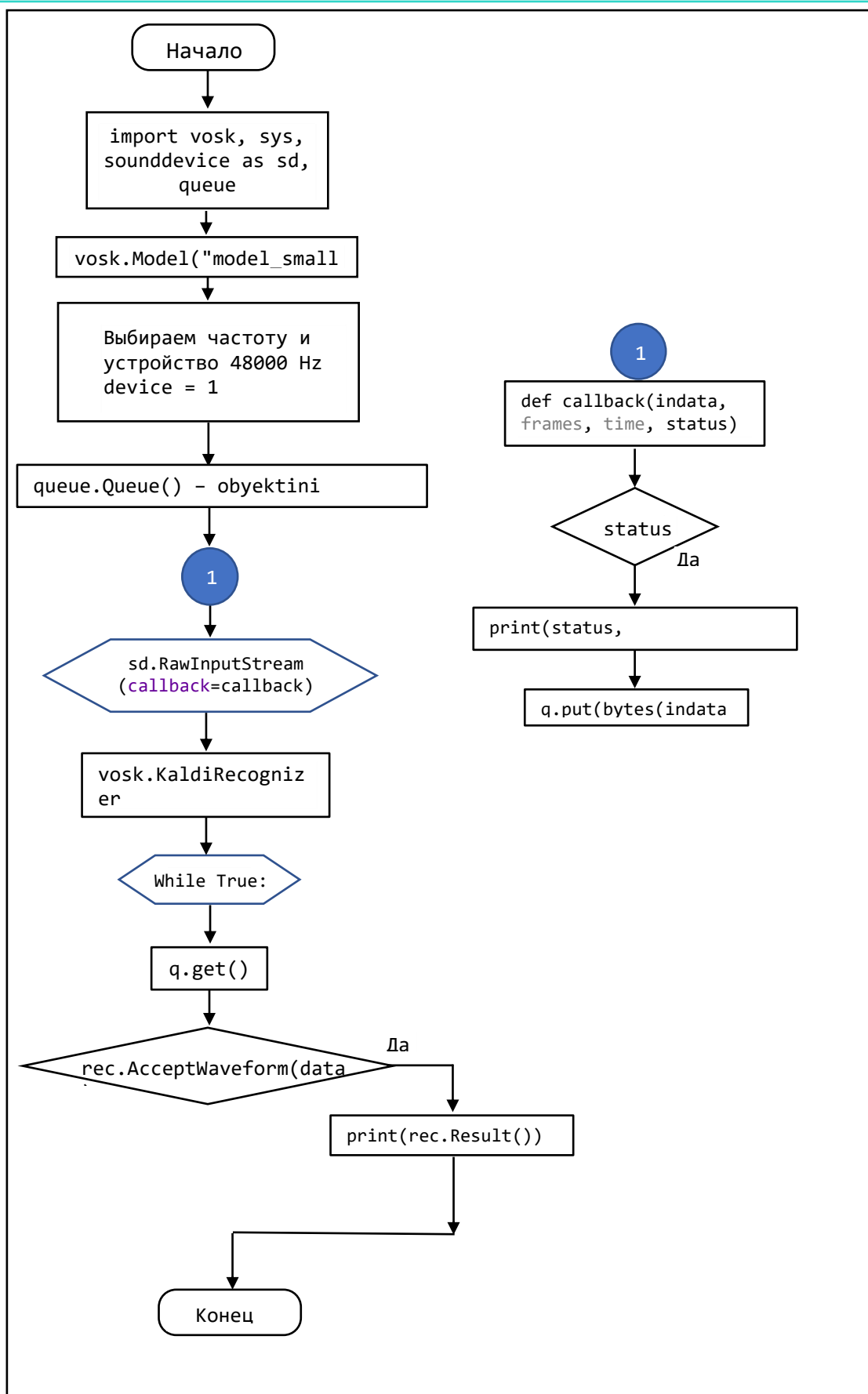


Рис.-5. Блок схема голосового помощника 2 ого варианта

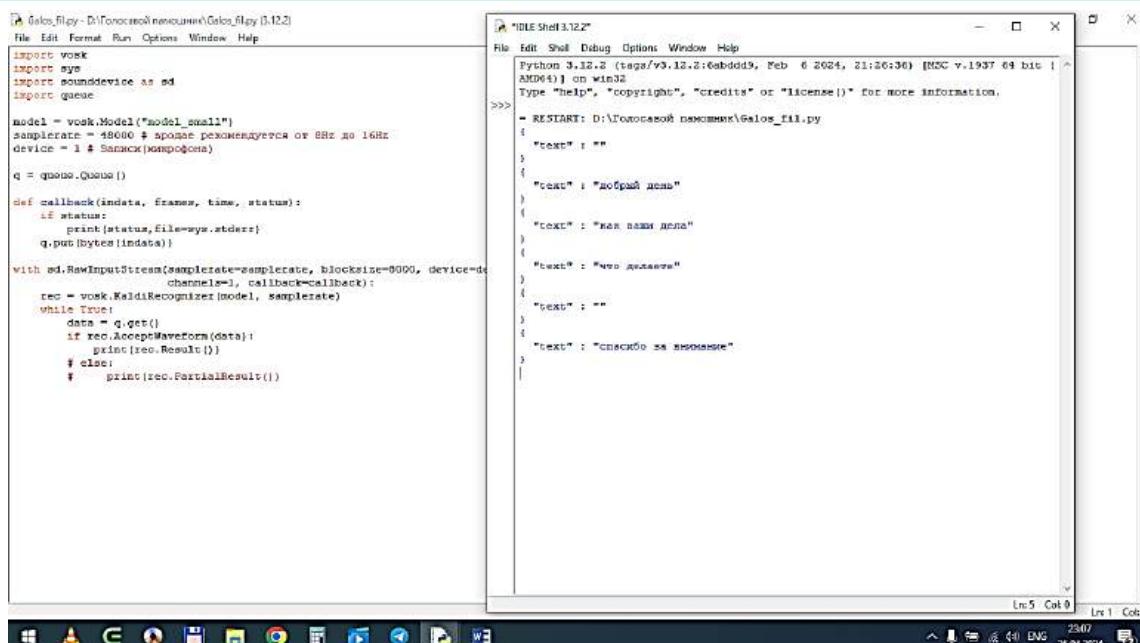


Рис.-6. Результат голосового помощника вариант-2

В заключение отметим, что вступление в эпоху голосовых технологий – это не просто тенденция, а необходимость для потребителей, которые хотят процветать в эпоху цифровых технологий. Возможности, которые предлагают голосовые технологии, огромны и разнообразны от расширения возможностей для бизнеса до повышения вовлеченности клиентов, повышения производительности и получения конкурентных преимуществ. Используя голосовые технологии, пользователи могут оказаться в авангарде цифровой революции, обеспечивая долгосрочный успех и развитие, заботясь о своем благополучии. Итак, давайте воспримем эпоху голоса и изучим весь потенциал преимуществ в эту захватывающую новую эпоху. Голосовые помощники становятся все более распространенными и интегрируются в нашу повседневную жизнь, предоставляя удобный и эффективный способ взаимодействия с технологиями. Очевидно, что при большей подготовке виртуальных помощников качество их услуг станет еще более совершенным и будет внедрено в другие сферы, например, медицину, обучение, транспорт, а также в повседневную жизнь людей.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

- [1] <https://fastercapital.com/ru/content/Почему-голосовая-технология---это-будущее-предпринимательства.html>
- [2] <https://rocketdata.ru/blog/voice-search-market>
- [3] <https://alphacephei.com/vosk/>
- [4] <https://cyberleninka.ru/article/n/golosovye-pomoschniki/viewer>
- [5] <https://journal.tinkoff.ru/best-smart-assistants/>
- [6] <https://xiaomi-smarthome.ru/vybor-golosovogo-pomoshhnika-dlya-umnogo-doma-xiaomi/>
- [7] <https://zoom.cnews.ru/publication/item/64123>
- [8] <https://www.kubsu.ru/sites/default/files/users/60639/portfolio/grishch>
- [9] <https://medium.com/nuances-of-programming/> создание-локально-работающего-голосового-помощника-4a1201dd3391

MQTT PROTOKOLI ASOSIDA IOT QURILMASIDA MOSQUITTO, HIVEMQ, ADAFRUIT IO BROKERLARINING SAMARADORLIGINI TAQQOSLASH

PhD., professor B.K. YUSUPOV

PhD., dotsent B.O. MUHAMADOV

O'R MV Axborot kommunikatsiya texnologiyalari va aloqa harbiy inistituti

Annotatsiya. Ushbu maqolada MQTT protokoli asosida ishlab chiqilgan IoT qurilmasi orqali Mosquitto, HiveMQ va Adafruit IO brokerlarining samaradorligi taqqoslab tahlil qilingan. Qurilma ESP32 mikrokontrolleri, DHT11 harorat sensori va LED dioddan iborat bo'lib, har 5 soniyada ma'lumot uzatadi. Brokerlarning samaradorligi kechikish va paket yo'qotish foizi bo'yicha solishtirildi.

Kalit so'zlar: IoT, internet, MQTT, broker, Mosquitto, HiveMQ, Adafruit IO, paketlar, ESP32, DHT11.

Аннотация: В данной статье рассматривается сравнение эффективности брокеров Mosquitto, HiveMQ и Adafruit IO на основе IoT-устройства, разработанного с использованием протокола MQTT. Устройство, состоящее из микроконтроллера ESP32, датчика температуры DHT11 и светодиода, передавало данные каждые 5 секунд.

Ключевые слова: IoT (Интернет вещей), интернет, MQTT, брокер, Mosquitto, HiveMQ, Adafruit IO, пакеты, ESP32, DHT11.

Abstract. This article analyzes the efficiency of Mosquitto, HiveMQ, and Adafruit IO brokers using an MQTT-based IoT device. The device, consisting of an ESP32 microcontroller, DHT11 temperature sensor, and LED, transmitted data every 5 seconds. Latency and packet loss metrics were compared.

Keywords: IoT, internet, MQTT, broker, Mosquitto, HiveMQ, Adafruit IO, packets, ESP32, DHT11.

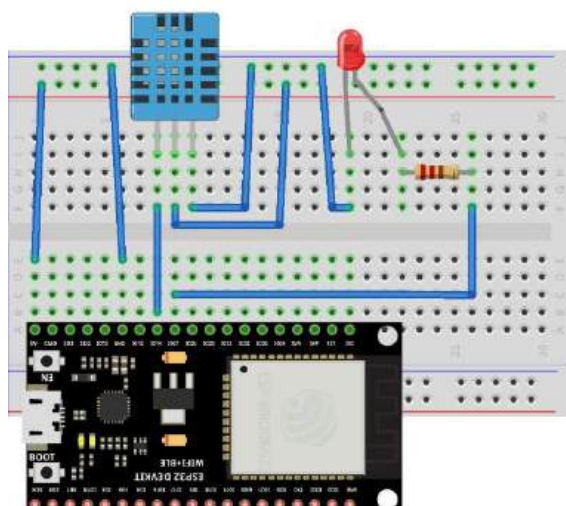
Internet o'z faoliyatini kichik, o'zaro bog'langan kompyuterlar tarmog'i sifatida boshlagan. Bugungi kunda esa u nafaqat kompyuterlar, balki turli xil qurilmalarni o'z ichiga olgan va ular orqali ma'lumot almashadigan va saqlaydigan Global tarmoqqa aylandi.

IoT (Internet of Things) yoki "Narsalar interneti" — bu turli xil qurilmalar, sensorlar va obyektlar o'zaro bir-biriga bog'lanib, ma'lumot almashish imkonini beruvchi tarmoq hisoblanadi. Ushbu qurilmalar internet orqali ulanishi va bir-biriga bog'lanishi natijasida, foydalanuvchilar o'z uylarini, transportni, sog'liqni saqlash tizimlarini va boshqa sohalarni avtomatlashtirish va boshqarish imkoniyatiga ega bo'lishadi. Bugungi kunda IoT texnologiyalari hayotimizni yanada qulayroq va samarali qilishga yordam bermoqda[1].

Narsalar Interneti (IoT) sohasining rivojlanishi sanoat, sog'liqni saqlash, qishloq xo'jaligi va aqlli uy kabi ko'plab sohalarda axborotni masofaviy monitoring qilish imkonini bermoqda. IoT qurilmalari odatda kam resursli mikrokontrollerlar asosida ishlab chiqiladi va ular uchun yengil, xavfsiz va ishonchli ma'lumot uzatish protokollaridan biri bu MQTT hisoblanadi[2].

MQTT (Message Queuing Telemetry Transport) protokoli mijoz-server arxitekturasiga asoslangan bo'lib, asosan brokerlar orqali ma'lumot uzatadi. MQTT – ma'lumotlarni past quvvat bilan, samarali uzatishni ta'minlaydigan yengil protokol bo'lib, sensorlar va qurilmalar o'rtasida ma'lumot uzatish uchun keng qo'llaniladi. MQTT ma'lumotlarni "Publish" va "Subscribe" (e'lon qilish va qabul qilish) modeli asosida uzatadi, bu esa tarmoqlarni samarali boshqarish imkonini beradi. Ushbu protokollar IoT tizimlarida energiyani samarali ishlatish imkonini beradi va qurilmalarni uzoq muddat ishlatishga imkon yaratadi[3].

Ushbu maqolada ESP32 asosida ishlab chiqilgan IoT qurilmasida Mosquitto, HiveMQ hamda Adafruit IO brokerlari bilan o'tkazilgan samaradorlikni tekshirish sinovlari natijalari tahlil qilinib xulosalar keltirilgan.



1-rasm. IoT qurilmasining ulanish chizmasi

IoT qurilmasi ESP32 mikrokontroller, DHT11 harorat va namlik sensori va LED diodlaridan tashkil topgan. Qurilmaning ulanish chizmasi 1-rasmda keltirilgan.

ESP32 har 5 soniyada DHT11 sensoridan o'qilgan harorat qiymatini brokerga yuboradi. Broker orqali kelgan led/on yoki led/off komandasi asosida ESP32 LED ni yoqadi yoki o'chiradi. Ma'lumot uzatish uchun MQTT protokoli ishlatildi.

Tajriba o'tkazish sharoitlari

Tajriba davomida har bir broker alohida 1 soat davomida sinovdan o'tkazildi. Sinovlar bir xil Wi-Fi tarmog'ida, ESP32 qurilmasi tarmoq routeriga 1 metr masofada joylashgan holatda amalga oshirildi. Har 5 soniyada bitta publish va unga javoban subscribe amalga oshirilib, 720 ta sinov yozuvi olindi. Quyidagi mezonlar asosida baholash amalga oshirildi:

- RTT (round-trip time): yuborilgan xabar brokerga yetib borib, javob sifatida qaytguncha o'tgan vaqt[4].

- Paket yo'qotilishi: yuborilgan xabarlardan brokerga yetib bormagan yoki javobsiz qolganlar foizi[5].

- CPU yuklanishi: ESP32 protsessorining bir tsiklda ishlashga sarflagan umumiy vaqti asosida hisoblandi[6].

RTT (round-trip time) ko'rsatkichini hisoblash uchun ESP32 qurilmasida millis() funksiyasi bilan publish() yuborilish va subscribe() orqali xabar qabul qilish vaqt farqi o'lchandi. Buning uchun ESP32 mikrokontrolleriga quyidagi kod qismi kiritildi:

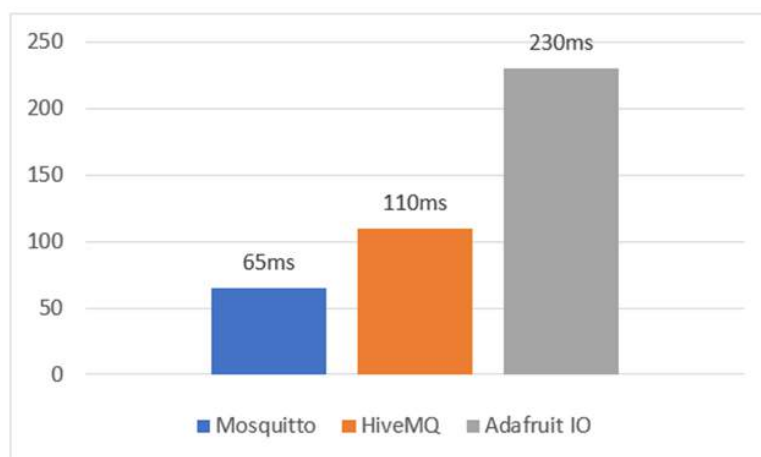
```
unsigned long startTime = millis();
client.publish("temp/data", tempString);
unsigned long endTime = millis();
unsigned long rtt = endTime - startTime;
```

Bu jarayon 720 marta bajarildi (1 soat davomida har 5 soniyada ma'lumot yuborilgan, 1 soatda $3600/5 = 720$ marta signal uzatilgan).

O'rtacha RTT quyidagi 1-formula asosida hisoblandi[7]:

$$RTT_{avg} = \frac{\sum_{i=1}^{720} RTT_i}{720} \quad (1)$$

Barcha brokerlar bilan o'tkazilgan tajribalar asosida olingan RTT ko'rsatkichlari natijalarining grafik ko'rinishi 2-rasmda keltirilgan.

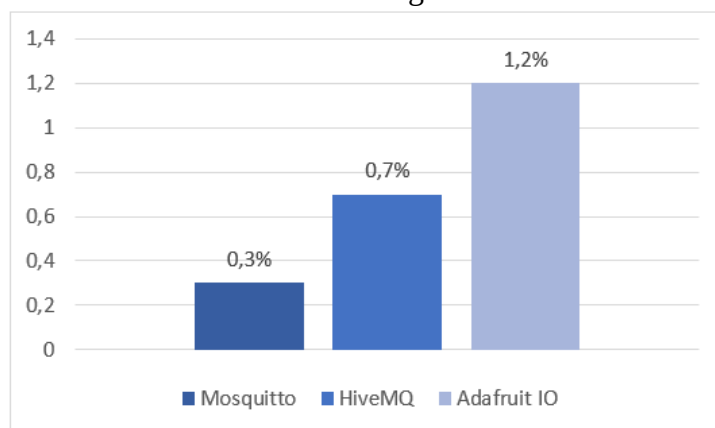


2-rasm. Brokerlar RTT ko'rsatkichlari

Paket yo'qotilishi ko'rsatkichini aniqlash uchun yuborilgan 720 ta xabarning har biridan keyin subscriber tomonidan message arrived bo'lishi kutildi. Agar message arrived 1 soniyada kelmasa, "yo'qolgan" deb belgilandi hamda 2-formula orqali hisoblandi[8].

$$\text{Paket yo'qotilishi (\%)} = \frac{\text{Kelmagan xabarlar soni}}{720} * 100 \quad (2)$$

Barcha brokerlar bilan o'tkazilgan tajribalar asosida olingan paketlar yo'qotilishi ko'rsatkichlarining grafik ko'rinishi 3-rasmida keltirilgan.



3-rasm. Brokerlardagi paketlar yo'qotilishi ko'rsatkichlari

CPU yuklanishi (%) ni aniqlash

ESP32 da to'g'ridan-to'g'ri markaziy protsessorga yuklamani o'lchash qiyin, lekin nisbiy metodik yondashuv bilan amalga oshirish mumkin. Buning uchun loop() funksiyasi ichida micros() bilan har siklning davomiyligi o'lchanadi[9].

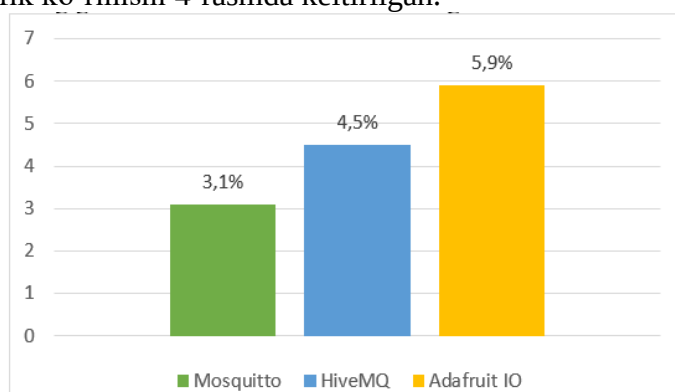
```
unsigned long loop_start = micros();
unsigned long loop_end = micros();
```

Olingan qiymatlar asosida ish vaqtining umumiy siklga nisbatini 3-formula orqali hisoblanadi:

$$\text{CPU_load} = \frac{\text{loop_end} - \text{loop_start}}{t} * 100 \quad (3)$$

Bu yerda t – bu sikl vaqti, bizning tajribamizda 5 sekundga teng. micros() funksiyasi mikrosekundlarda ishlagani sababli t vaqt mikrosekundlarda kiritildi. Ya'ni, 5 sekund = 500000 mikrosekund.

Barcha brokerlar bilan o'tkazilgan tajribalar asosida olingan CPU yuklanishi ko'rsatkichlarining grafik ko'rinishi 4-rasmda keltirilgan.



4-rasm. ESP32 markaziy protsessoridagi yuklanish ko'rsatkichlari

Brokerlarning ishonchlilik ko'rsatkichlari paketlardagi yo'qotishlar asosida quyidagi 4-formula orqali hisoblandi[10]:

$$K_{\text{ishonchlilik}} = 100 - P (\%) \quad (4)$$

1-jadval.

Brokerlar samaradorligi

Broker	RTT (ms)	Paket yo'qotilishi (%)	CPU yuklanish (%)	Ishonchlilik (%)
Mosquitto	65	0.3	3.1	99.7
HiveMQ	110	0.7	4.5	99.3
Adafruit IO	230	1.2	5.9	98.1

Olib borilgan tadqiqot natijalari shuni korsatmoqdaki, Mosquitto lokal broker bo'lgani sababli RTT eng past bo'ldi. HiveMQ umumiy serverda ishlayotgan bo'lsa-da, barqaror ishlashni ta'minladi. Adafruit IO interfeys jihatdan qulay bo'lsa-da, kechikish va yo'qotish foizi yuqoriroq bo'ldi. Adafruit IOda LED komandalari ba'zan 2 soniyagacha kechikib yetib kelgan. HiveMQ

1 soniya atrofida ishladi. Mosquitto real-time ishlash talab qilinadigan holatlarda yuqori ustunlikka ega.

Xulosa. Ushbu maqolada ESP32 asosida ishlab chiqilgan IoT qurilmasi orqali Mosquitto, HiveMQ va Adafruit IO brokerlari sinovdan o'tkazildi. Sinov natijalari asosida quyidagilarni xulosa qilish mumkin:

- Mosquitto: Mahalliy tarmoqda ishlatilganda ishonchlilik va tezlik bo'yicha eng yaxshi natijalarni berdi.

- HiveMQ: Bulutli muhitda yetarlicha barqaror ishladi, kichik kechikishlarga ega.

- Adafruit IO: Yangi o'rganuvchilar va grafik kuzatuvlar uchun foydali, lekin tezlik va yo'qotish foizi yuqoriroq.

IoT qurilmalarini ishlab chiqishda, tarmoq va vazifaga qarab broker tanlanishi zarur. Real-time monitoring talab qilinadigan loyihalarda Mosquitto, umumiy tarmoqda HiveMQ, vizual interfeys kerak bo'lsa Adafruit IO tavsiya etiladi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

[1] Abdug'aniyev B.B. "Narsalar interneti (IoT) xavfsizligi" // "International scientific and practical conference "smart technologies and innovative approaches in research: building a digital future", FEBRUARY 22, 2025 85-87-b.

- [2] Aman M. N., Chua K. C., Sikdar B. Mutual Authentication in IoT Systems Using Physical Unclonable Functions // IEEE Internet of Things Journal. 2017. № 5 (4). P. 1327–1340.
- [3] Raxmatullayev D. A., Nurillayev B.Sh., “IoT tizimlarida energiya samaradorligini oshirish va energiya tejash imkoniyatlari”//“Экономика и социум” №1(128)-2 2025, 1008-1012-b.
- [4] Dr. Sarika Choudhary, Gaurav Meena Internet of Things: Protocols, Applications and Security // ScienceDirect Procedia Computer Science 215 (2022) P. 274–288
- [5] Afzal, B., Umair, M., Shah, G.A., Ahmed, E., 2019. Enabling IoT platforms for social IoT applications: vision, feature mapping, and challenges. // Future Generation Computer Systems 92, P. 718–731.
- [6] Anthi, E., Williams, L., Słowinska, M., Theodorakopoulos, G., Burnap, P., 2019. A supervised intrusion detection system for smart home iot devices.// IEEE Internet of Things Journal 6, 9042–9053. doi:10.1109/JIOT.2019.2926365.
- [7] Ashton, K., That ‘internet of things’ thing. RFID journal 22, 2022 P. 97–114.
- [8] Baronti, P., Pillai, P., Chook, V.W., Chessa, S., Gotta, A., Hu, Y.F., Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and zigbee standards. // Computer communications 30, 2017 P. 1655–1659.
- [9] Bawany, N.Z., Shamsi, J.A., Seal: Sdn based secure and agile framework for protecting smart city applications from ddos attacks.// Journal of Network and Computer Applications 145, 2022 P. 102-106.
- [10] Bormann, C., Castellani, A.P., Shelby, Z., Coap: An application protocol for billions of tiny internet nodes. // IEEE Internet Computing 16, 2022 P. 62–67..

TARMOQ MONITORINGI AVTOMATIZATSIYASI UCHUN ZARUR TEXNIK YECHIMLAR VA IQTISODIY XARAJATLAR TAHLILI

PhD, dotsent I.I. NISHANOV, SH.T.MAHMUDOV

O'R MV Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti

Annotatsiya. Mazkur maqolada tarmoq monitoringi tizimini avtomatlashtirish bo'yicha dastlabki investitsiyalar, doimiy texnik xizmat ko'rsatish va tizimni muntazam yangilash bilan bog'liq xarajatlar tahlil qilinadi. Unda avtomatlashtirilgan monitoring tizimlarining samaradorligi, moliyaviy barqarorligi va texnik xizmatlarning uzluksizligi uchun zarur bo'lgan asosiy xarajatlar ko'rib chiqiladi. Maqola tarmoq boshqaruvi sohasida ish olib boruvchi mutaxassislar hamda moliyaviy rejalashtirish bilan shug'ullanuvchi tadqiqotchilar uchun mo'ljallangan.

Kalit so'zlar: tarmoq monitoringi, avtomatlashtirish, texnik xizmat, investitsiya, xarajatlar.

Аннотация. В данной статье анализируются первоначальные инвестиции, затраты на постоянное техническое обслуживание и регулярное обновление системы автоматизированного сетевого мониторинга. Рассматриваются основные расходы, необходимые для эффективности, финансовой устойчивости и непрерывности технической поддержки таких систем. Статья предназначена для специалистов в области сетевого управления и исследователей, занимающихся финансовым планированием.

Ключевые слова: сетевой мониторинг, автоматизация, техническое обслуживание, инвестиции, расходы.

Abstract. This article analyzes the initial investments, ongoing technical maintenance costs, and regular update expenses related to the automation of network monitoring systems. It examines the key expenditures required for ensuring the efficiency, financial stability, and uninterrupted technical support of such systems. The article is intended for professionals in network management and researchers involved in financial planning.

Key words: network monitoring, automation, technical maintenance, investment, costs

Raqamli transformatsiya jarayonlari tez sur'atlarda rivojlanayotgan hozirgi kunda axborot-kommunikatsiya texnologiyalari barcha sohalarda markaziy o'rinni egallamoqda. Keng qamrovli va murakkab raqamli infratuzilmalar uzluksiz ishlashi uchun ularning holatini real vaqt rejimida monitoring qilish va samarali boshqarish talab etiladi. Bu esa tarmoq monitoringini avtomatlashtirish zaruratini yuzaga keltiradi.

Tarmoq monitoringini avtomatlashtirish tizimlari tarmoqlardagi nosozliklarni erta aniqlash, xavfsizlik tahdidlarini bartaraf etish va tizimlarning barqaror ishlashini ta'minlash imkonini beradi. Biroq ushbu tizimlarni joriy qilish va samarali ishlatish jarayoni ma'lum bir kapital va operatsion xarajatlar talab qiladi. Xususan, dastlabki investitsiyalar, dasturiy va apparat ta'minot xarajatlari, litsenziya va obuna to'lovlari, shuningdek, uzluksiz texnik xizmat ko'rsatish va tizimlarni yangilab borish xarajatlari muhim ahamiyatga ega [1].

Tarmoq monitoringi tizimini avtomatlashtirish dastlabki investitsiya, uzluksiz texnik xizmat va yangilash xarajatlari bilan bog'liq bo'lib, bu jarayon uzoq muddatli iqtisodiy rejalashtirishni talab qiladi. Monitoring tizimining umumiy xarajatlarini baholash uchun quyidagi formulalardan foydalaniladi hamda umumiy xarajat modeli (Total Cost - TC) quyidagicha ifodalanadi:

$$TC=I+M+U \quad (1)$$

Bu yerda:

I – Dastlabki investitsiya xarajatlari (Initial Investment)

M – Texnik xizmat ko'rsatish xarajatlari (Maintenance Cost)

U – Yangilash va modernizatsiya xarajatlari (Upgrade Cost)

Uzoq muddatli xarajatlarning amortizatsiyasi (Annual Cost - AC):

$$AC = \frac{TC}{N} \quad (2)$$

formula orqali hisoblanadi. Bu yerda: N – Tizimning ekspluatatsiya muddati (yillar).

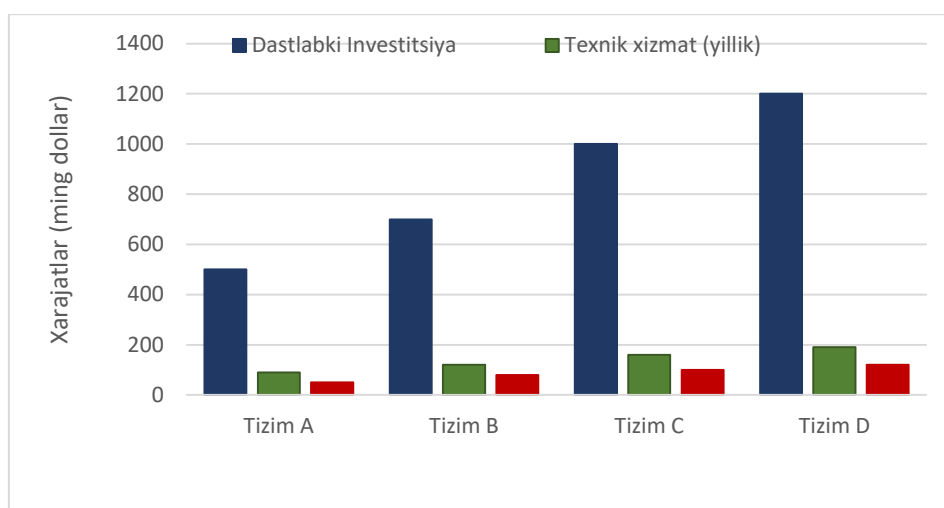
Turli avtomatlashtirilgan monitoring tizimlarining xarajatlari quyidagi jadvalda solishtiriladi:

1-jadval

Umumiy xarajatlar ishlatiladigan asosiy ko'rsatkichlar

Ko'rsatkich	Tushuntirish	Formula
Umumiy xarajatlar (TC)	Dastlabki investitsiya, texnik xizmat va yangilash	$TC=I+M+U$
Yillik xarajatlar (AC)	Umumiy xarajatlarning amortizatsiyasi	$AC = \frac{TC}{N}$

Turli avtomatlashtirilgan monitoring tizimlari uchun investitsiya, texnik xizmat va modernizatsiya xarajatlari taqqoslanadi, 1-rasmda avtomatlashtirilgan monitoring tizimlari uchun investitsiya, texnik xizmat va modernizatsiya xarajatlari taqqoslanadi. Dastlabki investitsiya tizimning boshlang'ich xarajatlari eng katta ulushni tashkil etib, texnik xizmat ko'rsatish yillik xizmat xarajatlari uzoq muddatda umumiy xarajatga ta'sir qiladi, modernizatsiya xarajatlari tizimni dolzarb saqlash uchun talab qilinadi va vaqt o'tishi bilan oshishi mumkin [2].



1-rasm. Avtomatlashtirilgan monitoring tizimlari xarajatlari

Avtomatlashtirilgan monitoring tizimlarining rivojlanishi bilan xavfsizlik masalalari tobora dolzarb bo'lib bormoqda. Ushbu tizimlar foydalanuvchi ma'lumotlarini yig'ib, saqlashi sababli xavfsizlik huquqlari buzilishi, shuningdek, tizimning o'zi kiberhujumlarga nishon bo'lishi mumkin. Avtomatlashtirilgan monitoring tizimlari foydalanuvchilarning toifalangan ma'lumotlarini kuzatishi va saqlashi mumkin, bu esa xavfsizlik huquqlari buzilishiga sabab bo'lishi ehtimoli yuqori. Shu bilan birga, tizimlarning o'zi ham kiberhujumlar uchun mo'ljall bo'lish xavfini oshiradi. Bunday muammolarni baholash uchun ma'lumotlarni himoya qilish darajasi (Data Security Index - DSI) va kiberhujum ta'sir darajasi (Cyber Attack Impact - CAI) ni hisoblash mumkin. Monitoring tizimlarining xavfsizlik darajasini baholash uchun quyidagi ko'rsatkichlar qo'llaniladi. [3] Ma'lumotlar xavfsizligi indeksi (DSI - Data Security Index) - ushbu indeks monitoring tizimining toifalangan ma'lumotlarni himoya qilish darajasini ko'rsatadi:

$$DSI = \frac{E}{D} \times 100\% \quad (3)$$

Bu yerda:

E - himoyalangan ma'lumotlar hajmi (GB)

D - umumiy qayta ishlanayotgan ma'lumotlar hajmi (GB)

Kiberhujumlar ta'sir darajasi (Cyber Attack Impact - CAI) – tizimga qarshi amalga oshirilgan muvaffaqiyatli hujumlar natijasida yuzaga keladigan yo'qotishlar quyidagicha ifodalanadi:

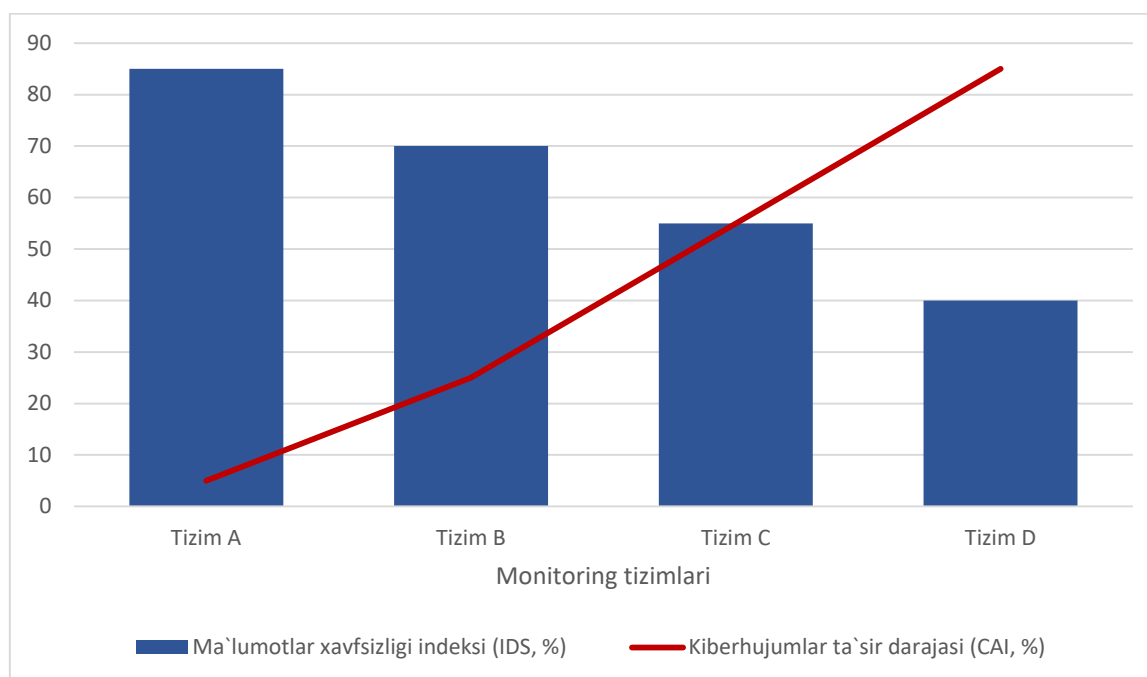
$$CAI = \frac{L}{A} \times 100\% \quad (4)$$

Bu yerda:

L – zarar ko'rgan ma'lumotlar hajmi

A – tizimda saqlanayotgan umumiy ma'lumotlar hajmi

Turli monitoring tizimlarida ma'lumotlar xavfsizligi indeksi (DSI) va kiberhujumlarning ta'sir darajasi (CAI) solishtiriladi (2-rasm).



2-rasm. Monitoring tizimlarida xavfsizlik darajalari

Yuqoridagi rasm turli monitoring tizimlarida ma'lumotlar xavfsizligi indeksi (DSI) va kiberhujumlarning ta'sir darajasi (CAI) ni solishtiradi. DSI (Ma'lumotlar xavfsizligi indeksi) yuqori bo'lsa - toifalangan ma'lumotlar yaxshi himoyalangan, past bo'lsa – tizim toifalangan ma'lumotlarni yetarli darajada himoya qila olmaydi. CAI (Kiberhujumlarning ta'sir darajasi) - yuqori bo'lsa, tizim ko'proq zarar ko'rgan va hujumlarga nisbatan zaif, past bo'lsa - tizim hujumlardan yaxshi himoyalangan.

Real vaqt masalalari monitoringi tezkor va ishonchli ma'lumotlarni qayta ishlash talab qiladi. Tizim samaradorligiga kechikishlar, tarmoqdagi trafik o'zgarishlari va hisoblash resurslarining yetarli emasligi jiddiy ta'sir ko'rsatishi mumkin [4]. Ushbu omillar tahdidlarni o'z vaqtida aniqlash imkoniyatini kamaytirib, xavfsizlik darajasini pasaytiradi. Monitoring tizimining real vaqt samaradorligini baholash uchun quyidagi ko'rsatkichlar ishlatiladi:

Kechikish (Latency - L) – real vaqt tizimlarida kechikish (tizimning javob berish vaqti) quyidagicha hisoblanadi:

$$L = \frac{P}{B} \quad (5)$$

Bu yerda:

P – Ishlov berilishi kerak bo‘lgan ma’lumotlar hajmi (MB)

B – Tizimning ishlov berish kengligi (MB/s)

Trafikning keskin o‘zgarishlari ta’siri (Traffic Variability Impact - TVI) - tarmoqdagi trafikning o‘zgarishi tizimga qanday ta’sir qilishini baholash uchun quyidagi formula ishlatiladi:

$$TVI = \frac{|T_{max} - T_{min}|}{T_{avg}} \times 100\% \quad (6)$$

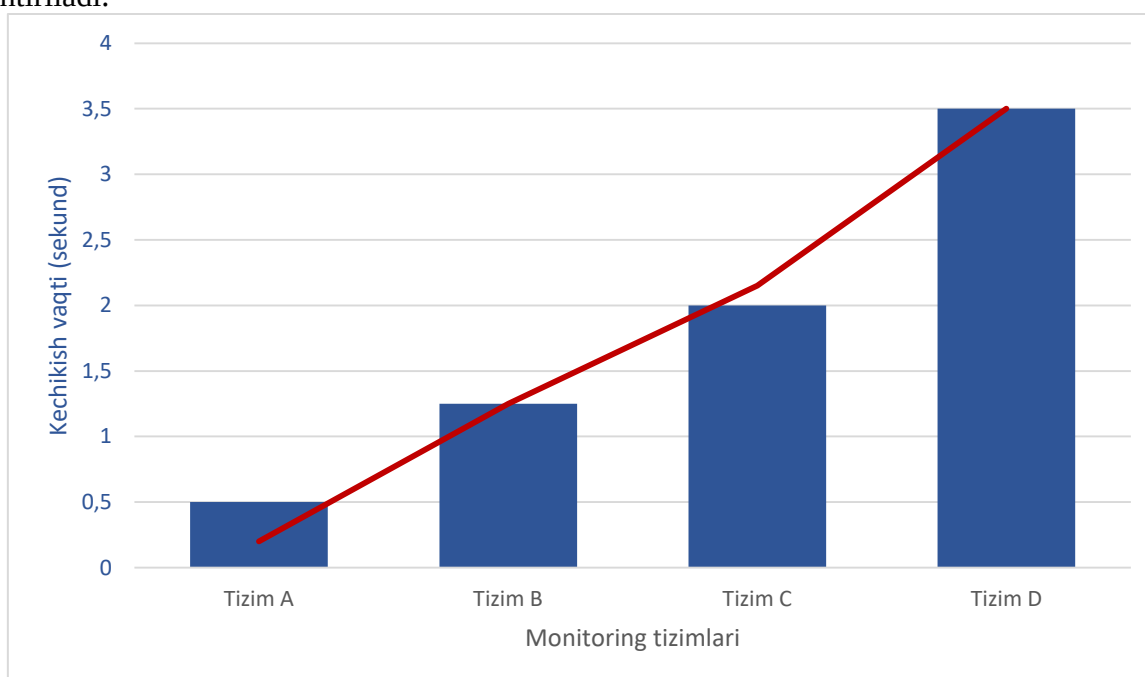
Bu yerda:

T_{max} -eng yuqori tarmoq trafik darajasi (MB/s)

T_{min} -eng past tarmoq trafik darajasi (MB/s)

T_{avg} -o‘rtacha tarmoq trafik darajasi (MB/s)

Turli monitoring tizimlarida kechikish darajasi va trafik o‘zgarishining tizimga ta’siri solishtiriladi.



3-rasm. Monitoring tizimlarida real vaqt masalalari

Yuqoridagi rasm turli monitoring tizimlari bo‘yicha kechikish vaqti (Latency - L) hamda trafik o‘zgarishining ta’siri (TVI) ni solishtiradi. Kechikish vaqti (L - Latency) – past qiymatlar tizim real vaqt monitoringi uchun mos va tezkor ishlaydi, yuqori qiymatlar – kechikish sababli tahdidlarni kech aniqlash xavfi ortadi. Trafik o‘zgarish ta’siri (TVI - Traffic Variability Impact) – yuqori qiymatlar tarmoq yuklamasi keskin o‘zgarishi natijasida tizim ishlashi barqaror emas, past qiymatlar – tizim yuklamaning o‘zgarishiga moslasha oladi.

Skalabellik - tarmoq monitoring tizimlarining shkalasini kengaytirish (scalability) ularning o‘sib borayotgan tarmoq hajmi va murakkabligiga moslasha olish qobiliyatiga bog‘liq. Katta miqyosli tarmoqlarni samarali kuzatish resurslarning yetarli emasligi, tarmoq yuklamasining oshishi va monitoring tizimlarining cheklavlari sababli qiyinlashadi. Monitoring tizimining skalabelligini baholash uchun monitoring samaradorligi indeksi (MEI - Monitoring Efficiency Index) ko‘rsatkichi ishlatiladi. Tizimning o‘sib borayotgan tarmoq hajmiga moslasha olish darajasi quyidagicha hisoblanadi:

$$MEI = \frac{R}{N} \quad (7)$$

Bu yerda:

R – monitoring tizimining ishlov bera oladigan maksimal resurslari (serverlar yoki hisoblash quvvati);

N – tarmoqdagi aktiv qurilmalar yoki ulanishlar soni;

Katta tarmoqlar uchun samaradorlik (LSE - Large Scale Efficiency) tizimning kengayishi bilan ishlash samaradorligi quyidagicha baholanadi:

$$LSE = \frac{P_{base}}{P_{scale}} \times 100\% \quad (8)$$

Bu yerda:

P_{base} - asosiy miqyosda tizimning ishlash samaradorligi.

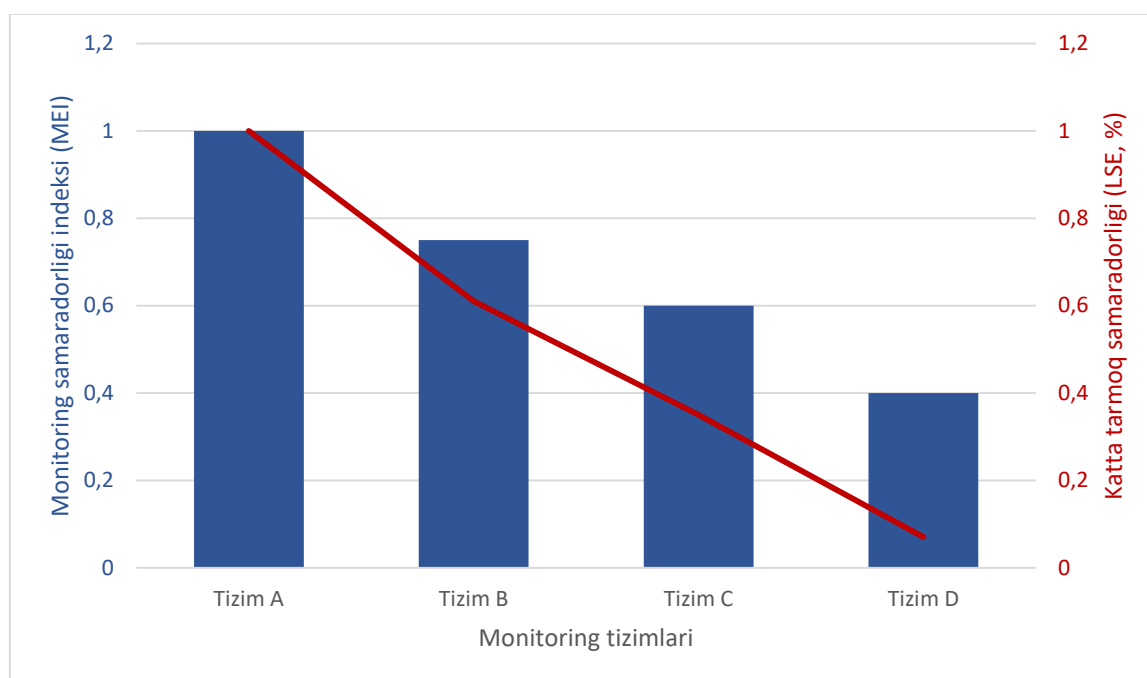
P_{scale} - katta miqyosda tizimning ishlash samaradorligi.

2-jadval

Kengaytirilgan tarmoqlarda samaradorligini baholash

Ko'rsatkich	Tushuntirish	Formula
Monitoring samaradorligi indeksi (MEI)	Tarmoq hajmi oshganda monitoring tizimi samaradorligi	$MEI = \frac{R}{N}$
Katta tarmoqlar samaradorligi (LSE)	Katta miqyosda tizim samaradorligi foizi	$LSE = \frac{P_{base}}{P_{scale}} \times 100\%$

Turli monitoring tizimlarining skalabellik ko'rsatkichlari, ya'ni monitoring samaradorligi (MEI) va katta tarmoqlar samaradorligi (LSE) solishtiriladi.



4-rasm. Monitoring tizimlarida skalabellik darajalari

Turli monitoring tizimlarining monitoring samaradorligi indeksi (MEI) va katta tarmoqlardagi samaradorligi (LSE) bo'yicha solishtiradi. MEI (monitoring samaradorligi indeksi) - yuqori qiymatlar tizim tarmoq hajmi ortishiga moslasha oladi, past qiymatlar – tizim ko'paygan yuklamaga bardosh bera olmaydi. LSE (katta tarmoq samaradorligi) - yuqori qiymatlar tizim katta tarmoqlarda ham samarali ishlay oladi, past qiymatlar – tizim miqyos kengayganda ishlash tezligi pasayadi [5].

Soxta signallar muammosi – avtomatlashtirilgan monitoring tizimlari ko‘pincha noto‘g‘ri ogohlantirishlar (false positives - *FP*) yoki haqiqiy tahdidlarni e‘tibordan chetda qoldirish (false negatives - *FN*) muammosiga duch keladi. Bu esa xavfsizlik operatorlarining e‘tiborini chalg‘itib, haqiqiy tahdidlarning aniqlanmay qolishiga sabab bo‘lishi mumkin. Monitoring tizimining soxta signallarni filtrlash samaradorligini baholash uchun quyidagi ko‘rsatkichlar ishlatiladi:

Aniqlik (Precision - *P*) - tizim tomonidan aniqlangan tahdidlarning nechta qismi haqiqiy ekanini ko‘rsatadi:

$$P = \frac{TP}{TP + FP} \times 100\% \quad (9)$$

Bu yerda:

TP – to‘g‘ri ijobiy natijalar (True Positives)

FP – soxta ijobiy natijalar (False Positives)

Ishonchlilik (False Positive Rate - *FPR*) - tizimda sodir bo‘ladigan soxta ijobiy natijalar ulushini ifodalanishi:

$$FPR = \frac{FP}{FP + TN} \times 100\% \quad (10)$$

Bu yerda:

TN – to‘g‘ri salbiy natijalar (true negatives)

Noaniqlik (False Negative Rate - *FNR*) - haqiqiy tahdidlarning noto‘g‘ri rad etilishi foizi:

$$FNR = \frac{FN}{FN + TP} \times 100\% \quad (11)$$

Bu yerda:

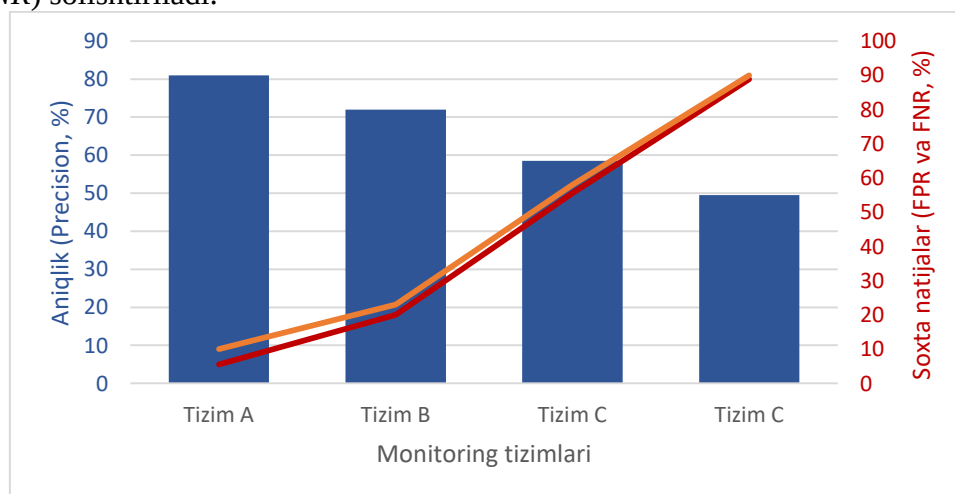
FN – soxta salbiy natijalar (false negatives)

3-jadval

Monitoring tizimlarining soxta signallar bilan ishlash samaradorligi

Ko‘rsatkich	Tushuntirish	Formula
Aniqlik (<i>P</i> - Precision)	Tizimning haqiqiy tahdidlarni aniqlash foizi	$P = \frac{TP}{TP + FP} \times 100\%$
Soxta ijobiy natijalar (<i>FPR</i>)	Tizimning noto‘g‘ri ijobiy signallar berish ehtimoli	$FPR = \frac{FP}{FP + TN} \times 100\%$
Soxta salbiy natijalar (<i>FNR</i>)	Haqiqiy tahdidlarni noto‘g‘ri rad etish ehtimoli	$FNR = \frac{FN}{FN + TP} \times 100\%$

Turli monitoring tizimlari uchun aniqlik (*P*), soxta ijobiy natijalar (*FPR*) va soxta salbiy natijalar (*FNR*) solishtiriladi.



5-rasm. Monitoring tizimlarida soxta signallar muammosi

Aniqlik (precision - P) - yuqori qiymatlar tizim haqiqiy tahdidlarni aniqlashda ishonchli, past qiymatlar – ko‘plab noto‘g‘ri tahdidlarni aniqlaydi va operatorlarning ishonchini pasaytiradi. Soxta ijobiy natijalar (FPR - False Positive Rate) - yuqori qiymatlar tizim ko‘plab noto‘g‘ri tahdidlarni qayd etadi, bu esa e‘tiborni chalg‘itadi, past qiymatlar – tizim faqat haqiqiy tahdidlarni aniqlaydi. Soxta salbiy natijalar (FNR - False Negative Rate) - yuqori qiymatlar – haqiqiy tahdidlar e‘tibordan chetda qoladi, past qiymatlar – tizim barcha tahdidlarni aniqlaydi [6].

Xulosa qilib aytganda tarmoq monitoringi tizimini avtomatlashtirish bugungi raqamli muhitda axborot xavfsizligini ta‘minlash va xizmat sifatini oshirishning muhim vositasidir. Tadqiqot natijalari shuni ko‘rsatadiki, bunday tizimlarni joriy qilish uchun dastlabki investitsiya xarajatlari asosan apparat va dasturiy ta‘minotni xarid qilish, o‘rnatish va sozlashga sarflanadi. Biroq, tizim samaradorligini saqlash va uni rivojlantirish uchun uzluksiz texnik xizmat ko‘rsatish hamda yangilash xarajatlari muntazam ravishda rejalashtirilishi lozim. Avtomatlashtirilgan monitoring tizimlari nafaqat real vaqt rejimida tahdidlarni aniqlash va bartaraf etishni ta‘minlaydi, balki ishchi kuchi va vaqt xarajatlarini kamaytirib, operatsion samaradorlikni oshiradi. Shu bilan birga, tizimlarning uzoq muddatli barqarorligi va zamonaviy talablarni qondirish qobiliyati muntazam texnik xizmat va yangilash ishlariga bevosita bog‘liqdir. Maqolada ta‘kidlanganidek, ushbu jarayonlarda xarajatlarni oqilona boshqarish va strategik rejalashtirish orqali maksimal iqtisodiy samaradorlikka erishish mumkin. Shunday qilib, tarmoq monitoringi tizimini avtomatlashtirish nafaqat dastlabki investitsiya, balki davomiy xizmat ko‘rsatish va doimiy modernizatsiya jarayonlarini ham qamrab oluvchi kompleks loyiha bo‘lib, u tashkilotlarning raqamli xavfsizlik va operatsion samaradorligini ta‘minlashda muhim ahamiyat kasb etadi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

- [1] Stallings, W. Network Security Essentials: Applications and Standards. Pearson Education, 2017.
- [2] Conti, M. Security and Privacy in Internet of Things (IoT): Models, Algorithms, and Implementations. Springer, 2021.
- [3] Rouse, M. What is network monitoring? SearchNetworking, TechTarget, 2022, 18–24-betlar.
- [4] Jo‘rayev M.T. “Tarmoq oqimini monitoring qilish dasturiy tizimi” // Index Copernicus, 2024, 1(7), 73–77-betlar. (Index Copernicus)
- [5] Begbo‘tayev A.E., Yusupov R.M. Tarmoq texnologiyalari (o‘quv qo‘llanma). Jizzax davlat pedagogika universiteti, 2021, 48–52-betlar. (Jizzax Pedagogika Universiteti)
- [6] Ro‘ziyev Y.Z., Abdullayeva B.S. Mediasavodxonlik va axborot madaniyati (darslik). Toshkent, 2024, 98–104-betlar (Renessans Ta‘lim Universiteti)
- [7] Xamrakov U.Sh., Risqaliyev J.D., Tashmanov Y.B. Ochiq ma‘lumotlarga asoslangan tadqiqotlar: O‘quv qo‘llanma. Ichki ishlar vazirligi Malaka oshirish instituti, 2024, 76–79-betlar (ИПКМВД)
- [8] “Axborot xavfsizligining siyosati” // Nauchniy impuls, maqola, 2024, 68–73-betlar (Научный Импульс)
- [9] Alsmadi, I., Xu, D. Security of Internet of Things: Perspectives and Challenges. Springer, 2021.
- [10] Scarfone, K., Mell, P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94, 2021 edition.
- [11] Zhou, W., Zhang, Y. Network Intrusion Detection: Machine Learning Approaches. CRC Press, 2022.
- [12] Garuba, M., Liu, Y. Cybersecurity Monitoring and Threat Detection. Elsevier, 2023.

HARAKATLANUVCHI DRON TIZIMLARIDA BOSHQARUV SIGNALLARINI UZATISHNING MAVJUD YECHIMLARI

Sh.O'. SINDAROV, A.X. FAYZULLAYEV

O'R MV Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti

Annotatsiya. Ushbu maqolada harbiy maqsadlarda qo'llaniluvchi uchuvchisiz uchish apparatlari (UUA) uchun qo'llanilayotgan zamonaviy aloqa arxitekturalari, ya'ni radiochastotali aloqa, mobil aloqa (4G/5G), sun'iy yo'ldoshli aloqa tizimlari (SATCOM) va ularning kombinatsiyasiga asoslangan gibril tizimlar texnik va funksional jihatdan batafsil tahlil qilinib, mazkur tizimlarning kechikish, tarmoqli kenglik, qamrov, rezilyentlik va energiya sarfi kabi parametrlar bo'yicha ko'p mezonli qiyosiy tahlili taqdim etiladi. Shuningdek, maqolada dasturiy ta'minotli radio (SDR), FANET va kognitiv radio kabi ilg'or yondashuvlar asosida interferensiyaga bardoshli, yuqori ishonchlilikka ega real vaqtli boshqaruv aloqalarini tashkil etish imkoniyatlari yoritiladi.

Kalit so'zlar: uchuvchisiz uchish apparatlari (UUA), radiochastotali aloqa, mobil tarmoqlar (4G/5G), sun'iy yo'ldoshli aloqa tizimlari (SATCOM), gibril aloqa arxitekturalari, dasturiy ta'minotli radio (SDR), FANET, kognitiv radio, interferensiyaga bardoshlilik, real vaqtli boshqaruv, C2 tizimi, spektrni dinamik boshqarish, DSSS, FHSS, FSO texnologiyasi.

Abstract. This article presents a comprehensive technical and functional analysis of modern communication architectures employed in military unmanned aerial vehicles (UAVs), including radio frequency (RF) systems, mobile networks (4G/5G), satellite communication systems (SATCOM), and hybrid architectures based on their integration. The study provides a multi-criteria comparative assessment of these systems with respect to parameters such as latency, bandwidth, coverage, resilience, and power consumption. Furthermore, the article explores the potential of advanced approaches such as software-defined radio (SDR), flying ad-hoc networks (FANET), and cognitive radio for establishing real-time, interference-resilient, and highly reliable control communication links.

Key words: unmanned aerial vehicles (UAVs), radio frequency communication, mobile networks (4G/5G), satellite communication systems (SATCOM), hybrid communication architectures, software-defined radio (SDR), FANET, cognitive radio, interference resilience, real-time control, C2 systems, dynamic spectrum management, DSSS, FHSS, FSO technology.

Radiochastota spektroskopik diapazonidagi o'ta qisqa to'lqinlar (ing. VHF – 30–300 MHz) hamda ultra qisqa to'lqinlar (ing. UHF – 300–3000 MHz) diapazonlari uchuvchisiz uchish apparatlari (UUA) boshqaruvi tizimlarida keng qo'llaniladi, chunki ushbu chastotalarning so'nish koeffitsienti past, atmosferaning difraktsiya va refraktsiya xususiyatlari evaziga ushbu diapazondagi signallarning tabiiy to'siqlardan samarali o'tishini ta'minlanadi[1]. An'anaviy analog chastota modulyatsiyali tizimlar spektral zichlik nuqtai nazaridan cheklangan bo'lsa-da, yuqori interferensiyaga chidamliligi sababli harbiy operatsiyalarda keng tatbiq etiladi. Shuningdek, ko'p tashuvchili OFDM yoki fazali QPSK modulyatsiyasini joriy etish orqali ma'lumot uzatish tezligi 5 Mb/s dan 10 Mb/s gacha ko'tariladi va shovqinbardosh kodlash mexanizmlari ko'p kirishli ta'sir effekti (ing. multipath effect) va shovqinli muhit sharoitida ham signal sifatini yuqori darajada saqlashga xizmat qiladi.

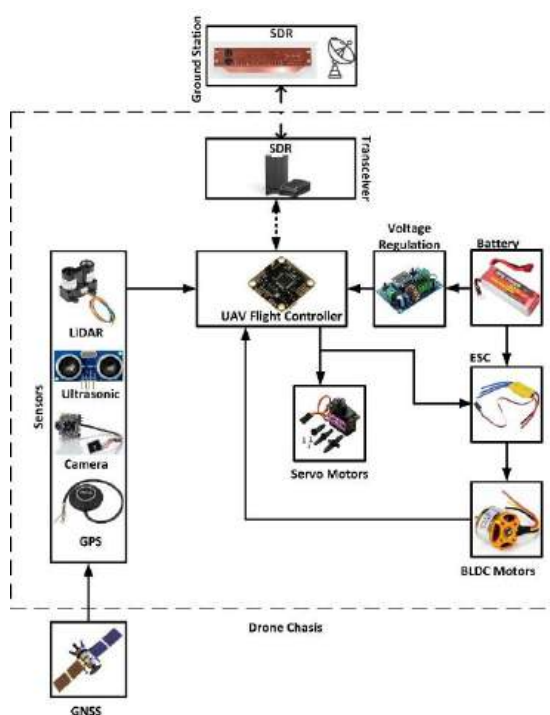
Zamonaviy radiochastotali aloqa tizimlarida dasturiy ta'minotli radio (ing. software-defined radio – SDR) yondashuvi dominant rol o'ynaydi, chunki u chastota diapazonini, modulatsiya turini va hatto filtrlash xususiyatlarini dasturiy ta'minot orqali parvoz jarayonida o'zgartirishga, shuningdek, real vaqtda interferensiya monitoringi va dinamik spektr boshqaruvi algoritmlarini qo'llashga imkon beradi (1-rasm). Bunday arxitektura radioelektron bosim holatlarida chastota almashtirish, DSSS (ing. direct-sequence spread spectrum – to'g'ridan-to'g'ri ketma-ket yoyilgan

spektr) va FHSS (ing. frequency-hopping spread spectrum – sakratuvchi chastotali yoyilgan spektr) kabi tashqi hujum mexanizmlariga qarshi samarali kurashish vositalarini taqdim etadi [2]. Shu tariqa ma'lumot paketlarini uzatish zanjiri bir martalik kanalga emas, balki bir nechta mustaqil radiochastotali aloqa yo'nalishlariga parallel ravishda tarqatishi orqali bir yo'nalishdagi nosozlik butun tizim ishiga ta'sir ko'rsatmaydi.



1-rasm. Gospel GR-227 SDR qurilmasi

Zamonaviy uchuvchisiz uchish apparatlari boshqaruvida radiochastota spektridan maksimal darajada samarali foydalanishni ta'minlash maqsadida SDR texnologiyalari qo'llanilmoqda, bunda protsessorlar yordamida chastota diapazonini, modulyatsiya turini hamda filtrlash parametrlarini real vaqt rejimida moslashtirish mumkin bo'lib, bu esa nafaqat dushmanning radioelektron bosim berishi va sun'iy interferensiya holatlarida kanalni avtomatik ravishda aniq past quvvatli yo'nalishga o'tkazish, balki spektrda bo'sh joylarni aniqlab, dinamik spektr shakllantirish algoritmlari orqali uzluksiz buyruq va boshqaruv signallarini tarqatish imkonini beradi. Bu yondashuv tufayli nafaqat analog chastotali tizimlarning chidamliligi, balki raqamli OFDM protokollarning yuqori ma'lumot uzatish tezligi ham ta'minlanadi. 2-rasmda UUA'larga SDR qurilmasini o'rnatish arxitekturasini keltirilgan.



2-rasm. UUAga o'rnatilgan SDR arxitekturasini

Bundan tashqari, harbiy va tijorat SDR qurilmalari sifatida AN/PRC-163 portativ radio terminali hamda USRP N310 qurilmasi ancha keng qo'llanilmoqda. Ushbu qurilmalar bir vaqtning o'zida VHF/UHF diapazonlarida ishlay olishi, 4G/5G tarmoqlariga ulanib, hatto LTE TDD va FDD formatlarini ham qo'llab-quvvatlashi tufayli dronlar buyruq va boshqaruv signallari (ing. Command and control – C2), telemetriya signallari va yuqori aniqlikdagi video oqimini yagona apparat platformasida uzatishni amalga oshiradi [3].

Radiochastotali aloqa arxitekturasining yana bir muhim qismiga FANET (ing. Flying Ad Hoc Network – Uchuvchi o'z-o'zini tashkil qiluvchi tarmoq) tarmog'i kiradi. Bu yondashuvda har bir UUA nafaqat yakka boshqaruv nuqtasi, balki marshrut uzatuvchi uzal sifatida ishlaydi. Bunda paketlar uzatilishida real vaqtda marshrutni qayta hisoblash va yo'nalishlarni o'zgartirish imkoniyati mavjud bo'lib, shuningdek, dronlar o'rtasida o'zini-o'zi tiklay oluvchi aloqa mexanizmi tashkil etiladi. Shu bilan masofa yoki to'siq tufayli markaziy stansiya bilan to'g'ridan-to'g'ri bog'lanish uzilganda ham butun tarmoqning uzluksiz ishlashini ta'minlaydi [4]. Bu texnologiya ayniqsa keng maydonli, ko'p nuqtali razvedka va izlov-qutqaruv missiyalarida samarador bo'lib, dron floti orqali mintaqaning real vaqtli xaritasini tuzish hamda xavfli zonalarini markaziy stansiyaga uzluksiz yetkazib berish imkonini beradi. Shuningdek, dron floti ichida o'z-o'ziga bog'liq FANET (Flying Ad Hoc Network) tarmog'i har bir individual UUAning nafaqat qabul qiluvchi, balki paketni keyingi tugunga uzatuvchi oraliq uzal sifatida ishlashini ta'minlaydi, bu uslub bir tomondan butun tarmoqning uzilishlarga qarshi chidamliligini oshirsa, ikkinchi tomondan kuzatuv va razvedka paytida dronlar o'rtasidagi kuzatuv hududining to'liq qamrovini kafolatlaydi. FANETda ishlatiladigan OLSR (ing. Optimized Link State Routing – optimallashtirilgan bog'lanish holati asosidagi marshrutlash) va AODV (ing. Ad hoc On-Demand Distance Vector – talabga asoslangan masofa vektorli marshrutlash) kabi marshrutlash algoritmlari harakatlanuvchi tugunlarning geolokatsiyasiga mos ravishda dinamik ravishda eng qisqa va ishonchli yo'nalishni qayta hisoblab, tarmoqning real-vaqt ishlashini saqlab qoladi.

Mobil tarmoqlar (3G/4G/5G) va UUAda qo'llanilishi

3G, 4G va 5G mobil tarmoqlari ilk bor tijorat sohasida ko'p ma'lumotli multimedia xizmatlarini ta'minlash maqsadida joriy etilgan bo'lsa-da, kundalik hayotda talab ortib borishi natijasida harbiy va maxsus operatsiyalar uchun ham yetarli darajada ishonchlilik, past kechikish (<20 ms) va katta o'tish tezligi (bir necha yuz megabitlardan gigabit darajasigacha) bilan ajralib turadi; mazkur tarmoqlarning yuqori tarmoqli kengliklari orqali dronlarda real vaqtda telemetriya signallarini, yuqori aniqlikdagi kadrlardan tashkil topgan video oqimini, shuningdek, qisqa buyruq-javob signallarini uzatish imkoniyati paydo bo'ldi [5].

4G LTE (ing. Long Term Evolution – uzoq muddatli rivojlanish) texnologiyasining keyingi rivojlangan varianti bo'lgan LTE Advanced (LTE-A) tarmog'i mobil operator infratuzilmasi yordamida 100 Mbps gacha uzatish tezligini, 30–50 ms kechikishni va katta foydalanuvchi zichligida ham barqaror tarmoq ishini kafolatlaydi. Mazkur texnologiya asosida ishlovchi DJI Matrice 210 va Parrot Disco Bepop dronlari tijorat tarmoqlari orqali boshqaruvni qo'llab-quvvatlash maqsadida moslashtirilgan. Ular LTE-A modemlar bilan jihozlanib, masofadan turib 7–10 km oralig'ida kam kechikish orqali yuqori rasm sifati va telemetriya signallari almashinuvini ta'minlaydi.

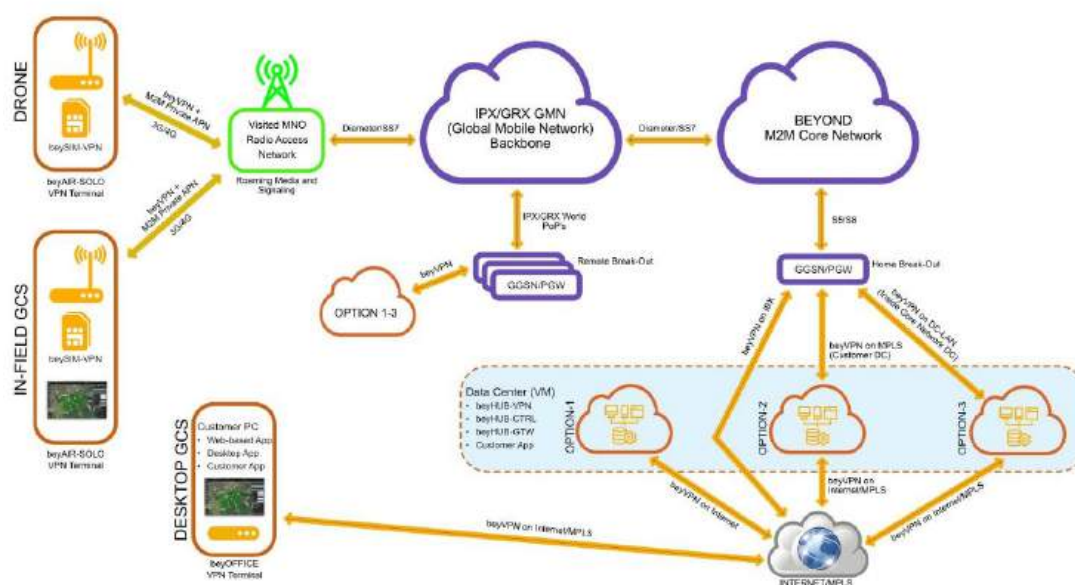
Biroq, 4G LTE tarmog'idagi kechikish va tarmoqqa bog'liqlik muammolarini bartaraf etish maqsadida ishlab chiqilgan 5G texnologiyasi kechikishni 1–5 ms gacha kamaytirishi, O'QT diapazonidagi yuqori chastota kanallari esa 1 Gbps dan yuqori o'tish tezligiga erishishi natijasida dronlar bilan uzluksiz C2 va HD/4K video uzatish rejimini barqaror ravishda qo'llash imkonini berdi. Masalan, Singapur mudofaa departamenti 2022-yilda miniatyura 5G bazasini mobil dron stansiyalariga joylashtirib, Matrice 600 Pro dronlari bilan 3 km radiusda uchuvchi dronlar asosida 4K video oqimini uzatishga erishdi [6].

Aniqlik va uzluksiz boshqaruvni ta'minlash maqsadida 4G LTE va 5G tarmoqlari dronlarda nafaqat telemetriya va video uzatish, balki bevosita C2 kanali sifatida ham keng yoyilishiga erishdi.

Misol uchun, 2018-yilda Verizon kompaniyasi tomonidan AQShda o'tkazilgan sinovlarda DJI Matrice 210 Pro droni ichiga o'rnatilgan LTE modem yordamida operatsion radius 8 km gacha yetkazildi va 30 fps tezlikda HD video oqimi yasaldi, bunda tarmoqqa ulanadigan yakka SIM-kartalar 4G LTE tarmoq kengligidan uzluksiz foydalanishga qodir ekanligi isbotlandi.

Shuningdek, 2021-yilda SK Telecom kompaniyasi tomonidan Janggang hududida tashkil etilgan tajribalarda Ericsson 5G standarti asosida Mosquito dronlari sinovdan o'tkazilib, 3 ms dan kam kechikish bilan real vaqtda C2 signallari uzatilgani, bu esa an'anaviy radiochastotali aloqa va LTE muammolari bo'lgan radioelektron bosimlarga qarshi yuqori chidamlilik ko'rsatdi.

Bundan tashqari, Parrot Anafi dronlari Fransiya va Germaniyada 2019–2020 yillarda olib borilgan MCX (Mission-Critical eXtended) loyihalarida 4G LTE modemlar bilan jihozlanib, NATO standarti bo'yicha sinovdan o'tkazilgan holda 15 kmgacha radiusda xavfsiz C2 aloqasini saqlab qola oldi, shu bilan birga, dron yonidagi mobil bazalarda joylashgan serverlarga rudimentar AI model qayta yuklanib, obyekt aniqlash va yo'nalish tuzishda operatorga kechikish minimal darajada bo'lishi ta'minlandi. 3-rasmda UUALar uchun 3G/4G LTE tarmoqlarni tashkil etish arxitekturasini aks etgan.



3-rasm. UUALar uchun 3G/4G LTE tarmoqlarni tashkil etish arxitekturasini

2022-yilda Rolls-Royce va Nokia hamkorligida tashkil etilgan “5G Connected Sky” loyihasida Airbus Aibot dronlari 5G NSA (non-standalone) rejimida yuqori yuklanishli L2–L4 turidagi ma'lumotlarni kamroq kechikish bilan uzatib, kelajakda shahar razvedkasi va belgilangan yo'nalish monitoringi uchun standart C2 infratuzilmasini namoyish etdi [7].

Sun'iy yo'ldosh aloqa (SATCOM)

Sun'iy yo'ldosh aloqa (SATCOM) tizimlari UUALar boshqaruvi sohasida global miqyosda past to'siq ta'sirisiz ma'lumot almashinuvini tashkil etish imkonini beruvchi asosiy vosita bo'lib, bu texnologiya yer stansiyasi va dron o'rtasida GEO (geostatsionar), MEO (o'rta yer orbitasi) hamda LEO (quyi yer orbitasi) turidagi sun'iy yo'ldoshlar yordamida uzluksiz butunjahon qamrovini ta'minlaydi, bunda geostatsionar orbitadagi platformalar dronlarga 35 786 km balandlikdan barqaror va doimiy pozitsiyada osilib turuvchi statik aloqani, LEO tizimlari esa past kechikish (50–100 ms) hamda tezkor orbital o'zgarishlar orqali yuqori qamrov zichligini, MEO esa bu ikki xususiyatning o'rtacha balansini ta'minlaydi [8].

GEO-sun'iy yo'ldoshlar bilan bog'lanishda signallar arktik, tropik hamda cho'l hududlardagi relyef va ob-havoga qaramasdan yetkaziladi, chunki signal uzatilish uchun kerakli balandlikdagi antennalar va transponderlar elektr energiyasi sarfini inobatga olgan holda katta quvvat bilan

ishlashiga to'g'ri keladi, shuning uchun GEO terminallarining quvvati 20–100 Vt gacha yetib, antenna diametri esa 0,6–1,2 m oralig'ida loyihalanadi, bu esa parvoz paytida va yer stansiyasida alohida logistika va energiya manbalarini talab etadi.

Boshqa tomondan, LEO tizimlarida signallar 500–1500 km balandlikda aylanishi natijasida kechikish ancha kamroq bo'ladi, ammo orbital tezlikning yuqoriligi fonida sun'iy yo'ldoshning o'z pozitsiyasini tez-tez o'zgartirib, dron bilan o'zaro aloqani uzluksiz saqlash uchun yaw-va yawratish mexanizmlarini qo'llash va ground-tracking antennalarini uzluksiz kuzatib turish zaruriyati paydo bo'ladi; shuningdek, LEO tizimlari ko'p elementli konstellatsiyalarni talab qilib, ularning boshqaruv va resurslar tarmoqlarini yaratishda ham murakkab texnik va iqtisodiy omillarni yuzaga keltiradi.

Shu bilan birga, SATCOM terminalarining zaruriy tarkibiy qismlaridan biri bu shifrlash va autentifikatsiya modullari bo'lib, odatda Type 1 klassidagi kriptografik apparat-dasturiy vositalar (AES-256, ECC-RSA) orqali jo'natilayotgan C2 komandalarining maxfiyligi va yaxlitligi kafolatlanadi, bu esa harbiy standartlarga muvofiq bo'lib, masalan, ARC-210 terminali "o'ta maxfiy" darajasiga muvofiq shifrlashni amalga oshiradi va normal holatda 10⁻⁹ darajasida bit xatoligi ko'rsatkichini (ing. bit error rate – BER) saqlab turadi.

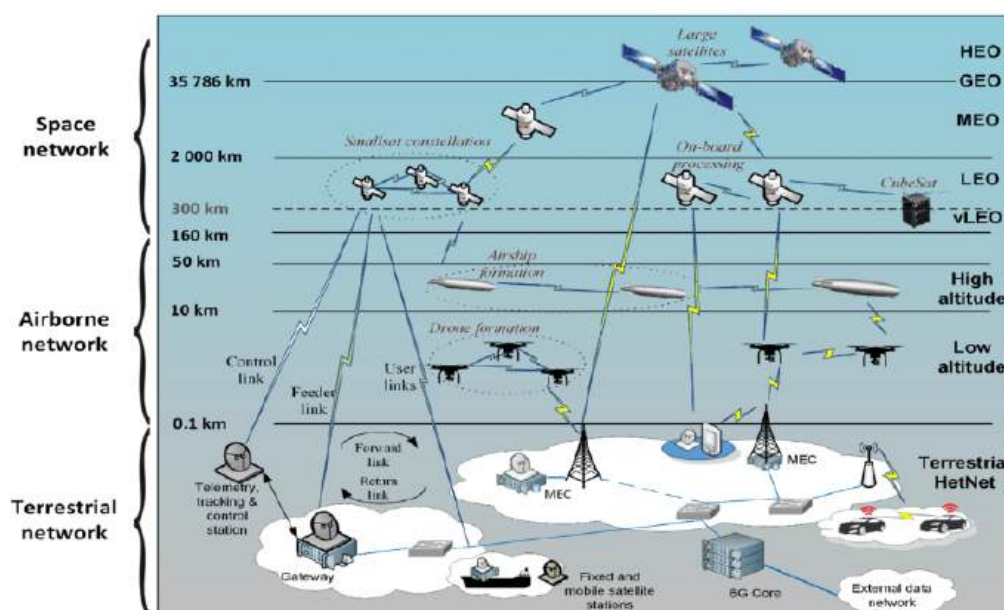
Demak, SATCOM asosida tashkil etilgan C2 arxitekturasida dronlarni masofadan boshqarishda beqiyos afzalliklar taqdim etadi, biroq quvvat talablari, terminal hajmi va murakkab orbitani kuzatish infrastrukturasi xarajatlari tufayli kichik, yengil va past quvvatli UUA platformalarida ba'zan zaxira sifatida yanada ixcham radiochastotali aloqa yoki mobil tarmoqlarga tayanish pragmatik yechim bo'lib qolaveradi.

GEO va LEO sun'iy yo'ldosh tizimlari orqali global darajadagi BLOS (Beyond-Line-Of-Sight) aloqani ta'minlash jarayonida UUA'larga o'rnatilgan SATCOM terminalarining monolitik apparat-dasturiy kompleksi muhim rol o'ynaydi, masalan AQSh Harbiy Havo Kuchlarining

"RQ-4 Global Hawk" dronida ishlatiladigan AN/USC-61 multimodal SATCOM terminali

1,2–1,4 GHz L-band va 7,9–8,4 GHz C-band chastotalarida uzluksiz ishlovchi qabul qilish bloklari bilan ta'minlangan bo'lib, u o'z ichida telemetriya signallari, real vaqti video oqimlari va

AES-256 algoritmi orqali amalga oshiriladigan C2 paketlarini qayta ishlash imkonini bir vaqtning o'zida yuklaydi; ushbu yondashuv "Global Hawk"ning 15 000 km masofada 30 soatdan ortiq davom etuvchi uzoq muddatli razvedka missiyalarida uzluksiz aloqani saqlashni kafolatlaydi. 4-rasmda GEO, MEO, LEO orbitalar va dron aloqasini ta'minlash arxitekturasini aks etgan.



4-rasm. GEO, MEO, LEO orbitalar va dron aloqasini ta'minlash arxitekturasini

Shu bilan birga, tijorat kosmik kommunikatsiya xizmati provayderi OneWeb kompaniyasining LEO konstellatsiyasi 2021-yilgi sinovlarda DJI Matrice 600 Pro dronlari bilan integratsiyalashgan bo'lib, u LEO orbitalari orqali 50–100 ms oralig'ida kechikish bilan 10 Mbps doirasida barqaror SIP-boshqaruvli C2 va video qabul qilish tizimini namoyish etdi. Bu tajribada dronlarga o'rnatilgan kuzatuv antennalari yordamida OneWeb kompaniyasining 650 ta sun'iy yo'ldoshidan biri bilan real vaqtli signal almashish amalga oshirildi, natijada radiochastotali aloqa va 4G tarmoqlarga nisbatan 50% ga kam kechikish bilan yuqori o'tkazuvchanlikka erishildi [9].

Gibrid aloqa arxitekturalari. Zamonaviy UUALar boshqaruvida radiochastotali aloqa tizimlari past kechikish va ob-havo sharoitidagi barqarorlik xususiyatlari bilan bir qatorda sun'iy yo'ldosh (SATCOM) kanallarining global BLOS imkoniyatlarini ham birlashtiruvchi gibrid arxitekturalar bugungi kunda strategik va taktik operatsiyalarning muqobil hamda ishonchli C2 yechimi sifatida keng qo'llanilmoqda. Mazkur yondashuvlar doirasida asosiy kanal sifatida tezkor radiochastotali aloqa yo'nalishlari ishlatilishi, agarda radiochastotali aloqa signallari radioelektron bosim, interferensiya yoki boshqa to'siqlarga duchor bo'lsa, uzluksiz aloqani saqlash maqsadida SATCOM yo'nalishlariga avtomatik ravishda qayta aloqa amalga oshiriladi, bu esa tizimning kechikish darajasini 10 ms dan 300 ms gacha bo'lgan diapazonda saqlagan holda yuqori o'tkazuvchanlikni ta'minlaydi.

Shu bilan birga, ochiq havoda optik aloqa (ing. Free-Space Optics – FSO) texnologiyasi yuqori chastotali lazerli to'lqinlar yordamida gigabit tezlikda ma'lumot uzatish imkonini beruvchi, elektromagnit to'lqin interferensiyasidan deyarli tozalangan, ammo ob-havo omillariga (tuman, yog'ingarchilik) sezgir texnologiya ham radiochastotali aloqa va SATCOM yo'nalishlari bilan to'liq integratsiyalashgan texnologiya sifatida namoyon bo'lmoqda. Bu texnologiyadan foydalanuvchi UUALarga misol qilib LaserKom va RFModex kompaniyasini UUALarini keltirish mumkin. Ularning korporativ yechimlarida FSO texnologiyasi asosidagi asosiy kanalga ob-havo xatarlari aniqlandi deguncha "RF-fallback" (radiochastotali aloqa asosida qayta aloqa) mexanizmi faollashadi hamda aloqaning barqarorligini saqlab qoladi. Bu kabi ikki qavatli (optik+radiochastotali aloqa) arxitekturalar 1–10 Gbps ma'lumot uzatish tezligi va UUALar uchun aloqa mavjudligini kafolatlab, zamonaviy strategik missiyalarning eng yuqori talablari uchun mo'ljallangan.

Gibrid aloqa arxitekturalarida kognitiv radio yondashuvi ham keng qo'llanilmoqda. Ushbu texnologiyada dastlab spektrni real vaqt rejimida tahlil qilinadi, spektrda tashqi radiochastotali aloqa uchun radioelektron bosimlar yoki tabiiy interferensiya ta'sirini aniqlanadi hamda radiochastotali aloqa, FSO yoki SATCOM kanallaridan mosini avtomatik tanlashni ta'minlaydi. Bunday tizimlarda dron bortidagi SDR bloklari millisekund darajasida kanal sifatini baholaydi va yangi yo'nalishni ishga tushirish uchun minimal kechikish (0,5–2 ms) bilan qayta aloqa mexanizmini ishga soladi [10].

Ikkinchi turdagi gibrid yondashuv – "multi-hop relay" (ing. ko'p sakrashli rele) konsepsiyasi bo'lib, unda yer usti yoki havo vositalarida joylashgan bir nechta uzal dronlar o'rtasida paketlarni navbatma-navbat uzatadi, bu esa uzoq masofalarda ham uzluksiz aloqani saqlash imkonini beradi. DARPA Phoenix dasturida sinovdan o'tgan Gremlins dronlarida RF-FSO kombinatsiyali dronlar tarmog'i tashkil etilib, LEO SATCOM texnologiyasi yordamida yer stansiyasiga yetkazish orqali butun tarmoqning 300+ km masofada uzluksiz C2 va telemetriya signallari almashinuvini amalga oshirish imkoniyatlari namoyish etildi.

Uchinchi yondashuv – stratosferik platformalar (HAPS) va statik antennalar bilan bir qatorda radiochastotali aloqa-FSO releni birlashtirish bo'lib, bu arxitektura dronlar lazer nurlarini stratosferik platformalarga uzatadi va u yerdagi multimodal terminallar radiochastotali aloqa yoki SATCOM yo'nalishlariga paketlarni uzatadi [11]. Airbus Zephyr platformasi misolida o'tkazilgan 2022-yilgi demo-sinovlar, dron-HAPS-yer stansiyasi zanjirini 20–30 ms kechikish bilan saqlagan holda 1 Gbps tezlikda ma'lumot uzatishni ta'minlaganini ko'rsatdi.

Integrallashgan sezish va aloqa tizimi (ing. Integrated Sensing and Communication – ISAC) konsepsiyasi ham gibril arxitekturalarga yangi imkoniyatlar qo'shadi, chunki radiochastotali aloqa qurilmalari radiolokatsiya va FSO LIDAR singari sensorlarni bitta spektr orqali boshqarish, dronning joylashuvi va kanallar holatini bir vaqtning o'zida aniqlashni amalga oshiradi. Bunday yechim 2024-yildagi ISAC droni prototipida 20 sm pozitsion aniqlikda radiochastotali aloqa+LIDAR algoritmlarini tatbiq etish orqali ham harbiy, ham fuqarolik missiyalarida spektr samaradorligini 40 % ga oshirdi[12].

Uchuvchisiz uchish apparatlarida (UUA) qo'llaniladigan radiochastotali aloqa, mobil, SATCOM va gibril aloqa usullarini qiyosiy tahlil qilish, ularning tizim talablari, muhit sharoitlari va operatsion masalalarni hal etishdagi samaradorligini taqqoslash imkonini beradi. Bunday tahlil dronning aniqlik, uzluksizlik, kechikish, qamrov, energetik xarajat va iqtisodiy samaradorlik kabi bir nechta mezonlar asosida optimal C2 (Command & Control) yechimlarini tanlash uchun muhimdir.

Solishtirish mezonlari

- Kechikish (Latency): buyruq yuborishdan qabulgacha bo'lgan vaqt, millisekundlarda.
- Ma'lumot uzatish imkoniyati (Bandwidth): Mbps yoki Gbps.
- Qamrov (Coverage): operatsion radius yoki global qamrov.
- Rezilyentlik (Resilience): radioelektron bosim, interferensiya va ob-havo sharoitlariga chidamlilik darajasi.
- Murakkablik (Complexity): apparat va dasturiy infratuzilma darajasi.
- Energetik sarf (Power Consumption): quvvat sarfi.
- Tashkiliy va logistik xarajat (Cost): bir terminalning o'rnatish va ekspluatatsiya qiymati.

Quyidagi 1-jadvalda harakatlanuvchi dron tizimlarida boshqaruv signallarini uzatishning mavjud yechimlari qiyosiy tahlil qilingan.

1-jadval.

UUA tizimlarida boshqaruv signallarini uzatish usullarining qiyosiy tahlili

Usul	Kechikish	Tezlik	Qamrov	Rezilyentlik	Murakkablik	Energiya sarfi	Xarajat
Radiochastotali aloqa (UHF/VHF)	5–15 ms	1–10 Mbps	LOS: 20–50 km	O'rta (FHSS/DSSS orqali sezilarli)	Past–o'rta	Past	Past
Mobil (4G/5G)	1–50 ms	100 Mbps–1 Gbps	Operator qamrovi ichida; chekka hudud: kam	O'rta–Yuqori (URLLC, MEC)	O'rta–yuqori	O'rta	O'rta–Yuqori
SATCOM	GEO: 250–300 ms; LEO: 50–100 ms	10–100 Mbps	Global (BLOS)	Yuqori (global, REBga bardoshli)	Yuqori	Yuqori	Yuqori
Gibril	5 ms–300 ms	1 Mbps–1 Gbps	Global + lokal	Eng yuqori	Eng yuqori	O'rta–yuqori	Eng yuqori

Yuqoridagi taqqoslashdan ko'rinib turibdiki, radiochastotali aloqa eng past kechikish va quvvat sarfi bilan birga ob-havo to'siqlarga chidamliligi ham yetarlicha yuqori bo'lsa-da, qamrov va ma'lumot uzatish tezligi jihatidan cheklovlarga duch keladi. Mobil tarmoqlar (4G/5G) esa yuqori o'tkazish tezligi va past kechikish imkoniyatini taqdim etsa-da, tarmoq qamrovi va xavfsizlikdagi potensial zaifliklar tufayli operatsion maydon tanlovi bilan cheklanadi. SATCOM global qamrov va

yuqori rezilyentlikni kafolatlaydi, lekin yuqori kechikish va energetik hamda moliyaviy xarajatlarni talab qiladi. Nihoyat, gibridd arxitekturalar barcha yuqoridagi usullarning afzalliklarini dinamik tarzda birlashtirib, maksimal uzluksizlik, moslashuvchanlik va xavfsizlikni ta'minlaydi, biroq shu bilan birga murakkab apparat va dasturiy infratuzilmaga bo'lgan ehtiyoj ham sezilarli darajada ortadi. UUALarning C2 tizimini loyihalashda ushbu mezonlar va ularning vazifaga mosligi jiddiy e'tiborga olinishi lozim.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

- [1] Johnson D., Smith P. Advanced RF Communication for Unmanned Aerial Vehicles. Journal of Aerospace Communication. 2021;12(3):45–62.
- [2] Lee R., Thompson M. Adaptive Spread Spectrum Techniques in Tactical SDRs. IEEE Trans. Mil. Commun. 2022;58(7):1124–1135.
- [3] Ettus Research. USRP N310 User Manual. Ithaca: Ettus Research; 2022.
- [4] Perkins C., Royer E. Ad-Hoc On-Demand Distance Vector Routing. Proc. IEEE WMCSA. 1999;234–244.
- [5] Smith J., Carter L. Evolution of Cellular Networks for Unmanned Aerial Vehicle Control. Int. J. Commun. Sys. 2021;34(4):e4567.
- [6] Ministry of Defence Singapore. “5G-Enabled UAV Trials Report.” 2022
- [7] SK Telecom. “5G Low-Latency UAV Control Demonstration,” Technical Report, 2021.
- [8] Marine Corps Warfighting Publication (MCWP) 3-16.1 «Satellite Communications», HQ USMC, Washington, DC; 2016.
- [9] OneWeb. “LEO Constellation UAV Trial Report.” London; 2021.
- [10] Wang L., Li Z. Cognitive Radio and Dynamic Spectrum Access in UAV Networks. Sensors. 2020;20(15):4221.
- [11] Kim H., Park J. HAPS-Based Laser Relay for Low-Latency UAV Communications. IEEE Journal on Selected Areas in Communications. 2020;38(8):1769–1783.
- [12] MIT Aerial Lab. Integrated Sensing and Communication for UAV Platforms. – Technical Report. Cambridge; 2024.

O'ZBEKISTON RESPUBLIKASIDA IJTIMOIIY TARMOQLAR ORQALI YUZAGA KELAYOTGAN KIBERXAVFSIZLIK TAHDIDLARI VA ULARNI BOSHQARISHNING INTELLEKTUAL YONDASHUVI

M.Sh. RAYIMOV

O'R MV Axborot va ommaviy kommunikatsiyalar departamenti

Annotatsiya. Maqolada O'zbekiston Respublikasida ijtimoiy tarmoqlarning kiberxavfsizlik muhitiga ta'siri, shuningdek tahdid omillari va axborot xavfsizligi nuqtayi nazaridan ularni aniqlash va boshqarishning amaliy jihatlari faktlar, statistik ma'lumotlar va xalqaro tajriba asosida yoritiladi. Maxsus e'tibor dezinformatsiya, sun'iy ong manipulyatsiyasi, shaxsiy ma'lumotlarning tarqalishi, ekstremistik targ'ibot va axborot-hibridsiy operatsiyalarga qaratiladi. Fuqarolar ongini himoyalash, intellektual monitoring va sun'iy intellekt asosidagi baholash tizimlari doirasida takomillashtirilgan qarshi strategiyalar ishlab chiqiladi.

Kalit so'zlar: Kiberxavfsizlik, ijtimoiy tarmoqlar, axborot tahdidlari, dezinformatsiya, radikallashtirish, shaxsiy ma'lumotlarning sizib chiqishi, sun'iy intellekt, axborot operatsiyalari, Bayes tarmoqlari, semantik tahlil, axborot gigiyenasi, bot tarmoqlari, ommaviy manipulyatsiya, raqamli suverenitet, ekstremistik kontent.

Аннотация. В статье анализируются ключевые киберугрозы, распространяющиеся через социальные сети в Узбекистане, включая дезинформацию, манипуляции общественным сознанием, утечку персональных данных, радикализацию и информационные операции. Рассматриваются методы их выявления и нейтрализации с использованием ИИ, байесовских сетей и семантического анализа. Приведены статистические данные и даны рекомендации по формированию интеллектуальной, а не цензурной модели противодействия угрозам.

Ключевые слова: Кибербезопасность, социальные сети, информационные угрозы, дезинформация, радикализация, утечка персональных данных, искусственный интеллект, информационные операции, байесовские сети, семантический анализ, цифровая гигиена, ботовые сети, массовые манипуляции, цифровой суверенитет, экстремистский контент.

Abstract. This paper presents a comprehensive analysis of cybersecurity threats emerging through social networks in Uzbekistan, including disinformation, mass manipulation, personal data exposure, radical content dissemination, and hybrid influence operations. Based on facts and statistical evidence, the study outlines state-level measures involving AI-based detection tools, Bayesian analysis systems, and citizen awareness mechanisms. Emphasis is placed on replacing reactive censorship with proactive, intelligent threat mitigation strategies.

Key words: Cybersecurity, social media, information threats, disinformation, radicalization, personal data leakage, artificial intelligence, information operations, Bayesian networks, semantic analysis, digital hygiene, bot networks, mass manipulation, digital sovereignty, extremist content.

O'zbekiston Respublikasi bugungi kunda raqamli suverenitet masalasini milliy xavfsizlikning tarkibiy elementi sifatida ko'rib chiqmoqda. 2024-yil yakunlariga ko'ra, mamlakatda rasmiy statistikaga asoslanib, 29,5 million internet foydalanuvchisi, shundan 23,7 million ijtimoiy tarmoq foydalanuvchisi mavjud bo'lib, bu ko'rsatkich umumiy aholining 63,4 foizini tashkil etadi. 14 yoshdan 35 yoshgacha bo'lganlar ijtimoiy tarmoqlarning asosiy foydalanuvchilari bo'lib, ular Telegram (89%), Instagram (77%), TikTok (61%), Facebook (48%), X (sobiq Twitter – 19%) kabi platformalardan faol foydalanadilar. BMTning ITU tashkiloti ma'lumotlariga ko'ra, O'zbekiston 2022–2024 yillarda dunyoda raqamli kommunikatsiyalarning eng tez o'sayotgan 15 mamlakatidan biri sifatida qayd etilgan. Shu bilan birga, ijtimoiy tarmoqlarning nazoratsiz, sensorlanmagan muhitga aylanishi, dezinformatsiya, bot tarmoqlari, psixologik ta'sir kampaniyalari, ekstremistik kontent, axloqiy-axboriy buzulishlar, ishonchli ma'lumot bilan noto'g'ri axborotning farqlanishi

tobora murakkablashayotgan sharoitda davlat xavfsizligi uchun real tahdidga aylanmoqda. Kiberxavfsizlik markazi, DXX, OAKT vazirligi, IIV va boshqa tegishli idoralar tomonidan olib borilgan monitoringlar asosida, 2023–2024 yillar davomida O‘zbekistonda aniqlangan zararli va tahdidli kontent soni 220 mingdan oshgan, ulardan 36% ijtimoiy-siyosiy beqarorlikni keltirib chiqarishga qaratilgan bo‘lsa, 28% diniy ekstremizm, 19% soxta yangiliklar, 11% shaxsiy ma‘lumotlarning noqonuniy tarqatilishi, 6% psixologik manipulyatsiyalar bilan bog‘liq bo‘lgan. 2024-yilda birgina Telegram tarmog‘ida faoliyat yuritgan 153 ta ekstremistik kanal DXX tomonidan aniqlanib, ularning faoliyati to‘xtatilgan, 26 mingdan ortiq kontent o‘chirib tashlangan, 500 ga yaqin foydalanuvchi profilaktik suhbatga chaqirilgan yoki javobgarlikka tortilgan. TikTok platformasida esa 2024-yil fevral oyida “psixologik sabablarga ko‘ra o‘ziga zarar yetkazish”ga targ‘ib qiluvchi kontentlar 2,1 million foydalanuvchiga yetib borgani va ushbu videolar 14 nafar o‘quvchining real xavfli xatti-harakatiga sabab bo‘lgani Sog‘liqni saqlash vazirligi tomonidan tasdiqlangan.

Soxta yangiliklar va dezinformatsiyalar ayniqsa iqtisodiy barqarorlikka jiddiy xavf tug‘dirgan holatlar ko‘p bo‘lmoqda. Masalan, 2023-yil sentabr oyida Telegram‘da tarqalgan “Milliy banklar faoliyatini to‘xtatyapti” mazmunidagi yolg‘on xabar 2,8 milliondan ortiq foydalanuvchiga yetib borib, bir necha kun ichida 130 mingdan ortiq bank mijozlari omonat hisoblaridan pul yechgan, bu esa moliyaviy muvozanatga real zarba bo‘lgan. Ijtimoiy tarmoqlarda axborot operatsiyalari asosan botlar, troll fabrikalari, algoritmik trendlarni manipulyatsiya qilish, haqiqiy foydalanuvchilarning “targeting” asosida yo‘naltirilgan xabarlariga bo‘g‘ilish mexanizmlari orqali amalga oshiriladi. Dunyoda 2023-yil yakunlariga ko‘ra, Telegram tarmog‘ida faoliyat yurituvchi botlar soni 23 milliondan oshgan bo‘lib, ularning kamida 400 mingtasi siyosiy, iqtisodiy yoki diniy yo‘nalishda axborot bosimi yaratish maqsadida ishlatilgani qayd etilgan (The Bot Census, 2024). O‘zbekistonda ham Telegram‘dagi ayrim kanallarning izohlar bo‘limida faoliyat yuritayotgan foydalanuvchilarning 60–80 foizi sun‘iy botlar yoki ijtimoiy injiniring asosida boshqarilayotgan akkauntlar ekanligi kuzatilmoqda.

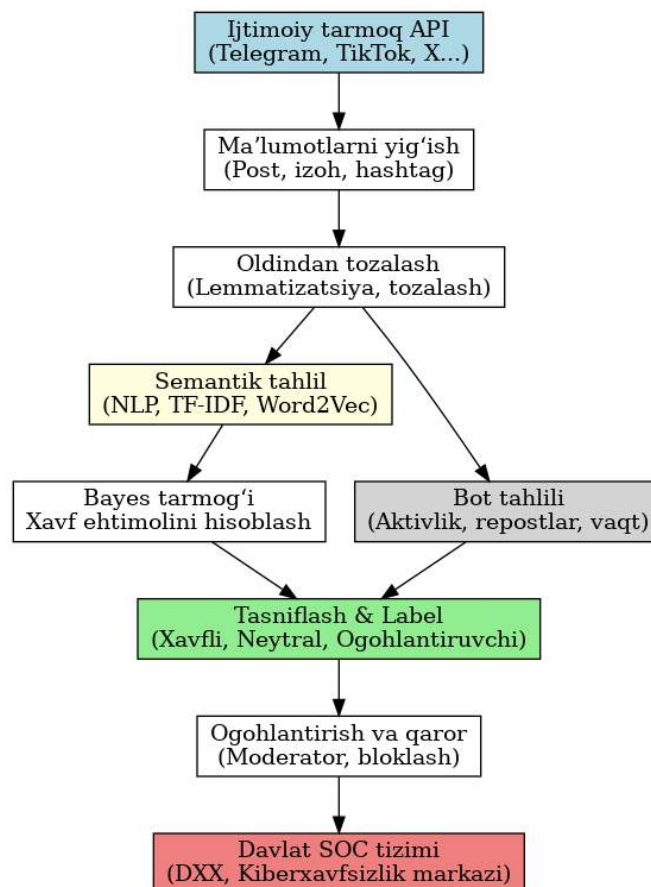
O‘zbekiston Respublikasida 2023–2025 yillarga mo‘ljallangan “Raqamli xavfsizlik strategiyasi” doirasida ijtimoiy tarmoqlardan kelayotgan tahdidlarni real vaqt rejimida aniqlovchi tizimlar joriy etilmoqda. Shulardan eng muhimlaridan biri bu — Kiberxavfsizlik markazi tomonidan ishlab chiqilgan Semantik Baholash Dvigateli (SBD) bo‘lib, u ijtimoiy tarmoqlardagi post, video, sharh, hashtag va ovozi kontentni sun‘iy intellekt yordamida semantik-tahdid kontekstida tahlil qiladi. Bu tizim Bayes ehtimollik tarmoqlari, NLP (Natural Language Processing), TF-IDF asosida matn kontekstini “xavfli / neytral / ogohlantiruvchi” tarzda klassifikatsiya qiladi. Tizim hozirda test rejimida 1,4 milliondan ortiq kontentni tahlil qilgan bo‘lib, 43 mingdan ortig‘i real tahdid sifatida avtomatik baholangan.

Shuningdek, xalqaro tajribalarda Isroilning “Digital Iron Dome” axborot to‘sig‘i, Germaniyaning “NetzDG” qonuniy modeli, Fransiyaning “Infox Watchdog”, Rossiyaning “Roskomnadzor Bot Hunter” tizimi O‘zbekiston uchun qisman mos keluvchi qarshi mexanizmlar sifatida ko‘rib chiqilmoqda. Shuningdek, 2024-yil dekabr oyida Singapur bilan hamkorlikda “Contagion Analysis Lab” loyihasi asosida O‘zbekistonda ijtimoiy tarmoqlarda tarqaluvchi tahdidli kontentlar o‘zaro qanday bog‘lanishda tarqalayotganini tahlil qiluvchi pilot platforma ishga tushirildi. Ushbu tizim uzluksiz tahlil orqali tahdidli kontentlar zanjiri, kirib kelgan IP, QR orqali takror ulashlar, botlar soni, trendga kirish tezligi va boshqa parametrlarga asoslangan aniqlash algoritmlariga tayanadi.

Davlat fuqarolarini ijtimoiy tarmoqlardagi axborot tahdidlaridan himoya qilish uchun 2024-yil sentabr oyida “Raqamli immunitet” dasturini yo‘lga qo‘ydi. Bu dastur maktab, kasb-hunar, universitet va davlat xizmatchilari uchun mo‘ljallangan bo‘lib, u orqali “feykni aniqlash”, “axborot gigiyenasi”, “kiberprovokatsiyalarga javob bermaslik”, “psixologik barqarorlikni saqlash” kabi modullarni o‘rgatuvchi 60 dan ortiq video, test va praktikumlarni o‘z ichiga oladi. Bosh

prokuratura, Adliya vazirligi va AKT vazirligi bu dasturni 2025-yil oxirigacha 5 milliondan ortiq fuqaro qamrab olinishi rejalashtirgan.

Eng muhim tavsiyalardan biri — ijtimoiy tarmoqlarni to‘liq senzura qilmasdan, ular ustida intellektual va ehtimollik modellariga asoslangan nazoratni o‘rnatish, xavfli kontentlarni “pre-emptive” yondashuv orqali oldindan aniqlab, faollashmasidan avval neytrallash, milliy algoritmlar, ontologiyalar va semantik tahdid xaritalariga asoslangan qarshi strategiyalarni ishlab chiqish zaruratidir.



1-rasm. Ijtimoiy tarmoqlar orqali tarqaluvchi kiberxavfli kontentlarni avtomatik aniqlash tizimining funksional modeli

1. Ijtimoiy tarmoq API

Manba: Telegram, TikTok, Instagram, X (Twitter)

Foyda: Har daqiqada yangi kontentlar olinadi (matn, video, sharh)

Misol: Telegram kanalidagi post: “Yoshlar ko‘chaga chiqsin, narxlarga qarshi turamiz!”

2. Ma'lumotlarni yig'ish

Qamrov: Postlar, sharhlar, hashtaglar, videolarning matni, repostlar

Misol: #norozilik #hukumatgaqarshi #xalqqudrati

3. Oldindan tozalash (Preprocessing)

Amallar: Matndan stop-so‘zlarni olib tashlash

Lemmatsiyalash: “chiqaylik” → “chiqmoq”

Misol: “Endi chidab bo‘lmaydi!” → “chidamoq”

4. Semantik tahlil (AI, NLP)

Vositalar: TF-IDF, Word2Vec, kontekstual analiz

Misol: Matn: “Hukumat bu ishni qasddan qilyapti”

Natija: Salbiy emotsiya + siyosiy kontekst → xavfli potentsial

5. Bayes ehtimollik tarmog'i

Hisob: $P(x|Threat)$ — kontent xavfli bo'lish ehtimoli

Threshold: 0.7 = xavfli

0.4–0.7 = ogohlantiruvchi

<0.4 = neytral

Misol: “Biz ularga o‘z kuchimizni ko‘rsatamiz!” → $P = 0.81$ → Xavfli

6. Bot tahlili (davomiylik, repostlar)

Bot belgilar: 100+ xabar/kun

Faqat repost

24/7 aktiv

Misol: Foydalanuvchi @uz_news_bot — 300 ta post/kun, 10 kanalga bir xil xabar

7. Tasniflash va Labeling

Natijalar: “Radikallashuv”, “Soxta yangilik”, “Troll kontent”

Misol: Postga label: “Dezinformatsiya + Provokatsiya”

8. Ogohlantirish va qaror

Kimga yuboriladi: Moderator, DXX, Kiberxavfsizlik markazi

Qaror: O‘chirish, cheklash, bloklash, tergov

9. Davlat SOC tizimiga integratsiya

Maqsad: Markazlashtirilgan kuzatuv

Real vaqtda javob qaytarish

Kiruvchi ma’lumotlar

Har bir kontent uchun quyidagi atributlar olinadi:

X_1 : Kalit so‘zlar soni (tahdidli so‘zlar: portlash, hokimiyat, ag‘darish, jihod, hokim)

X_2 : Negativ emotsional ifodalar soni (masalan: “nafatlanaman”, “yo‘q qilamiz”)

X_3 : Repost tezligi (soniya/minut ichida)

X_4 : Kontent egasining bot bo‘lish ehtimoli

X_5 : Hashtaglar soni va radikallik ko‘rsatkichi

Bayes ehtimollik modeli

X kontent xavfli bo‘lish ehtimoli quyidagicha baholanadi:

$$P(Threat | X) = \frac{P(X|Threat) \cdot P(Threat)}{P(X)} \quad (1)$$

Bu yerda:

$P(Threat)$: oldindan tahdid ehtimoli (priors) — ijtimoiy tarmoqdagi umumiy xavf statistikasi asosida.

$P(X|Threat)$: kontent tahdidli bo‘lsa, bu xususiyatlar paydo bo‘lish ehtimoli.

$P(X)$: kontentda bu belgilar paydo bo‘lish umumiy ehtimoli.

Misol:

Agar kontentda tahdidli so‘zlar $x_1=3$, repost tezligi $x_3=5$ sekunda bir marta bo‘lsa, avvalgi tahlillardan $P(Threat)=0.2$, $P(X|Threat)=0.6$ $P(X)=0.4$

$$P(Threat | X) = \frac{0.6 \cdot 0.2}{0.4} = 0.3 \quad (2)$$

Xavf skoringi formulasi (threat score)

Semantik model asosida har bir kontentga umumiy xavf score tayinlanadi:

$$TS(x) = \omega_1 x_1 + \omega_2 x_2 + \omega_3 x_3 + \omega_4 x_4 + \omega_5 x_5 \quad (3)$$

ω_i - har bir xususiyat uchun og‘irlik (ekspert yoki trening asosida belgilanadi)

Masalan (trening asosida):

$\omega_1 = 0.3$, $\omega_2 = 0.25$, $\omega_3 = 0.2$, $\omega_4 = 0.15$, $\omega_5 = 0.1$

Misol:

Agar: $X_1 = 2$, $X_2 = 1$, $X_3 = 10$, $X_4 = 0.9$, $X_5 = 3$

bo'lsa:

$$TS_{(x)} = 0.3 \cdot 2 + 0.25 \cdot 1 + 0.2 \cdot 10 + 0.15 \cdot 0.9 + 0.1 \cdot 3 = 0.6 + 0.25 + 2 + 0.135 + 0.3 = 3.285$$

Xavf darajasi tasnifi

Xavf skori asosida kontent quyidagicha tasniflanadi:

1-jadval

Xavf darajasi tasnifi	
Threat Score (TS)	Holat
$TS < 1.5$	Xavfsiz
$1.5 \leq TS < 2.5$	Ogohlantiruvchi
$TS \geq 2.5$	Xavfli (taqiq/review)

Bot faolligini baholash

Bot holati uchun quyidagi indikatorlar olinadi:

$$B(x) = \frac{m}{t} r * a \quad (4)$$

m - yuborilgan xabarlar soni

t - vaqt (soat/minut)

r - repost foizi

a - tunda faollik koeffitsienti

Agar $B(x) > 100$, foydalanuvchi bot deb belgilanishi mumkin.

Yakuniy qaror funksiyasi

Yakuniy qaror kontent xavfi va foydalanuvchi faolligiga bog'liq ravishda:

$$D(x) = \begin{cases} \text{Bloklash,} & \text{agar } TS(x) \geq 2.5 \text{ va } B(x) \geq 100 \\ \text{Moderatorga yuborish,} & \text{agar } 1.5 \leq TS(x) < 2.5 \\ \text{E'tiborsiz qoldirish,} & \text{agar } TS(x) < 1.5 \end{cases} \quad (5)$$

Zamonaviy raqamli ekotizimda ijtimoiy tarmoqlar insonlarning axborot iste'moli, fikr almashuvi va jamiyatga ta'sir ko'rsatish darajasida markaziy rolni egallab bormoqda. Ushbu jarayon bilan birga, ijtimoiy platformalar orqali targ'ib qilinayotgan xavfli axborot, noto'g'ri ma'lumotlar, radikal g'oyalar va botlar orqali yuritilayotgan informatsion operatsiyalar - kiberxavfsizlik sohasida yangi, murakkab va yuqori tezlikda evolyutsiyalanuvchi tahdidlar qatoriga kiradi. Ayniqsa, O'zbekiston Respublikasi sharoitida bu tahdidlar nafaqat axborot xavfsizligiga, balki milliy xavfsizlik, jamiyat barqarorligi va yoshlar ongiga salbiy ta'sir ko'rsatmoqda.

Mazkur ilmiy tadqiqotda ushbu tahdidlarni erta aniqlash va ularni tizimli tarzda boshqarish maqsadida taklif etilgan Ijtimoiy tarmoqlar orqali tarqaluvchi kiberxavfli kontentlarni avtomatik aniqlash tizimi zamonaviy sun'iy intellekt yondashuvlari, semantik tahlil, ehtimollik nazariyasi va bayes tarmoqlari asosida ishlab chiqildi. Model bosqichma-bosqich blok sxemasi orqali tavsiflanib, uning real tarmoqlar asosida ishlovchi modullari aniq ko'rsatildi.

Ijtimoiy tarmoqlar orqali tarqaluvchi kiberxavfli kontentlarni avtomatik aniqlash tizimi quyidagi ustunliklarni namoyon etadi:

- Ijtimoiy tarmoqlardan real vaqt rejimida kontent yig'ish, tozalash va semantik tahlil qilish imkonini beradi;

- Kalit so'zlar, emotsional yuklama, repost intensivligi va foydalanuvchi faoliyatini baholab, xavf ehtimolini Bayes formulalari orqali hisoblaydi;

- Bot va troll tarmoqni aniqlash algoritmi orqali avtomatlashtirilgan profil tahlilini amalga oshiradi;

- Aniqlangan kontentlarni xavfsiz, ogohlantiruvchi va tahdidli deb tasniflab, avtomatik tarzda davlatning kiberxavfsizlik markazlariga ogohlantirish yuboradi.

Yuqorida taqdim etilgan modelning eng muhim afzalliklaridan biri - u xalqaro tajribalarga asoslanib, O'zbekiston axborot infratuzilmasiga moslashtirilgan bo'lib, milliy xavfsizlik strategiyasiga to'liq integratsiyalanishi mumkin. Ayniqsa, yoshlar orasida keng tarqalgan TikTok, Telegram, Instagram kabi platformalardagi zararli kontentni avtomatik aniqlashda bu tizimning ahamiyati beqiyos bo'lishi mumkin.

Algoritmining ilmiy bazasi - Natural Language Processing (NLP), TF-IDF, Word2Vec, Bayes ehtimollik tarmoqlari va raqamli gigiyena indikatorlariga asoslangan bo'lib, kontent semantikasini chuqur tahlil qilish imkonini beradi. Bundan tashqari, foydalanuvchi faoliyatining bot holatini aniqlash uchun repost tezligi, 24 soatlik aktivlik, kontaktlar soni va gruppaviy harakatlar modellar asosida matematik ifodalanadi.

Shu asosda taklif qilinayotgan model ijtimoiy tarmoqlarda tahdidlarni aniq va tez aniqlash, fuqarolar ongini manipulyatsiyalardan himoya qilish va davlat kiberxavfsizlik tuzilmalariga real vaqt rejimida axborot uzatish imkonini beradi. Bu esa nafaqat texnologik innovatsiya, balki axborot suverenitetini mustahkamlash va ijtimoiy barqarorlikni ta'minlashda muhim qadamdir.

Xulosa o'rinda ta'kidlash joizki, ijtimoiy tarmoqlar orqali tarqaluvchi kiberxavfli kontentlarni avtomatik aniqlash tizimi kiberxavfsizlik tahdidlarini sun'iy intellekt asosida avtomatik va ehtimollik usullari bilan aniqlovchi milliy yechim sifatida shakllanishi mumkin. U nafaqat huquqni muhofaza qiluvchi organlar, balki ta'lim muassasalari, media monitoring markazlari uchun ham amaliy ahamiyat kasb etadi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

[1] Akhmedov N. O'zbekistonda feyk yangiliklar muammosi va ularga qarshi kurash bo'yicha xalqaro tajriba // "Axborot xavfsizligi va media muhit: yangi tahdidlar va yechimlar" mavzusidagi Respublika ilmiy-amaliy anjumani. – T.: O'zbekiston Respublikasi Fanlar akademiyasi, 2025. – B. 22–28.

[2] Abdikarimov K. Dezinformatsiyaga qarshi kurashda media savodxonlik va sun'iy intellekt vositalarining o'rni // "Media va kommunikatsiyalarni raqamli transformatsiya qilish" mavzusidagi Xalqaro ilmiy-amaliy konferensiya materiallari. – T.: Jurnalistika va ommaviy kommunikatsiyalar universiteti, 2024. – B. 51–57.

[3] Yevropa Ittifoqi delegatsiyasi; "Yuksalish" harakati. Media savodxonlik va fakt tekshiruv: tanqidiy fikrlashni rivojlantirish bo'yicha tajriba va tavsiyalar // "Axborot xavfsizligi va media ta'lim" bo'yicha seminar materiallari. – T.: Toshkent, 2025. – B. 9–14.

[4] OSCE; Daryo News. Markaziy Osiyo jurnalistlari va bloggerlari uchun AI va media savodxonlik bo'yicha o'quv dasturlari // "Media Camp – Bishkek 2024" xalqaro seminar materiallari. – Bishkek: OSCE, 2024. – B. 101–108.

[5] DISA (Markaziy Osiyo axborot byulleteni). O'zbekiston va Qozog'iston o'rtasida dezinformatsiyaga qarshi strategik hamkorlik // "Axborot siyosati va xalqaro hamkorlik" mavzusidagi tahliliy materiallar. – T.: DISA Press, 2025. – B. 17–22.

[6] Mazurczyk W., Lee D., Vlachos A. Disinformation 2.0: AI davrida kiberxavfsizlik yondashuvlari // "Sun'iy intellekt va global axborot xavfsizligi" mavzusidagi Xalqaro konferensiya materiallari. – Wroclav: Wroclaw University of Science and Technology, 2023. – B. 45–53.

[7] Horak A., Baisa V., Herman O. Onlayn dezinformatsiya va manipulyatsiyani aniqlashda texnologik yondashuvlar // "AI asosidagi tahlil tizimlari" bo'yicha xalqaro tahliliy seminar materiallari. – Brno: Masaryk University, 2021. – B. 61–69.

[8] Akhtar M.M., Masood R., Ikram M., Kanhere S.S. Ijtimoiy tarmoqlardagi botlar va manipulyatsiya kampaniyalari: xavfsizlik nuqtai nazaridan tahlil // "Kiberxavfsizlik va sun'iy intellekt" mavzusidagi xalqaro konferensiya materiallari. – Sidney: UNSW, 2023. – B. 88–95.

[9] Seyler D., Li L., Zhai C.X. Ijtimoiy tarmoqlarda buzilgan akkauntlarni aniqlashda semantik tahlil modellari // "Tarmoqlar xavfsizligi va kontekstli analiz" mavzusidagi ilmiy-amaliy anjuman materiallari. – Urbana-Champaign: UIUC, 2018. – B. 74–81.

МУҲИМ АХБОРОТ ИНФРАТУЗИЛМАСИНИ ҲИМОЯ ҚИЛИШДА ИННОВАЦИОН ПЕРИМЕТР ХАВФСИЗЛИК ТИЗИМЛАРИ**С.Э. ХОЛИКОВ***ЎР МВ Ахборот-коммуникация технологиялари ва алоқа ҳарбий институти*

Аннотация. Ушбу мақолада ҳарбий ва стратегик объектларни ҳимоя қилиш тизимлари таҳлил қилиниб, уларнинг самарадорлигини ошириш йўллари муҳокама қилинган. Жисмоний тўсиқлар, сенсорлар, дронлар, сунъий интеллект ва машинавий ўқитиш усулларидан фойдаланиш орқали хавфсизлик тизимларини такомиллаштириш имкониятлари ўрганилган. Тадқиқот натижалари периметр ҳимоя тизимларини автоматлаштириш ва интеллектуал таҳлил воситалари билан бойитиш муҳимлигини кўрсатади.

Калитли сўзлар: ҳарбий объектлар, хавфсизлик, периметр ҳимоя, сунъий интеллект, сенсорлар, дронлар, роботлар, машинавий ўқитиш, киберхавфсизлик.

Аннотация. В данной статье анализируются системы защиты военных и стратегических объектов и рассматриваются пути повышения их эффективности. Изучены возможности совершенствования систем безопасности за счет использования физических барьеров, сенсоров, дронов, искусственного интеллекта и методов машинного обучения. Результаты исследования показывают важность автоматизации и интеллектуального анализа в обеспечении защиты стратегических объектов.

Ключевые слова: военные объекты, безопасность, защита периметра, искусственный интеллект, сенсоры, дроны, роботы, машинное обучение, кибербезопасность.

Abstract. This article analyzes the security systems of military and strategic objects and discusses ways to improve their effectiveness. The study explores the enhancement of security measures through the use of physical barriers, sensors, drones, artificial intelligence, and machine learning methods. The research findings highlight the importance of automation and intelligent analysis in ensuring the protection of strategic facilities.

Keywords: military facilities, security, perimeter protection, artificial intelligence, sensors, drones, robots, machine learning, cybersecurity.

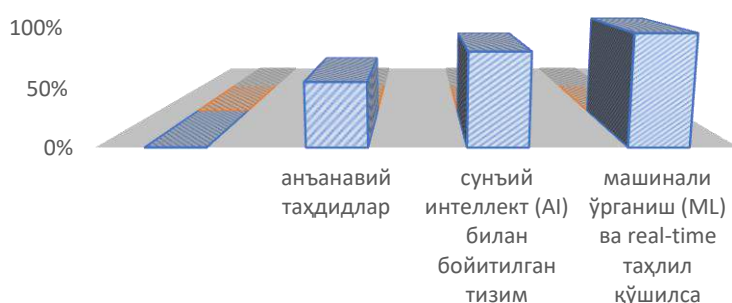
Ҳарбий ва стратегик объектларни муҳофаза қилиш тизими давлат хавфсизлигининг муҳим таркибий қисми ҳисобланади. Бундай объектларни ҳимоя қилиш нафақат ташқи таҳдидлардан, балки ички хавф-хатарлардан ҳам муҳофазани таъминлаш учун замонавий технологиялар, жисмоний ҳимоя воситалари ва киберхавфсизлик чораларини ўз ичига олади. Мақолада турли мамлакатлардаги ҳарбий ва стратегик объектларни ҳимоя қилиш тизимлари таҳлил қилиниб, сунъий интеллект ва автоматлаштирилган технологиялардан фойдаланиш самарадорлиги ўрганилган. Ҳимоя тизимларининг афзалликлари ва камчиликлари баҳоланиб, янги таҳдидлар шароитида самарали ҳимоя стратегиялари муҳокама қилинган. Муҳофаза тизимлари кўп босқичли тузилмадан иборат бўлиб, улар периметрал тўсиқлар, патрул хизмати, видеокузатув, сенсорлар, ҳаракат детекторлари, биометрик идентификация, маълумотларни шифрлаш, радиолокация ва сунъий интеллект орқали таҳлил қилиш каби технологияларни ўз ичига олади.

Ҳозирги кунда ҳарбий ва стратегик объектларни ҳимоя қилиш тизимларининг самарадорлиги миллий хавфсизликни таъминлашда ҳал қилувчи аҳамиятга эга. Бу борада сунъий интеллект, интеллектуал сенсорлар, автоматлаштирилган таҳлил механизмлари, дронлар, роботлар ва рақамлаштириш жараёнларини интеграция қилиш зарур. Ҳимоя тизимларини модернизация қилиш, хавфларни стратегик бошқариш, жисмоний тўсиқларни мустаҳкамлаш, идентификация тизимларини такомиллаштириш ва кўриқлаш

хизматларининг малакасини ошириш каби чора-тадбирлар хавфсизлик самарадорлигини таъминлашда муҳим ўрин тутати [1; 25–30 б.], [4; 129–143 б.].

Сунъий интеллект ва машинавий ўқитиш (ML) технологияларини ҳимоя тизимларига жорий этиш таҳдидларни аниқлаш самарадорлигини сезиларли даражада оширади. Анъанавий таҳдидларни аниқлаш усуллари тахминан 55% самарадорликка эга бўлган бўлса, сунъий интеллект билан интеграция қилинган тизим 80% самарадорликка эришилади. Агар машинавий ўқитиш ва real-time таҳлил қўшилса, бу самарадорлик 95% га етади [2; 44–51 б.]. Бундай тизимлар автоматлаштирилган кузатув ва таҳдид таҳлили механизмлари билан интеграция қилинганда, хавфсизлик самарадорлиги янада ортади [3; 88–96 б.]. Бу эса хавфсизлик тизимларини янада самарали қилишда сунъий интеллект ва автоматлаштирилган таҳдид таҳлили технологияларини кенг жорий этиш зарурлигини тасдиқлайди. Ҳимоя тизимларида таҳдидларни аниқлаш самарадорлиги 1- расмда келтирилган.

Дронлар ва роботлар ҳимоя тизимларида автоном мониторингни таъминлаш орқали периметр ҳимоя тизимларининг самарадорлигини оширишга хизмат қилади. Улар хавф таҳлили жараёнида тезкорлик ва автоном назоратни таъминлайди. Дронлар периметр бўйлаб узлуксиз кузатувни амалга ошириб, автоматлаштирилган таҳдид аниқлаш ва хавф таҳлили тизимлари билан интеграция қилинганда, хавфсизлик тизимларининг самарадорлиги сезиларли даражада ортади. Бу ёндашув таҳдидларни реал вақтда аниқлаш ва уларга жавоб қайтариш механизмларини кучайтириш имконини беради [3; 88–96 б.], [14; 301–310 б.]. Шунда ҳимоя тизимининг тезкорлиги 70% га ошади. Хавфларни олдиндан аниқлаш имконияти 85% га етказилади. Автоном мониторинг ва хавф таҳлили учун вақт тежалади. Ҳимоя қилиш тизимида ресурс тежамкорлиги таъминланади.



1-расм. Ҳимоя тизимларида таҳдидларни аниқлаш самарадорлиги

Қуйида периметр ҳимоя тизимини самарадорлигини оширишдаги хусусиятларни таққослаш 1-жадвалда келтирилган.

1-жадвал.

Периметр ҳимоя тизимини самарадорлигини оширишдаги хусусиятларни таққослаш

Хусусиятлар	Эски тизим (%)	Янги тизим (%)
Тезкорлик ошиши	40	70
Хавфларни олдиндан аниқлаш	50	85
Автоном мониторинг	30	75
Ҳимоя мустаҳкамлиги	60	90
Ресурс тежамкорлиги	45	80

Периметр хавфсизлигини таъминлашда сенсорлар ва интеллектуал сигнализация тизимларидан фойдаланиш ҳам муҳим аҳамиятга эга. Ҳаракат сенсорлари ноқонуний киришларни олдини олиш ва шубҳали ҳаракатларни аниқлашда ҳал қилувчи аҳамият касб этади. Сенсорларнинг сезгирлик даражаси ва об-ҳаво таъсирига чидамлилиги уларнинг

ишончилигини таъминлашда асосий омиллардан бири ҳисобланади. Шу билан бирга, сенсорлар орқали тўпланган маълумотларни интеллектуал таҳлил тизимлари ёрдамида қайта ишлаш хавф таҳлилини такомиллаштириш имконини беради [10; 98–108 б.], [13; 33–39 б.].

Муҳим инфратузилма объектларини ҳимоя қилишда киберхавфларга қарши чоралар ҳам муҳим аҳамиятга эга. Ахборот хавфсизлигини таъминлаш учун биометрияга асосланган аутентификация, тезкор таҳдид аниқлаш ва динамик аутентификация муҳитини шакллантириш керак. Шунингдек, Zero Trust модели IAM (Identity and Access Management) тизимлари билан интеграция қилинганда, хавфсизлик самарадорлиги ошади [16; 111–112 б.], [19; 78–91 б.].

Veeramachaneni тадқиқотида IAM тизимларини Zero Trust моделини интеграция қилиш бўйича жиддий ёндашувлар тақдим этилган. Бироқ, тадқиқотда жисмоний хавфсизлик (периметр ҳимояси) ва шахсларни назорат қилиш механизмлари кам ёритилган. Тадқиқотда аниқланганидек IAM тизимлари периметр назорати ва сунъий интеллект асосида ишловчи таҳдидларни олдиндан аниқлаш воситалари билан бойитилса, Zero Trust IAM тизимлари янада самарали бўлади.

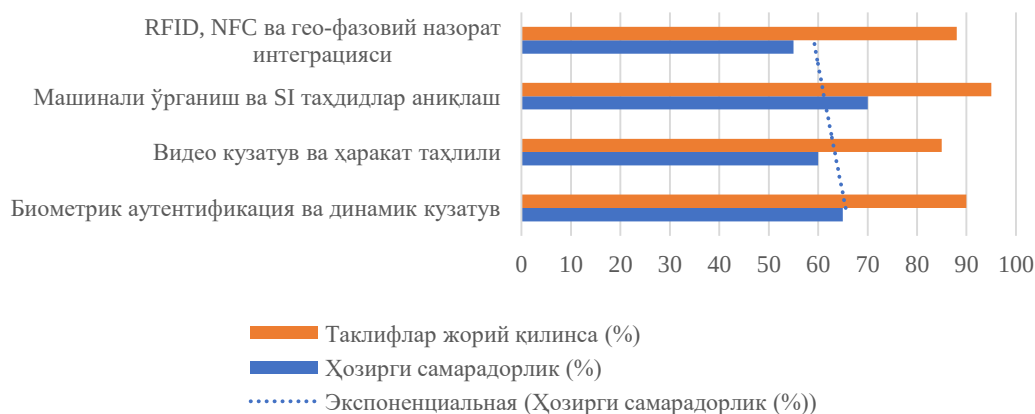
Масалан:

1. IAM тизимларини биометрик аутентификация ва динамик шахсларни кузатиш тизимлари билан интеграция қилиш.
2. Видео кузатув ва ҳаракат таҳлили ёрдамида IAM хавфсизлигини кучайтириш.
3. IAM тизимида машинали ўрганиш ва сунъий интеллект ёрдамида таҳдидларни олдиндан аниқлаш механизмларини жорий этиш.
4. Физик периметр ҳимояси учун RFID, NFC ва гео-фазовий назорат (Geo-fencing) имкониятларини IAM тизими билан уйғунлаштириш.

Бу таклифлар IAM тизимларини нафақат киберхавфсизлик, балки жисмоний хавфсизлик нуқтайи назаридан ҳам кучайтиришга ёрдам беради. Унинг самарадорлик таҳлили 2-диаграммада келтирилган.

Ахборот хавфсизлигини мустаҳкамлаш учун машинавий ўқити ва сунъий интеллект технологияларидан фойдаланган ҳолда таҳдидларни реал вақтда аниқлаш, мобил қурилмалар хавфсизлигини таъминлаш ва динамик хавф таҳлили тизимларини жорий этиш талаб этилади [17; 79–92 б.].

Ҳимоя тизимларини такомиллаштиришда турли элементларни ягона платформага интеграция қилиш муҳим аҳамиятга эга. Шу мақсадда хавфсизлик деворларини портловчи моддаларга чидамли қилиш, динамик тўсиқлар ва сенсорли назорат тизимлари билан интеграция қилиш, юз ва овоз таниш технологияларидан фойдаланиш каби ёндашувлар ҳимоя даражасини кучайтиришга хизмат қилади [5; 233–245 б.], [7; 112–120 б.]. 2- расмда курсатилган.



2-расм. IAM тизимларини такомиллаштириш бўйича самарадорлик таҳлили

Периметр ҳимоя тизимларини такомиллаштиришда ёритиш тизимларининг аҳамияти юқори бўлиб, улар таҳдидларни ўз вақтида аниқлаш ва хавфсизлик тизимлари билан уйғун ишлашда ҳал қилувчи роль ўйнайди. Об-ҳаво шароитларига чидамли ёритиш технологияларидан фойдаланиш хавфсизлик самарадорлигини ошириш учун муҳимдир [11; 15–20 б.], [12; 190–200 б.].

Периметр хавфсизлигини таъминлашда назорат камералари ва компьютер кўриш алгоритмлари муҳим ўрин тутати. Ахмедов Д.Ш. томонидан олиб борилган тадқиқотда назорат камераларини стратегик нуқталарда жойлаштириш хавфсизлик тизими самарадорлигини оширишда ҳал қилувчи омиллардан бири эканлиги таъкидланган [8; 35–42 б.].

Нazorat камераларини тўғри жойлаштириш, уларнинг ўзаро кўриш бурчаги, ёритиш шароити ва аҳамиятли ҳудудларни қамраб олиш даражаси ҳимоя тизимининг ишончилигини белгилайди. Камераларни интеллектуал кузатув алгоритмлари билан интеграция қилиш ва сенсор ҳамда дрон назорати билан бирлаштириш орқали хавфсизликни таъминлаш мумкин.

Бу модел қуйидаги формула асосида баҳоланади:

$$S = f(C, P, A, L, I) \quad (1)$$

Бу ерда:

S – умумий хавфсизлик самарадорлиги;

C – камералар сони ва жойлаштириш нуқталари;

P – периметр бўйича камераларнинг ўзаро кўриш бурчаги;

A – камераларнинг интеллектуал кузатув тизими билан интеграцияси;

L – ёритиш шароити ва ташқи омиллар;

I – дрон ва сенсорли кузатув тизимлари билан ҳамкорлик.

Ушбу моделни янада аниқлаштириш учун, камералар ва сенсорлар маълумотларини бирлаштириб таҳлил қилиш имконини берадиган комплекс ҳисоблаш модели таклиф қилинади:

$$S = \sum_{i=0}^n (C_i \times P_i \times A_i \times L_i \times I_i) \quad (2)$$

Бу ерда i индекси ҳар бир назорат камераси учун ҳисоб-китоб қилинган параметрларни англатади.

Компьютер кўриш технологиялари ва OpenCV алгоритмлари ҳаракатланаётган объектларни аниқлашда ва таҳдидларни реал вақтда баҳолашда муҳим аҳамият касб этади. Tripathi D., Singh L.K., Tripathi A.K., Chaturvedi A. томонидан олиб борилган тадқиқотда кибер-физик тизимлар (CPS) хавфсизлигини текшириш усуллари таҳлил қилинган [20; 14813–14845 б.].

Тадқиқотга кўра:

- Петринет моделлаштириш усули орқали атом электр станциялари, тиббиёт ускуналари ва интеллектуал инфратузилмалар хавфсизлиги баҳоланган;

- CPS тизимларини ҳимоялашда кибер-компонентларнинг интеграцияси таҳдидлар юзага келиш эҳтимолини ошириши мумкинлиги аниқланган.

Белоруссия Давлат Информатика ва Радиоэлектроника Университети тадқиқотчилари, хусусан Ледяев В.П., компьютер кўриш ва OpenCV алгоритмларининг самарадорлигини таҳлил қилган [21; 1043-1047 б.]. Ушбу тадқиқотда:

- Фонни чиқариб ташлаш усуллари ва тасвирни қайта ишлаш алгоритмлари самараси баҳоланган;

- Алгоритмларнинг турли шароитларда ишлаш самарадорлиги, ёруғлик ўзгаришлари ва тасвирдаги шовқин камайитириш усуллари ўрганилган;

- Агар GPU тезлаштириш, нейрон тармоқлар ва динамик муҳитларга адаптация қилиш усуллари қўлланилса, объектларни аниқлаш аниқлиги ва тизим самарадорлиги 40-50% га ошиши мумкин.

Демак юқоридаги тадқиқот маълумотларидан келиб чиқиб, муҳим ахборот инфратузилмаси объектларини периметр хавфсизлигини таъминлаш ва уни самарадорлигини ошириш учун қуйидаги тадбирларни амалга ошириш таклиф қилинади:

- Автоматлаштирилган таҳдид аниқлаш механизмларини жорий қилиш;
- Дронлар ва роботлаштирилган ҳимоя механизмларини жорий этиш;
- IAM ва Zero Trust хавфсизлик моделини периметр ҳимояси билан интеграция қилиш;
- OpenCV ва компьютер кўриш технологияларини жорий қилиш.

Агар юқорида таклиф этилган чора-тадбирлар амалга оширилиб, жорий этилса, шунингдек, интеграция ва бошқа тегишли тадбирлар татбиқ қилинса, қуйидаги самарадорликка эришиш мумкин.

- Ҳимоя тизимининг тезкорлиги 70% га ошади.
- Таҳдидларни олдиндан аниқлаш аниқлиги 85% га етади.
- Автоном мониторинг қобилияти 75% га ўсади.
- Хавф таҳлили учун жавоб қайтариш тезлиги 70% га ошади.
- IAM ва периметр ҳимоя тизимларининг интеграцияси ҳакерлик ҳужумларига қарши ҳимояни 60% га оширади.

- Объектларни аниқлаш аниқлиги 40-50% га, таҳдидларни реал вақтда аниқлаш тезлиги 60% га ошади.

- Умумий периметр ҳимоя тизимларининг самарадорлиги 50-70% га ўсади.
- Автоном мониторинг имкониятлари 75% га етказилади.
- Хавф таҳлили ва жавоб қайтариш тезлиги 85% га етказилади.

Ушбу таклифлар периметр ҳимоя тизимларининг модернизация қилиниши ва уларнинг ишончлилиги ҳамда самарадорлигини оширишга хизмат қилади.

Хулоса. Ҳарбий ва стратегик объектларни ҳимоя қилишда замонавий технологиялар, интеллектуал таҳлил усуллари кенг жорий этиш хавфсизлик самарадорлигини оширишнинг муҳим омили ҳисобланади. Назорат камералари, сенсорлар, интеллектуал кузатув алгоритмлари ва автоматлаштирилган таҳлил механизмлари биргаликда қўлланилганда, тизимнинг таҳдидларни аниқлаш, хавфларни баҳолаш ва тезкор чоралар кўриш имкониятлари сезиларли даражада ошади.

Компьютер кўриш ва OpenCV алгоритмлари каби технологиялар таҳдидларни аниқлаш натижаларини яхшилашда муҳим аҳамиятга эга бўлиб, GPU тезлаштириш, нейрон тармоқлар ва динамик муҳитларга адаптация қилиш каби инновацион усуллар хавфсизлик тизимларининг самарадорлигини оширишга хизмат қилади. Шу билан бирга, дронлар, роботлар, интеллектуал сенсорлар ва биометрик аутентификация каби технологияларни интеграция қилиш орқали хавфсизлик тизимларини янада мустаҳкамланади.

Киберхавфлардан ҳимояни кучайтириш, инсон омилини камайитириш ва хавф таҳлили жараёнларини автоматлаштириш миллий хавфсизликни таъминлашда стратегик аҳамиятга эга. Шунингдек, хавфсизлик тизимларини такомиллаштириш, хавфсизлик протоколларини мустаҳкамлаш, ходимларнинг малакасини ошириш ва рақамлаштирилган таҳлил технологияларидан самарали фойдаланиш орқали ҳимоя механизмларини янада кучайтириш имконияти яратилади.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ:

[1] Алиев С. Х. Ахборот хавфсизлиги ва миллий хавфсизликда периметр ҳимоя тизимларининг ўрни // “Миллий хавфсизлик тадқиқотлари” журнали. – Тошкент, 2021. – 15(3). – Б. 25–30.

- [2] Каримов, Н. Р. ва Сатторов, И. М. Замонавий дрон ва робот технологиялари асосида периметр хавфсизлигини таъминлаш // “Инновация ва хавфсизлик тадқиқотлари” журналі. 2022. – 16(1). – Б. 44–51.
- [3] Wright A., Evans, D. Critical Infrastructure Surveillance Using AI-Powered Drones. Journal of Technological Innovations in Security, 2020. 14(2), 88–96. DOI: 10.1016/j.tis.2020.02.007.
- [4] Johnson P. M., Clarke E. D. Modern Challenges in Perimeter Security Integration. International Journal of Infrastructure Safety, 2021. 12(3), 129–143. DOI: 10.1016/j.iis.2021.06.005.
- [5] Smith J., Brown T. (). Advances in Perimeter Security for Critical Infrastructure Protection. Journal of Information Security and Cyber Defense, 2020.18(4), 233–245. DOI: 10.1016/j.iscd.2020.04.001.
- [6] Юлдошев Ф. Т. Электрон сигнализация тизимлари: муаммолар ва ечимлар. Ахборот технологиялари ва хавфсизлик илмий тадқиқотлари журналі, 2021. 25(2), 22–28.
- [7] Miller T., Robinson K. Enhancing Physical Barriers in Perimeter Protection. Physical Security and Barrier Systems, 2020. 10(3), 112–120. DOI: 10.1016/j.psbs.2020.07.008.
- [8] Ахмедов Д.Ш. Назорат камераларининг хавфсизлик тизимидаги роли ва уларни жойлаштириш стратегиялари. Ахборот ва технология хавфсизлиги тадқиқотлари журналі, 2020. 19(3), 35–42.
- [9] Саидов Х. М. Қўриқлаш хизматлари ва периметр ҳимоя тизимининг интеграцияси. Миллий хавфсизликда замонавий ёндашувлар журналі, 2021. 13(2), 27–33.
- [10] Gonzalez, L., & Patel, R. (2019). The Role of Sensors in Enhancing Perimeter Protection. Sensors and Actuators Journal, 45(6), 98–108. DOI: 10.1016/j.sensors.2019.03.012.
- [11] Раҳмонов З.Х. Ёритиш тизимларининг периметр хавфсизлигидаги аҳамияти. Техник хавфсизлик ва барқарорлик журналі, 2018. 8(1), 15–20.
- [12] Chen H., Zhao, Y. Integration of Lighting Systems in Perimeter Defense. Energy Efficient Security Systems, 2019. 8(4), 190–200. DOI: 10.1016/j.eess.2019.04.010.
- [13] Исмоилов Ш.Х. Ҳаракат сенсорлари ва уларнинг хавфсизлик тизимларидаги роли. Технология ва хавфсизлик назарияси журналі, 2019. 11(4), 33–39.
- [14] Ahmed S., Williams P. Drone and Robotic Solutions for Critical Infrastructure. International Robotics and Automation Review, 2018. 6(4), 301–310. DOI: 10.1016/j.irar.2018.11.005.
- [15] Li Y., Wu, Z. Strategic Integration of Perimeter Security Systems. Global Journal of Security Studies, 2022. 19(2), 89–99. DOI: 10.1016/j.gjss.2022.02.011.
- [16] Мухитдинова М.Х. Защита информации посредством искусственного интеллекта. Ёш олимлар ахборотномаси – Вестник молодых ученых – The bulletin of young scientists илмий журналі, 2020. 3 (4), 110–112.
- [17] Александров А. Защита периметра и «сеть без границ». Журнал сетевых решений/LAN", 2014. 207 (2), 79–92.
- [18] Yanjinkham Myagmar-Ochir, Wooseong Kim. A survey of video surveillance systems in smart city. Electronics журналі, 2023. 3567–3578.
- [19] Vinod Veeramachaneni, Integrating Zero Trust Principles into IAM for Enhanced Cloud Security, Harvard Business Review Press. 2024.7 (1), DOI:[10.5281/zenodo.14162091](https://doi.org/10.5281/zenodo.14162091).
- [20] Tripathi D., Singh L.K., Tripathi A.K., Chaturvedi A. (). An integrated approach of designing functionality with security for distributed cyber-physical systems. The journal of Supercomputing, 2022. 14813–14845.
- [21] Ледяев В.П. Обнаружение движущихся объектов с помощью компьютерного зрения и библиотеки OPENCV (2019). Экономика и социум" журналі, 12 (43), 1043–1047.

ТЕОРЕТИЧЕСКИЕ И ПРАКТИЧЕСКИЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ КОГЕРЕНТНЫХ СИГНАЛОВ В РАДИОЛОКАЦИИ

PhD, доцент Б.С.НУРМЕТОВ, З.Ё. АХМЕДОВ

Военный институт информационно коммуникационные технологии и связи МО РУз

Аннотация. В статье рассматриваются теоретические и практические аспекты использования когерентных сигналов в радиолокации. Представлены математические модели когерентных сигналов, методы измерения доплеровского сдвига, когерентная интеграция для повышения отношения сигнал/шум. Проведен сравнительный анализ когерентных и некогерентных методов обработки сигналов. Статья содержит научные факты и ссылки на авторитетные источники, что подтверждает важность когерентной обработки в современных радиолокационных системах.

Ключевые слова: амплитуда, когерентный сигнал, РЛС, эффективность фаз, чувствительность, импульс, согласование фаз.

Abstract. The article discusses theoretical and practical aspects of using coherent signals in radar. Mathematical models of coherent signals, methods for measuring the Doppler shift, and coherent integration for increasing the signal-to-noise ratio are presented. A comparative analysis of coherent and non-coherent signal processing methods is conducted. The article contains scientific facts and references to authoritative sources, which confirms the importance of coherent processing in modern radar systems.

Keywords: amplitude, coherent signal, radar, efficiency, phase, sensitivity pulse, phase matching.

Радиолокационные системы (РЛС) являются ключевыми средствами обнаружения, наведения и слежения. Эффективность РЛС напрямую зависит от способа обработки принимаемых сигналов. Когерентные сигналы, обладающие устойчивой фазовой связью между последовательными импульсами, позволяют проводить фазочувствительную обработку, что существенно расширяет функционал РЛС и улучшает точность измерений (Рис.-1).[1]

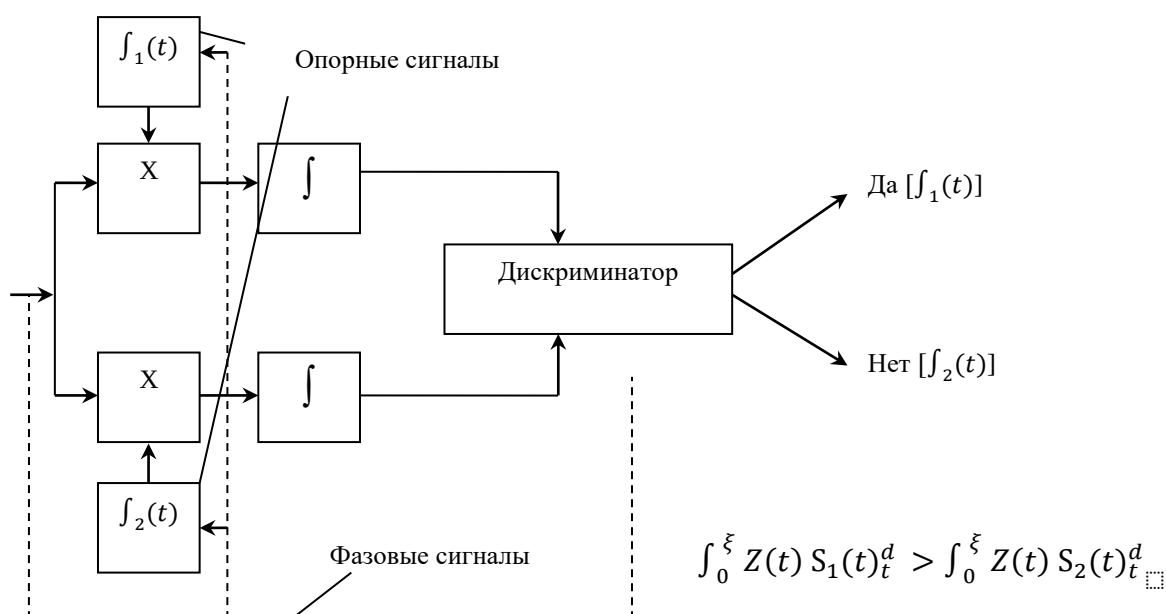


Рис.-1. Схема реализации оптимального приёма цифрового сигнала корреляторов при точных известных фазовых сигналах

Основы когерентных сигналов. Когерентность - означает согласованность фазовой структуры сигнала во времени. Сигнал считается когерентным, если его фаза сохраняется неизменной (или предсказуемой) на протяжении времени наблюдения Рис. -1.

Существует два основных типа когерентности:

Временная когерентность - устойчивость фазы сигнала во времени.

Пространственная когерентность - согласованность фаз в различных точках пространства (важно, например, для фазированных антенных решёток).

Для радиолокации особенно важна временная когерентность, так как она позволяет точно измерять доплеровское смещение и интегрировать сигналы на фоне шума. Которое является свойство сигнала, при котором его фаза сохраняет предсказуемую зависимость во времени. Когерентный радиолокационный сигнал описывается уравнением (1):

$$s(t)=A(t)\cos(2\pi f_0 t+\phi(t)) \quad (1)$$

где:

$A(t)$ - амплитудная огибающая,

f_0 - частота несущей,

$\phi(t)$ - фазовый сдвиг, изменяющийся плавно.

Сохранение когерентности обеспечивает возможность измерения фазовых изменений сигнала, связанных с движением цели [2].

В основном преимущества когерентных сигналов заключается в реализации сигналов и выглядят следующим образом:

Измерение доплеровского сдвига - позволяет определять скорость движения цели.

Когерентная интеграция - накопление эхо-сигналов от цели с сохранением фазы, что повышает соотношение сигнал/шум.

Формирование диаграммы направленности (beamforming) - используется в радарх с фазированной антенной решеткой.

Синтез апертуры (SAR/ISAR) - создание радиолокационного изображения с высоким разрешением.

Рассмотрим более широко применяемый метод, в радиолокации это доплеровский эффект на примере синтезированного апертурного радара.

SAR (Synthetic Aperture Radar)- Синтезированная апертура радара: это метод создания радиолокационных изображений с высоким разрешением, который позволяет получать детальные изображения объектов, даже если физический размер антенны радиолокатора невелик. Вместо использования физически большой антенны, SAR/ISAR использует движение антенны (в случае SAR) или движение объекта (в случае ISAR) для синтеза «Виртуальной» апертуры, эквивалентной значительно большей антенне.

Доплеровский эффект и измерение скорости. Отражённый от движущейся цели сигнал испытывает сдвиг частоты, описываемый формулой Доплера (2):

$$f_d=2v/\lambda \quad (2),$$

где:

v - скорость цели по направлению луча радара,

$\lambda=c/f_0$ - длина волны

c - скорость света.

Пример расчета:

Пусть $f_0=10$ ГГц, тогда $\lambda=0.03$ м.

Если цель движется со скоростью $v=150$ м/с, то

$$f_d=2 \cdot 150/0.03=10000 \text{ Гц}$$

Когерентность сигнала позволяет измерять доплеровский сдвиг с высокой точностью, что невозможно при некогерентной обработке [3].

Когерентная интеграция и повышение чувствительности

Для обнаружения слабых сигналов применяется когерентная интеграция - суммирование N последовательных импульсов с сохранением фазовой информации. Отношение сигнал/шум после интеграции увеличивается по формуле (3):

$$SNR_{инт} = SNR_{один} N \quad (3),$$

где $SNR_{один}$ - отношение сигнал/шум одного импульса.

Связь между временем задержки отражённого сигнала и дальностью цели:

$$R = c \cdot \tau / 2 \quad (4),$$

где:

R - дальность

$c \approx 3 \times 10^8$ м/с - скорость света

τ - задержка сигнала

Разрешение по дальности определяется длительностью импульса:

$$\Delta R = c \cdot \tau_p / 2 \quad (5),$$

где:

τ_p - длительность радиолокационного импульса.

Для повышения разрешения применяются линейные частотные модуляции (ЛЧМ).

1-таблица

Сравнительный анализ методов обработки сигналов

Параметр	Когерентная обработка	Некогерентная обработка	Да/нет
Измерение скорости цели			Да
Повышение отношения сигнал/шум при интеграции	Сохранение фазовой информации		Нет
Пропорционально N в корне		Низкая	Нет
Пропорционально N		Низкая	Нет
Сложность реализации	Высокая		Да
Чувствительность	Высокая		Да

Технические требования к когерентным РЛС

Для реализации когерентной обработки необходимо:

Высокостабильный генератор с низким фазовым шумом;

Система синхронизации фаз передатчика и приёмника;

Современные цифровые процессоры для обработки и компенсации фазовых ошибок [4,5].

Заключение: Когерентные сигналы - основа современных радиолокационных систем. Они обеспечивают возможность точного измерения доплеровского сдвига, увеличивают чувствительность и точность за счёт когерентной интеграции, а также расширяют функционал радаров благодаря фазочувствительной обработке.

Современные аппаратные решения и алгоритмы обработки продолжают совершенствовать методы сохранения и использования когерентности, что способствует развитию радиолокационных систем, а также позволяют точно определять параметры целей и существенно повышают чувствительность и разрешающую способность РЛС. Развитие

технологий синтеза частот, цифровой обработки сигналов и фазированной антенной решетки делает когерентные методы всё более важными в различных сферах.

Использование когерентных сигналов в радиолокации значительно расширяет возможности систем, позволяя точно измерять скорость и повышать чувствительность за счёт когерентной интеграции. Это требует усложнённой аппаратной реализации, однако современные технологии позволяют эффективно решать эти задачи.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

- [1] Skolnik, M. I. (2008). Radar Handbook (3rd ed.). McGraw-Hill.
- [2] Richards, M. A. (2014). Fundamentals of Radar Signal Processing. McGraw-Hill.
- [3] Oppenheim, A. V., & Schaffer, R. W. (2009). Discrete-Time Signal Processing (3rd ed.). Prentice Hall.
- [4] Kroupa, V. F. (1996). Handbook of Frequency Stability Analysis. NIST.
- [5] Doppler, C. (1842). Über das farbige Licht der Doppelsterne und einiger anderer Gestirne des Himmels. Abhandlungen der Königlich Böhmisches Gesellschaft der Wissenschaften.
- [6] Winzer P.J., Essiambre R.J. Advanced optical modulation formats // Proc. ECOC 2003. Rimini, 2003. Vol. 4. P. 1002.
- [7] Величко М.А., Наний О.Е., Сусьян А.А. Новые форматы модуляции в оптических системах связи // Lightwave Russian Edition. 2005. № 4. С. 21.

К ВОПРОСУ ЭКСПЕРИМЕНТАЛЬНОЙ ОЦЕНКИ РЕАЛЬНОЙ ПОМЕХОУСТОЙЧИВОСТИ ЛИНЕЙНЫХ ТРАКТОВ ЦИФРОВЫХ СИСТЕМ ПЕРЕДАЧИ МЕТОДАМИ НАТУРНЫХ ИСПЫТАНИЙ

к.т.н., доцент А.Я. НЕГРИЕНКО,

PhD, доцент Р.Ж. РАХМАТБАЕВ

*Научно-исследовательский институт изучения проблем обороны
и военной безопасности ВС РУ*

Аннотация. В статье раскрываются особенности оценки реальной помехоустойчивости цифровых систем передачи методами натурных испытаний. Рассмотрен метод сокращения времени измерений коэффициента ошибок с применением итерационной процедуры и использования априорной информации о потоке цифровых ошибок в линейных трактах.

Ключевые слова: цифровые системы передачи, цифровой линейный тракт, реальная помехоустойчивость, коэффициент ошибок, испытательные сигналы, параметрические функции, итерационная процедура.

Abstract. The article reveals the features of assessing the real noise immunity of digital transmission systems using field testing methods. A method for reducing the time of measuring the error rate using an iterative procedure and using a priori information about the flow of digital errors in linear paths is considered.

Key words: digital transmission systems, digital linear path, real noise immunity, error rate, test signals, parametric functions, iterative procedure.

В настоящее время при разработке цифровых систем передачи (ЦСП) значительное внимание уделяется созданию методики и средств для экспериментальной оценки параметров цифрового линейного тракта (ЦЛТ), определяющих его реальную помехоустойчивость. К этим параметрам в первую очередь относятся средняя вероятность ошибок, а также фазовое дрожание импульсов цифрового сигнала.

Вероятность ошибок в тракте оценивается частотой сбоев или коэффициентом ошибок Кош, среднеарифметическое значение которого для многоуровневого сигнала равно

$$K_{ош} = \rho_v \frac{m_v}{N_v}, \quad (1)$$

где m_v - количество ошибочных символов многоуровневого сигнала, выявленное за время передачи N_v символов многоуровневого сигнала, ρ_v - коэффициент, учитывающий вид преобразования исходного двоичного сигнала в многоуровневый.

Экспериментальная оценка реальной помехоустойчивости ЦЛТ методом натурных испытаний может проводиться с исследовательскими целями, в порядке текущего контроля, а также при регламентных работах, настройке и сдаче ЦЛТ в эксплуатацию.

При проведении испытаний с исследовательскими целями часто интересуются не только величиной вероятности ошибки и статистическими характеристиками (чаще всего эффективным значением) фазового дрожания, но и другими параметрами потока цифровых ошибок и фазовых флуктуаций (например, параметрами группирования ошибок, энергетическим спектром фазовых флуктуации и др.).

Измерения с целью текущего контроля, как правило, проводятся без перерыва связи, при передаче по тракту реальных сигналов.

Измерения, проводимые при регламентных работах, сдаче в эксплуатацию, а также измерения с исследовательскими целями проводятся с перерывом связи. При этом в исследуемый тракт посылается испытательный сигнал. На приемной стороне выявляются параметры, определяющие степень несоответствия переданного и принятого сигналов, Далее

с помощью специализированных устройств вычисляются параметры потока ошибок и (или) фазового дрожания. В простейших случаях определяется коэффициент ошибок и (или) эффективное значение фазового дрожания (дисперсия или пиковое значение).

Измерения с перерывом связи могут проводиться по двум схемам [1-3]:

тракт включается «шлейфом» - передающая и приемная части измерительного комплекса размещаются на одном конце тракта;

измерения проводятся «по направлению» - передающая и приемная части измерительного комплекса располагаются на разных концах тракта.

Рассмотрим особенности методов измерения коэффициента ошибок при передаче по тракту реальных и испытательных сигналов. Методы оценки вероятности ошибок при передаче реальных цифровых сигналов основаны на использовании информационной избыточности этих сигналов. Приборы, использующие эти методы, часто оформляются в виде встроенных блоков контроля регенераторов.

Чаще всего осуществляется слежение за текущей цифровой суммой (ТЦС) линейного сигнала. В частном случае при использовании кода с чередованием полярности импульсов (кода с ЧПИ) производится обнаружение нарушений чередования полярностей импульсов. Сложность таких устройств зависит от типа линейного кода. Оценка вероятности ошибок при передаче по тракту реальных сигналов неизбежно связана с появлением методической погрешности, обусловленной принятым методом выявления ошибок. Текущий контроль вероятности ошибок при передаче реальных сигналов может проводиться также по синхрогруппам, путем проверки на четность и специально вводимым в информационный сигнал символам [3].

При оценке вероятности ошибок и других характеристик потока ошибок с перерывом связи выявление ошибочно принятых символов испытательного сигнала чаще всего производится путем посимвольного сравнения последовательности, прошедшей через испытуемый тракт, с эталонной последовательностью [1,2]. Устройства, реализующие метод посимвольного сравнения, требуют жесткой тактовой и цикловой синхронизации сравниваемых сигналов.

Достоверность результатов измерений во многом зависит от выбора длительности сеанса измерений. Верхняя граница длительности сеанса измерений ограничивается временем, в течение которого условия работы тракта можно считать стационарными. При превышении этого времени может возникнуть ошибка смещения оценки, обусловленная изменением измеряемого параметра во времени. Нижняя граница сеанса измерений определяется требуемой точностью и надежностью полученного в результате измерений коэффициента ошибок. Под точностью оценки понимают доверительный интервал $K_{ош}-\lambda_1 P$, $K_{ош}+\lambda_2 P$, в котором может быть заключено истинное значение вероятности ошибок, где коэффициенты $\lambda_1 > 0$, $\lambda_2 > 0$ характеризуют относительную погрешность измерений. Надежностью оценки (доверительной вероятностью) называют вероятность β , с которой доверительный интервал накрывает истинное значение оцениваемого параметра [5].

Исходя из заданных значений доверительной вероятности и границ доверительного интервала можно составить неравенство

$$P\left\{\left(1-\lambda_1 P \leq \frac{m}{N} \leq (1+\lambda_2 P)\right)\right\} \geq \beta \quad (2)$$

которое использовать далее для определения числа опытов (количества символов тест - сигнала) N . Тогда требуемая длительность сеанса измерений

$$T_{изм} = \frac{N}{F_T}, \quad (3)$$

где F_T - тактовая частота.

При неизвестном законе распределения ошибок грубую оценку N можно получить с помощью неравенства Чебышева [5], однако она может оказаться чрезмерно

преувеличенной. При достаточно большом числе фиксируемых в процессе измерений ошибок ($m > 10$) количество символов N в реализации испытательного сигнала можно определить исходя из нормального приближения закона распределения числа ошибок согласно выражению

$$N \geq t_{\beta}^2 \sigma_0^2 / \varepsilon_{\beta}^2, \quad (4)$$

где $t_{\beta} = F^{-1}\left(\frac{1+\beta}{2}\right)$, $F^{-1}(x)$ - функция, обратная $F(x)$,

$$F(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{t^2}{2}} dt \quad - \text{нормальный интеграл вероятностей,}$$

ε_{β} - ширина доверительного интервала, σ_0 - дисперсия предполагаемого или полученного экспериментальным путем закона распределения ошибок.

При малых значениях вероятности ошибки время измерений для получения приемлемой достоверности результатов может оказаться чрезмерно большим. Рассмотрим один из возможных путей сокращения времени измерений без снижения достоверности получаемых результатов измерений.

Как показано в [4], среднеарифметическая оценка математического ожидания (м.о.) случайного процесса может быть уточнена с помощью параметрических функций, выражаемых через коэффициент вариации $K_{\sigma} = \sigma/Z$, где σ - среднеквадратическое отклонение, Z - м.о. оцениваемого параметра. При измерениях коэффициента ошибок оценка вероятности ошибок, уточненная с помощью мультипликативной параметрической функции $K = (1 + K_{\sigma}^2/N)^{-1}$, полученной из условия минимума среднеквадратической ошибки, где $K_{\sigma} = \sqrt{p(1-p)/p}$, имеет вид

$$K_{\text{ош}_{\lambda}} = m \left(N + \frac{1-P}{P} \right)^{-1}, \quad (5)$$

откуда видно, что априорная информация относительно вероятности ошибок P может быть использована для повышения точности оценки при выбранном числе испытаний, либо для сокращения времени измерений.

Пусть измерения проводятся с использованием итерационной процедуры [6]

$$K_i = K_{i-1} + \frac{1}{i} (K_{qi} - K_{i-1}), \quad (6)$$

где K_i - «долговременный» коэффициент ошибок, определенный за время от момента начала измерений до момента окончания i -го интервала счета ($i = 1, 2, \dots$), включающего в себя передачу $q > 1$ символов тест-сигнала; K_{qi} - частный коэффициент ошибок в i -м интервале счета, среднеарифметическое значение которого

$$K_{qi} = \frac{m_i}{q}, \quad (7)$$

где m_i - количество выявленных ошибок в i -м интервале счета.

Выберем значение q достаточно большим и разобьем каждый интервал счета на два равных подинтервала. Тогда для частного значения коэффициента ошибок можно записать следующие оценки с использованием параметрических функций:

$$K_{qi_1} = 2m_{i_1} \left(q + 2 \frac{1-k_1}{k_1} \right)^{-1}, \quad (8)$$

$$K_{qi_2} = 2m_{i_2} \left(q + 2 \frac{1-k_2}{k_2} \right)^{-1}, \quad (9)$$

где $k_1 = 2m_{i_1}/q$, $k_2 = 2m_{i_2}/q$, $m_{i_1} + m_{i_2} = m_i$

Сравним точность оценок (7), (8), (9), воспользовавшись выражением погрешности измерений, приближенно равной

$$\Delta K \approx t_{\beta} \sqrt{\frac{K_{\text{ош}}(1-K_{\text{ош}})}{q}}, \quad (10)$$

Обозначая $m_i / m_i = \alpha_i$ и подставляя в (10) выражения (7), (8), (9) с учетом того, что реально $K_{\text{ош}} < I$, получим

$$\Delta K_i \approx t_{\beta} m_i^{\mu/q}, \quad (11)$$

где

$$\mu = \begin{cases} 1/\sqrt{m_i}, & K_{\text{ош}} = K_{q_i} \\ \sqrt{\frac{2\alpha_i(1-\alpha_i)}{1+\alpha_i m_i}}, & K_{\text{ош}} = K_{q_{i_1}} \\ \sqrt{\frac{2\alpha_i(1-\alpha_i)}{1+(1-\alpha_i)m_i}}, & K_{\text{ош}} = K_{q_{i_2}} \end{cases}$$

Отсюда видно, что погрешность измерений в случае использования оценок (8) и (9) зависит от α_i , т.е. от неравномерности возникновения ошибок во времени. При достаточно большом числе фиксируемых ошибок и $\alpha_i = 0,5$ оценки (7), (8), (9) практически совпадают. При $\alpha_i > 0,5$ более точной является оценка (8), при $\alpha_i < 0,5$ - оценка (9). Например, при регистрации за интервал измерений 30 ошибок и при $\alpha_i = 1/3$ погрешность оценки (9) меньше погрешности оценки (7) на 20%. Таким образом, выбирая в каждом интервале счета более точную оценку - (8) или (9) в зависимости от α_i в качестве частного значения коэффициента ошибок K_{q_i} , можно добиться сокращения времени измерений. Полагая, что измерения должны быть прекращены по достижении одной и той же погрешности при использовании среднеарифметического коэффициента ошибок и оценок, уточненных с использованием параметрических функций, и считая, что значение α остается приблизительно постоянным в любом из интервалов счета, можно получить следующее выражение коэффициента выигрыша интервалов счета (времени измерений):

$$\lambda = \sqrt{(1+y)/2\alpha(1-\alpha)}, \quad (12)$$

где $y = \begin{cases} \alpha, & \alpha < 0,5 \\ 1-\alpha, & \alpha > 0,5 \end{cases}$

Допустим, $m=100$ и $\alpha=0,3$. Тогда имеем $\lambda=1,3$, то есть для проверки аппаратуры потребуется на 30% времени меньше.

Если предполагаемая вероятность ошибок значительно меньше, например, 10^{-6} (что характерно для телефонии), то измерения могут быть прекращены по достижении допустимого времени, отведенного для испытаний.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

- [1] Измерения коэффициента ошибок в цифровых каналах связи - Режим доступа: <https://cyberleninka.ru> – Дата обращения: 12.04.2025.
- [2] Измерения в цифровых системах связи - Режим доступа: <https://toologs.ru> - Дата обращения: 18.03.2025.
- [3] Измерение коэффициента ошибок – Режим доступа: <https://sibleg.ru> - Дата обращения: 25.12.2024.
- [4] Романенко, А.Ф. Аппроксимативные методы анализа случайных процессов./ А.Ф. Романенко, Г.А. Сергеев. – М.: Энергия. – 1974. – 176 с.
- [5] Гнеденко, Б.В. Курс теории вероятностей. / Б.В. Гнеденко – М.: Наука.–1965.–412 с.
- [6] А.С. 978368. Способ измерения коэффициента ошибок по импульсам и устройство для его осуществления/ Авт.: В.С. Балан, М.С. Гроссман, В.Э. Гуревич, А.Я. Негриенко – опубл. в БИ, 1982. - №44.

ОПЫТ ПРИМЕНЕНИЯ ГИС В ВОЕННОМ ДЕЛЕ

*к.т.н., доцент Н.А. КАЮМОВ**Управления Навигационно-геоинформационного обеспечения ГШ ВС РФ*

Аннотация. В статье представлен обзор геоинформационных систем, используемых в вооружённых силах различных государств, включая их функциональные возможности. Рассмотрены преимущества и недостатки использования ГИС ВН. Сделан вывод о необходимости дальнейшего развития и внедрения ГИС-технологий в военное дело с целью повышения эффективности управления войсками и оперативного принятия решений.

Ключевые слова: геоинформационные системы военного назначения, геопространственная информация, электронные топографические карты, автоматизированные системы управления.

В последнее время в современном обществе в целом активно внедряются информационные технологии, чему способствовало их мощное развитие последние десятилетия. Бурное развитие информационных технологий и их использования в ведущих армиях вызывает необходимость разработки специальных программных аппаратных средств позволяющих обрабатывать цифровую информацию о местности (окружающей среде) во взаимосвязи с различными геопространственными данными о противнике и своих войсках. Одними из таких средств являются геоинформационные системы военного назначения (ГИС ВН), представляющие собой программно-аппаратные комплексы, которые предназначены для сбора, обработки, хранения, анализа, моделирования и наглядного отображения геопространственной информации, необходимой для поддержки принятия решений по управлению войсками в мирное и военное время, а также создания цифровых (электронных) карт и выполнения военно-прикладных (расчетных) задач, связанных с оценкой оперативно-тактических свойств местности и планированием применения сил (средств) [1]. Современные армии активно внедряют ГИС ВН, оснащая войска современным программно-аппаратными комплексами. ГИС ВН становятся неотъемлемой частью автоматизированных систем управления войсками и оружием.

ГИС военного назначения – функционально-ориентированная ГИС для решения задач военного назначения, укомплектовывается ГИС-приложениями, решающими военно-прикладные задачи, предназначена для поддержки принятия решения, планирования боевых действий войск и мероприятий обеспечения в автоматизированных системах управления войсками и оружием [2]. ГИС ВН позволяют преобразовывать и представлять большие объёмы разнообразной координатно-временной информации в виде, удобном для использования органами военного управления (ОВУ) в процессе управления войсками.

Проведем краткий анализ имеющихся ГИС ВН в различных армиях мира:

В Российской Федерации в настоящее время приняты на вооружение два комплекса ГИС: «Интеграция» (приказ МО РФ № 750 от 22.07.2009 г.) и «Оператор» (приказ МО РФ № 598 от 15 августа 2013 года), которые работают в различных операционных системах, таких как Windows, Linux, MCBC. [1]

Наибольшую популярность в войсках и органах военного управления Вооружённых силах РФ получила ГИС «Оператор» [3], основные функции которой приведены на рис. 1. ГИС «Оператор» является разработкой конструкторского бюро «Панорама».

ГИС ВН «Оператор» в вооружённых силах РФ используется в основном для [4]

топогеодезического и навигационного обеспечения войск средствами топогеодезической информации, автоматизации учета и хранения данных, расчета запасов карт;



Рис. 1. Основные функции ГИС «Оператор»

ведения дежурных и оперативных карт и схем, автоматизации формирования графических документов;

инструментального информационного обеспечения учений и командно-штабных тренировок;

автоматизации процессов управления войсками, обеспечение развития концепции сетецентрических войн;

объемного моделирования местности оперативной обстановки, создание пространственных (виртуальных) макетов местности;

информационного обеспечения боевого применения высокоточного оружия;

оперативный поиск и обеспечение картографическими материалами на требуемый район;

анализа и прогнозирования оперативной (тактической) обстановки;

информационного обеспечения принятия оперативных решений;

обработки, визуального анализа тематических справочных данных, формирование наглядных графических документов с использованием цифровой картографической основы, автоматизированная обработка и отображение данных, результатов расчетов и прогнозов;

бортовой навигации и диспетчерского сопровождения транспортных средств.



Рис. 2. Информационное обеспечение с помощью ГИС «Оператор» учений и командно-штабных тренировок

ГИС «Оператор» активно применялась [5]:

в Сирийской Арабской Республике;

в Трехсторонней контактной группе по Украине;

в Турции и Иране при урегулировании конфликта на Ближнем Востоке;

в ходе специальных учений от тактического уровня звена до стратегического (рис.2);

при ликвидации последствий чрезвычайных ситуаций в Сибири и на дальнем Востоке.

В Вооруженных Сил Республики Беларусь на вооружение принят программно-информационный комплекс поддержки принятия решений на основе геоинформационных систем военного назначения модернизированный (ПИК ГИС-ВН-2М). Данная ГИС является отечественным продуктом разработанная Объединенным институтом проблем информатики Национальной академии наук Беларуси (Рис. 3). Данная ГИС предназначена для использования в органах управления штабами оперативного и тактического звена Вооруженных Сил Республики Беларусь при подготовке данных для принятия оперативных решений на проведение операций и применение оружия [6].



Рис. 3. Демонстрация ГИС-ВН-2М в XII Международной выставке вооружения и военной техники MILEX-2025

ПИК ГИС-ВН-2М является базовым комплексом для создания геоинформационных систем военного назначения в части нанесения, моделирования и анализа оперативно-тактической обстановки, решения оперативно-тактических задач на местности с использованием электронных карт местности. Он обеспечивает интеграцию, унифицированное представление, обработку, отображение и документирование разнородных данных, в том числе геопространственных и данных оперативной обстановки, необходимых должностным лицам органов военного управления для оценки обстановки и принятия решений по управлению силами (средствами).

В армиях США и стран НАТО на вооружении стоит ГИС «ArcGIS».

ArcGIS – это мощная ГИС, разработанная американской компанией Esri (Environmental Systems Research Institute). Она предназначена для сбора, хранения, анализа, визуализации и интерпретации географической информации [7]. ArcGIS широко используется в самых

разных областях – от градостроительства и экологии до обороны и военных операций. Применение ArcGIS вооружёнными силами США и стран НАТО в вооружённых конфликтах является важной составляющей в современных военных операциях.

Так, например во время службы на авиабазе Баграм в Афганистане аналитик Джон Берри использовал ArcGIS для быстрого решения тактической задачи: определить возможные точки запуска вражеских ракет [8]. С помощью инструмента Multiple Ring Buffer он создал концентрические буферы радиусом примерно 8 км для 107 мм ракеты и 20 км для 122 мм ракеты (Рис. 4), что позволило визуализировать возможные зоны запуска. С помощью инструментов пространственного анализа были определены безопасные маршруты, зоны повышенной угрозы и возможные пути обхода.

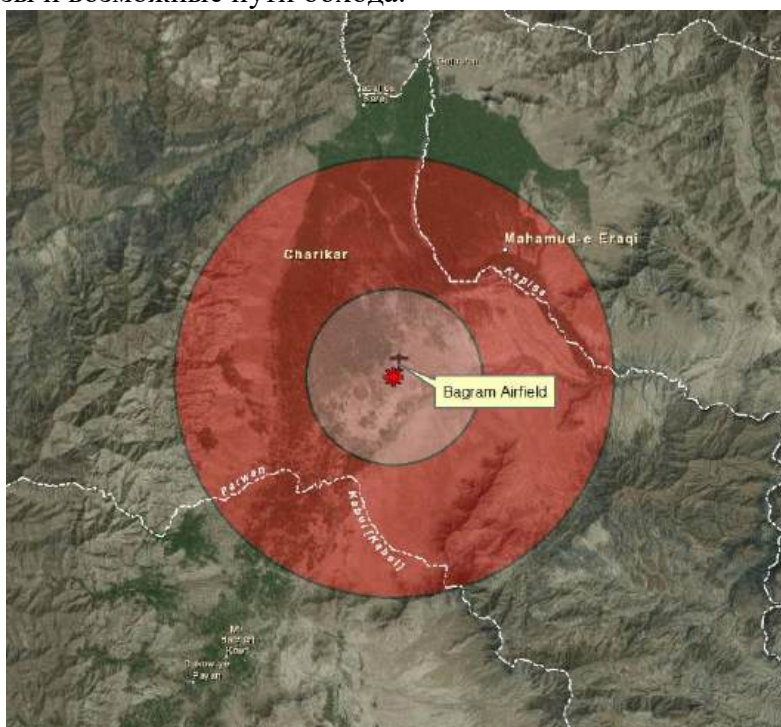


Рис. 4 Кольца дальности, созданные с помощью инструмента Multiple Ring Buffer

Одними из ключевыми направлениями применения ArcGIS в вооружённых конфликтах приведены в таблице 1.

Таблица 1

Ключевые направления применения ArcGIS в вооружённых конфликтах

№	Направление применения	Краткое описание
1.	Планирование и управление операциями	Построение 3D-карт, анализ рельефа, определение маршрутов передвижения и логистики.
2.	Поддержка разведки и анализа обстановки	Сбор, визуализация и анализ разведывательных данных, выявление угроз и уязвимых мест.
3.	Командование, контроль и связь (C4ISR)	Объединение данных на единой карте для поддержки ситуационной осведомлённости и принятия решений.
4.	Тактическое управление и навигация	Поддержка боевых подразделений в реальном времени, навигация на местности, обновление боевой обстановки.
5.	Гуманитарные операции	Оценка ущерба, планирование эвакуации, доставка помощи, картографирование зон бедствий.
6.	Интеграция с другими системами	Связь с системами управления боем, БПЛА, сенсорами и базами данных для комплексного анализа.

Преимущества и недостатки применения геоинформационных систем военного назначения

ГИС ВН играют ключевую роль в обеспечении топогеодезической и навигационной поддержки войск, а также в автоматизации процессов принятия решений в условиях сложной оперативной обстановки. Рассмотрим основные преимущества и недостатки использования ГИС военного назначения (ГИС ВН).

Преимущества:

Оперативность и обоснованность управленческих решений.

ГИС ВН позволяют в реальном времени анализировать пространственную и оперативную обстановку, тем самым повышая скорость и обоснованность принятия командных решений на различных уровнях управления.

Интеграция многокомпонентных данных.

Системы обеспечивают объединение и согласование разнородных данных (картографических, разведывательных, метеорологических, навигационных и др.) в едином информационном пространстве.

Наглядность и визуализация боевой обстановки.

Цифровое картографирование, визуальное отображение позиций войск, объектов инфраструктуры и маршрутов способствует более точному восприятию ситуации и принятию решений.

Функции моделирования и прогнозирования.

Возможности ГИС ВН включают сценарное моделирование развития обстановки, расчёт возможных направлений манёвра, зон поражения и оценки рисков.

Автоматизация топогеодезического обеспечения.

Использование ГИС ВН позволяет автоматизировать процессы создания и обновления цифровых карт, расчёта координат, построения маршрутов и определения геопространственных характеристик местности.

Интеграция с автоматизированными системами управления (АСУ).

ГИС ВН легко интегрируются в структуру АСУ, взаимодействуют с системами спутниковой навигации, беспилотными летательными аппаратами (БПЛА), средствами разведки и связи.

Недостатки:

Техническая зависимость.

Эффективное функционирование ГИС требует наличия вычислительных ресурсов, стабильного электропитания, защищённых каналов связи и серверной инфраструктуры.

Уязвимость к внешним воздействиям.

Системы подвержены угрозам со стороны кибератак, радиоэлектронного подавления (РЭБ), вмешательства в сигналы спутниковой навигации и другим формам информационного воздействия.

Сложность внедрения и сопровождения.

Необходимость наличия квалифицированного персонала, проведение технического и методического сопровождения, а также высокая стоимость оборудования и лицензий могут стать ограничивающими факторами.

Проблема актуальности данных.

Эффективность ГИС ВН во многом определяется своевременностью и достоверностью вводимой информации. Использование устаревших или непроверенных данных может привести к ошибкам в управлении.

Технологическая зависимость от разработчиков программного обеспечения.

В случае применения коммерческих (особенно зарубежных) решений существует риск технологической зависимости, ограничения доступа к обновлениям и возможное отключение в условиях санкционного давления.

Ограничения при использовании в полевых условиях.

Развёртывание и эксплуатация ГИС ВН в условиях активных боевых действий, ограниченного доступа к сети и дефицита ресурсов может быть затруднено или ограничено.

Вывод

Анализ опыта применения геоинформационных систем (ГИС) в военной сфере свидетельствует о высокой эффективности данных технологий в решении широкого круга задач, связанных с планированием, управлением и обеспечением боевых действий. ГИС позволяют существенно повысить точность и оперативность топогеодезического обеспечения, улучшить пространственный анализ, визуализацию оперативной обстановки и принятие обоснованных решений в реальном времени. Особое значение имеет интеграция ГИС с другими информационными системами и средствами автоматизации управления войсками, что открывает новые возможности для комплексной цифровизации процессов военного управления. Вместе с тем, успешное внедрение и использование ГИС требует наличия квалифицированных кадров, устойчивой инфраструктуры и соблюдения стандартов совместимости. Полученные результаты подтверждают актуальность и перспективность дальнейшего развития и совершенствования геоинформационных технологий в интересах национальной обороны и безопасности.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

[1] Осипов Г.К., Алексеев А.В. Концептуальная модель геоинформационной системы военного назначения. Труды Военно-космической академии имени А.Ф. Можайского. Выпуск 647, 2015. С.109 – 114.

[2] Мисьник С.И. Применение ГИС военного назначения. Геоинформационные системы военного назначения: теория и практика применения [Электронный ресурс] : материалы IX Респ. науч.-практ. конф., Минск: БГУ, 2023. С 73 – 76.

[3] Иванов В.К., Титов И., Морозов Д. Создание баз данных в ГИС «Оператор» для формирования интегрированной электронной карты. САПР и графика. 2019 №3. С. 4 – 12

[4] Описание применения Геоинформационной системы военного назначения «Оператор». – М.: Панорама, 2012. Официальный сайт <http://www.gisinfo.ru>.

[5] Долгов Е.И., Банин И.В. О становлении геоинформационных систем военного назначения и перспективах их дальнейшего развития // Военная Мысль. 2022. № 6. С. 79 – 85

[6] Богданов А. О., Кричевцов М. И., Черенко А. С. Автоматизированное составление специальных карт в СПО ПИК «ГИС-ВН-2М». ГИС-технологии в науках о Земле [Электронный ресурс], Минск: Минск : БГУ, 2025. С 30 – 35.

[7] GIS for Defense and Intelligence. <https://www.esri.com/~media/files/pdfs/library/brochures/pdfs/gis-for-defense.pdf>

[8] John Berry. Under Fire, Analyst Turns to GIS. <https://www.esri.com/about/newsroom/arcwatch/under-fire-analyst-turns-to-gis..>

**HARBIYLARGA XORIJIY TILLARNI O'QITISH JARAYONIDA KOMMUNIKATIV
KO'NIKMALARINI RIVOJLANTIRISHNING AHAMIYATI (INGLIZ TILI MISOLIDA)****DSc, professor D.A. ABDURAXIMOVA***O'zbekiston Respublikasi Qurolli Kuchlari Akademiyasi***A.A. UBAYDULLAYEVA***O'zbekiston Respublikasi Qurolli Kuchlari Tinchlik yo'lida hamkorlik markazi*

Annotatsiya. Maqolada talabalarni ingliz tilida muloqot qilish ko'nikmalarini shakllantirish, axborotlarni tahlil qilish va kundalik hayotda qo'llash qobiliyatlarini rivojlantirish zarurligi ta'kidlanadi. Harbiy ta'lim yo'nalishlarida ingliz tilidagi matnlarni tahlil qilish madaniy va lingvistik kompetensiyani belgilashda muhim ahamiyatga ega. Maqola, shuningdek, kommunikativ kompetensiya tushunchasini kengaytiradi, uning nazariy va amaliy jihatlarini o'rganadi hamda talabalar uchun zarur bo'lgan ko'nikmalarni rivojlantirishda metodologik yondashuvlarning ahamiyatini ta'kidlaydi. Kompetensiya va kompetentlik tushunchalari o'zaro bog'liq bo'lib, ularning to'g'ri tushunilishi va qo'llanilishi talabalarni muvaffaqiyatli tayyorlashda muhim rol o'ynaydi. Shu bilan birga, ingliz tilini o'rganayotgan talabalarning madaniy o'ziga xosliklar haqida bilimga ega bo'lishi tilni o'zlashtirish jarayonida muhim ahamiyat kasb etadi. Maqola xorijiy tillarni o'qitish jarayonida kommunikativ kompetensiyani rivojlantirishning didaktik asoslarini chuqur tahlil qiladi va zamonaviy ta'lim tizimida bu jarayonning ahamiyatini yoritadi.

Kalit so'zlar: harbiy ta'lim yo'nalishi, til ko'nikmlari, kompetensiya, kompetentlik, madaniy kompetensiya, lingvistik kompetensiya, kommunikativ kompetensiya.

Аннотация. В статье подчеркивается необходимость развития у студентов навыков общения на английском языке, анализа информации и ее применения в повседневной жизни. В военном образовании анализ английских текстов важен для определения культурной и языковой компетентности. В статье также расширяется понятие коммуникативной компетентности, исследуются ее теоретические и практические аспекты, подчеркивается важность методических подходов в формировании необходимых студентам умений. Понятия компетентности и компетенции взаимосвязаны, а их правильное понимание и применение играют важную роль в успешной подготовке студентов. В то же время знание культурных различий среди студентов, изучающих английский язык, важно в процессе овладения языком. В статье дается глубокий анализ дидактических основ формирования коммуникативной компетентности в процессе обучения иностранным языкам и подчеркивается важность этого процесса в современной системе образования.

Ключевые слова: военное образование, языковые навыки, компетентность, компетенция, культурная компетентность, языковая компетентность, коммуникативная компетентность.

Abstract. The article emphasizes the need to develop students' communication skills in English, their ability to analyze information and apply it in everyday life. In military education, the analysis of English texts is important in determining cultural and linguistic competence. The article also expands the concept of communicative competence, studies its theoretical and practical aspects, and emphasizes the importance of methodological approaches in developing the skills necessary for students. The concepts of competence and competency are interrelated, and their correct understanding and application play an important role in the successful preparation of students. At the same time, the knowledge of cultural characteristics of students learning English is of great importance in the process of language acquisition. The article deeply analyzes the didactic foundations of the development of communicative competence in the process of teaching foreign languages and highlights the importance of this process in the modern education system.

Keywords: military education, language skills, competency, competence, cultural competence, linguistic competence, communicative competence.

O'zbekiston Respublikasining mustaqillikka erishishi natijasida ta'lim tizimi tub islohotlardan o'tdi va xorijiy tillarni o'rganish milliy rivojlanish strategiyasining muhim yo'nalishlaridan biriga aylandi. "Ta'lim to'g'risida"gi qonunda uzluksiz ta'lim tizimidagi barcha islohotlar doirasida chet tillarni o'qitish ustuvor vazifa sifatida belgilandi. Bu esa mamlakatimizda raqobatbardosh kadrlar tayyorlash tizimini mustahkamlashga xizmat qiladi.

Jahon hamjamiyatida O'zbekiston ilm-fanining o'rnini yuqori darajaga ko'tarish maqsadida ingliz tilida muloqot qilish ko'nikmalarini shakllantirish belgilangan. Talabalar ingliz tilidagi axborotlarni izlab topish, tahlil qilish va zarur bilimlarni egallash uchun materiallarni ajratib olish, shuningdek, ularni kundalik hayotda qo'llay olish qobiliyatlarini rivojlantirishlari kerak.

Harbiy ta'lim yo'nalishlarida ingliz tilida bayon etilgan matnlarning tahlili real, madaniy va til kompetensiyasining darajalarini belgilashda muhim ahamiyatga ega. Talabalarning muloqot madaniyatini shakllantirish, o'qish jarayonida oldin egallagan ijtimoiy, madaniy, lingvistik va emotsional tajribalardan samarali foydalanish zarur. Ingliz tilida muloqot qilishda nafaqat lingvistik, balki nutqiy va madaniy malakalarni rivojlantirish ham muhimdir.

M.A. Ivanovning fikriga ko'ra, professional bilim, ko'nikma va malakalarning mavjudligi, intellektual o'rganuvchanlik qobiliyati, aqliy mehnat qila olish va hamkorlikda ishlash kabi komponentlar zamonaviy mutaxassis tayyorlashda muhim ahamiyatga ega [1]. Oliy harbiy ta'lim muassasasining asosiy maqsadi xalqaro standartlarga muvofiq yuqori malakali, kreativ va tizimli fikrlaydigan kadrlar tayyorlash hamda yoshlarning intellektual qobiliyatlarini rivojlantirishdan iboratdir.

Kompetensiya - bu nazariy bilimlar, ko'nikmalar va malakalar asosida amaliy faoliyatni yo'naltiruvchi umumiy jarayon. U shaxsning umumiy tayyorgarligini va faoliyatga tayyorligini ifodalaydi. Boshqacha aytganda, kompetensiya - bu kishi o'z bilimlarini va ko'nikmalarini qanday qilib amaliyotda qo'llay olishidir.

Kompetentlik esa, egallangan nazariy bilimlarni amaliyotda qo'llash qobiliyatini anglatadi. Bu har bir shaxsning individual xususiyatlari, tajribasi va shaxsiy qobiliyatlari bilan bog'liq bo'lgan faoliyatdir. Demak, kompetentlik shaxsning o'ziga xos xususiyatlariga bog'liq holda o'z bilimlarini amaliyotda qo'llash darajasini belgilaydi.

XX asrning 70-90 yillarida xorijiy tillarda kommunikativ kompetensiyaning bir nechta modellari ishlab chiqilgan. Bu jarayonda ko'plab xorijiy pedagog olimlar, jumladan Jennifer Wilkins, A.Xarding, P.Hartman va boshqalar, o'z tadqiqotlari orqali kommunikativ kompetensiyaning nazariy va amaliy jihatlarini o'rganishgan. Ularning ishlarida chet tillarni o'rganishda muloqotdagi muammolarni hal etishga qaratilgan yondashuvlar keltirilgan.

Dell Hymes tomonidan kiritilgan "kommunikativ kompetensiya" atamasi esa til bilishning faqat grammatik jihatlari bilan cheklanmay, balki ijtimoiy vaziyatlarda qanday qilib o'z bilimlarini qo'llay olishini ham ko'rsatadi. Bu o'z navbatida, til ta'limida kommunikativ kompetensiyalarini shakllantirishga qaratilgan metodologik yondashuvlarning ahamiyatini oshiradi. Maykl Kanale va Merril Swain tomonidan ilgari surilgan tadqiqotlar esa kommunikativ kompetensiyaning tarkibiy qismlarini - grammatik, sotsiolingvistik va strategik kompetensiyalarni ajratib ko'rsatadi. Bu yondashuvlar til o'rganish jarayonida talabalar uchun zarur bo'lgan ko'nikmalarni rivojlantirishda muhim rol o'ynaydi. Shunday qilib, "kompetensiya" va "kompetentlik" atamaları til ta'limi va kommunikativ kompetensiyani rivojlantirishda muhim tushunchalar bo'lib, ularning to'g'ri tushunilishi va qo'llanilishi talabalarni muvaffaqiyatli tayyorlashda katta ahamiyatga ega.

Ingliz tilini o'rganayotgan talabalarning madaniy o'ziga xosliklar haqida bilimga ega bo'lishi, ularning tilni o'zlashtirish jarayonida muhim ahamiyatga ega. Madaniyat va til o'rtasidagi bog'liqlik, talabalarga nafaqat tilni, balki uning kontekstini ham tushunishga yordam beradi. Bu esa nazariy bilimlarni amaliyotda qo'llay olish imkoniyatini oshiradi.

Talabalarning til bo'yicha olgan bilimlarini amaliyot bilan bog'lash, ularning nutqiy malakalarini rivojlantirishda muhim rol o'ynaydi. Masalan, talaffuz qoidolari yoki urg'u haqida

berilgan bilimlar, agar amaliy mashg'ulotlar bilan birlashtirilmasa, samarali bo'lmaydi. Talabalar o'zlashtirgan nazariy bilimlarini amaliyotda qo'llay olmasalar, bu bilimlar malakaga aylanishi qiyinlashadi. Xelsinki universiteti professori Yarko Lampiselkining fikriga ko'ra, XXI asr ko'nikmalari yaratuvchanlik, innovatsiyalar, tanqidiy fikrlash va muammoni yechish kabi qobiliyatlarni o'z ichiga oladi. Ushbu ko'nikmalar talabalarni raqobatbardosh kadr sifatida tayyorlashda muhimdir. Shuning uchun ta'lim jarayonida kompetentlikni rivojlantirishga yo'naltirilgan yondashuvlar zarur.

Umuman olganda, ingliz tilini o'rganishda faqatgina nazariy bilimlarni berish bilan cheklanmaslik kerak. Amaliyot va madaniyatni birlashtirgan holda ta'lim berish, talabalarni nafaqat tilni biluvchi, balki uni samarali qo'llay oladigan mutaxassislar sifatida tayyorlashga yordam beradi. Bu esa ularga global muhitda muvaffaqiyatli faoliyat yuritish imkonini beradi.

Tinglovchilar o'z kasbiy sohasida raqobatbardosh bo'lishi uchun yaratuvchanlik, innovatsiyalar, tanqidiy fikrlash, muammoni hal qilish va qaror qabul qilish kabi ko'nikmalarni rivojlantirishlari zarur. M.R. Kadirova zamonaviy pedagogik texnologiyalar orqali ingliz tilini o'qitish talabalarning ijodiy faolligini oshirish, kasbiy ko'nikmalarini shakllantirish va ilmiy-texnik qobiliyatlarini rivojlantirishga yordam berishini ta'kidlaydi [11]. Ta'lim jarayonining mazmunini yangilash ham muhim ahamiyatga ega. Ingliz tilini o'rganish jarayonida lingvistik kompetensiyani shakllantirish masalasi alohida e'tiborga loyiqdir. Lingvistik kompetensiya ingliz tilini o'qitish metodikasida til kompetensiyasi atamasi bilan sinonim sifatida ishlatiladi va nutqiy faoliyatda ko'nikma va malakalarni namoyon qiladi.

Kommunikativ kompetensiyalarga turli yondashuvlar mavjud. Amerikancha yondashuvda kompetensiyalar xodimlarning xulq-atvorini aks ettiradi, ya'ni zarur ko'nikma va bilimlarga ega bo'lgan xodim yaxshi natijalar ko'rsatadi. Yevropacha yondashuv esa kompetensiyalarni ish vazifalari va kutilayotgan natijalar bilan bog'lab, qabul qilingan standartlarga muvofiq harakat qilish qobiliyati sifatida ko'radi.

Etnolingvist Del Xayms Xomskiy kommunikativ kompetensiya atamasini lingvistik kompetensiya bilan bog'lab, real hayotdagi vaziyatlarga moslashtirgan. Kompetensiyaviy yondashuvning birinchi bosqichi (1960-1970) chet tili o'rganish nazariyasida Dell Hayms tomonidan til kompetensiya turlariga oid tadqiqotlar olib borilgan. Ikkinchi bosqich (1970-1990) esa chet tili nazariyasi va amaliyotida kasbiy mahorat va muloqotni o'rganishda kompetentlik kategoriyalarini qo'llashni o'z ichiga oladi.

J.Ravenning "Zamonaviy jamiyatda kompetentlik" asarida kompetentlik ko'plab mustaqil kompetensiyalardan iborat ekanligi ta'kidlanadi. V.Xutmaxer esa kompetensiyaning mazmuni hali to'liq ochilmaganligini va uning ijtimoiy hayotda va ishdagi vaziyatlarda qanday namoyon bo'lishini ta'kidlaydi. Unga ko'ra, kompetensiya shaxsiy va shaxslararo sifatlar, qobiliyatlar, bilimlar va ko'nikmalardan tashkil topadi.

Uchinchi bosqich 1990-yillardan boshlab kompetentlikni ta'limda ilmiy yondashuv sifatida o'rganish jarayonini ko'rsatadi. Bu davrda L.M. Mitina, L.A. Petrovskiy, N.V. Kuzmina, L.P. Alekseyeva va N.S. Shabligina kabi olimlar o'qituvchilarning kompetentligini o'rganishga e'tibor qaratdilar.

To'rtinchi bosqich esa kompetensiyaviy yondashuvning kasbiy ta'lim va umumta'lim fanlari standartlariga kiritilishi bilan bog'liq. I.N. Zotova kommunikativ kompetentlikni insonlar o'rtasidagi muloqotda malaka va ko'nikmalarga ega bo'lishi sifatida ta'riflaydi. Bu jarayonda "vaziyatga bog'liqlik" va "sherikchilik" kabi tushunchalar ko'p tadqiqotlarda ishlatiladi [9].

Ba'zi olimlar "til kompetensiyasi" o'rniga "tilni o'rganish" atamasini qo'llashni afzal ko'radilar. Masalan, I.A. Zimnya nutqiy faoliyatning asosiy turlari sifatida eshitish va gapirish ko'nikmalarini ajratib ko'rsatadi. U til kompetensiyasini grammatika, leksika va fonetika bo'yicha bilimlarni o'zlashtirish deb ta'riflaydi, bu esa nutqiy faoliyatning og'zaki va yozma shakllarida rivojlanadi.[8]

Til kompetensiyasi quyidagilarni o'z ichiga oladi: bayon qilish, e'lon qilish, ma'lumotni yetkazish va suhbatdoshining nutqini tushunish. "Chet tillari o'rganish kompetensiyasi" esa chet tilini o'rganish jarayonida qobiliyat, ko'nikma va malakalarni shakllantiruvchi kompleks jarayonni anglatadi. Lingvistik kompetensiya fonetik, orfografik va leksik vositalarni o'z ichiga oladi. Dastlab, bola chet tilidagi grammatik qoidalarni bilmasligi mumkin; u tilni eshitilgan ma'lumotlarni takrorlash orqali o'zlashtiradi. Avval eshitish va gapirish ko'nikmalari shakllanadi, keyin esa yozish va o'qish orqali grammatik qonun-qoidalar bilan tanishadi.

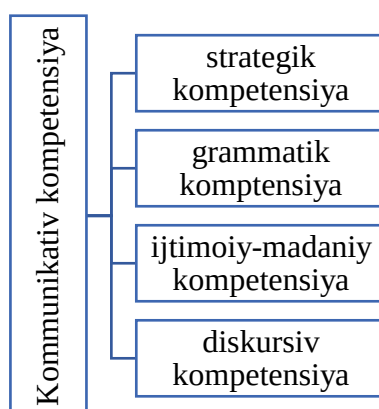
Nutqiy faoliyatga kirishish uchun nafaqat lingvistik kompetensiyani rivojlantirish, balki kommunikativ kompetensiya ham muhimdir. Bu kompetensiya til sistemasining strukturasini va qatlamlarini, ya'ni fonetika, leksika, morfologiya, sintaksis, matn stilistikasi, so'z yasalihi va so'z birikmalarini amaliyotda bir butun sifatida qo'llay olish ko'nikmasini o'z ichiga oladi. Bu haqida E.M. Vershagin, V.G. Kostomarov, D. Slobin, S. Muaran, S. Savinyon, L.F. Baxman, Yan Van Ek, M.N. Vyatutnev va G.V. Kolshanskiy kabi olimlar ta'kidlagan.

V.Ye.Gmurmanning fikricha, kompetensiyani shakllantirish jarayoni ixtiyoriy bosqichda yakuniy xarakterga ega bo'lib, ma'lum bir ko'rinishga intilish bilan bog'liqdir [9]. E.Z. Zeyer esa kompetensiyani samarali professional faoliyatni bajarish uchun zarur bo'lgan harakatlar va usullar majmui sifatida ta'riflaydi [6]. L.D. Petrovskiy kommunikativ kompetensiyani turli vaziyatlarda verbal va nonverbal vositalardan erkin foydalanish qobiliyati deb belgilaydi [13]. Yu.N. Yemelyanov esa bu qobiliyatni vaziyatga muvofiq ravishda ijtimoiy xulq-atvor normalariga amal qilgan holda ifodalaydi [5].

A.V. Xutorskiy kompetensiyani samarali faoliyatga o'quvchini tayyorlashda oldindan talab qilingan ijtimoiy talab sifatida ko'radi [15]. Lingvistik kompetensiya esa til qurilishi qoidalarni intuitiv darajada o'zlashtirish va nutqiy faoliyatda qo'llay olish ko'nikmasidir. A.A. Chuchalin esa kompetensiyani bilimlar, ko'nikmalar va ulardan foydalanish tajribasining birlashmasi deb ta'riflaydi.

Amerikalik psixolog D. Slobin muntazam muloqot davomida tilni tushunish ko'nikmasi paydo bo'lishini ta'kidlaydi [14]. Fransuz olimi S. Savinyon esa til kompetensiyasini grammatik kompetensiya bilan bir xil deb hisoblaydi, ya'ni bu tilning leksik, morfologik, sintaktik va fonologik qatlamlarini anglatadi.

M.Canale va M.Swain nazariyasiga ko'ra, kommunikativ kompetensiya to'rtta asosiy komponentga bo'linadi, va har bir komponent o'ziga xos jihatlar bilan muloqotni tashkil etishda muhim rol o'ynaydi [2].



1-rasm. M.Canale va M.Swain nazariyasiga muvofiq
kommunikativ kompetensiyaning tarkibiy qismi

Ushbu komponentlarni quyidagicha izohlash mumkin:

1. Strategik komponent: Bu komponent xorijiy tilni bilishdagi kamchiliklarni qoplash uchun zarur strategiyalarni o'z ichiga oladi. Nutqiy va ijtimoiy muloqot tajribasining yetishmasligi,

shuningdek, tilni qo'llashda yuzaga keladigan qiyinchiliklarni engish uchun turli xil strategiyalarni ishlab chiqish va qo'llash zarur.

2. Grammatik komponent: Bu komponent tilning grammatik va leksik asoslarini o'z ichiga oladi. U fonetika, imlo, semantika va sintaksisni o'z ichiga oladi, bu esa tilni to'g'ri va samarali ravishda ishlatish uchun zarurdir. Grammatik kompetensiya tilni tushunish va ifodalashda muhim ahamiyatga ega.

3. Ijtimoiy-madaniy komponent: Bu komponent muayyan vaziyatlarda tilning shakli va mazmunining muvofiqligini ta'minlaydi. Ijtimoiy madaniyat, kontekst va vaziyatga qarab, muloqotning qanday bo'lishi kerakligini tushunish va qo'llash qobiliyati muhimdir.

4. Diskursiv komponent: Bu komponent og'zaki va yozma nutqida yaxlit, izchil va mantiqiy fikrlarni ifodalashga qaratilgan. Diskursiv kompetensiya muloqot jarayonida fikrlarni aniq va izchil tarzda ifodalash imkonini beradi.

Ushbu to'rt komponent birgalikda kommunikativ kompetensiyani shakllantiradi va til o'rganishda muvaffaqiyatga erishishga yordam beradi. Har bir komponent o'zaro bog'liq bo'lib, tilni samarali ravishda o'rganish va foydalanishda muhim rol o'ynaydi.

Chet tilini o'qitish jarayonida kasbga yo'naltirilgan professional kommunikativ kompetensiyani shakllantirish, ayniqsa, oliy ta'lim muassasalarida, harbiy mutaxassislar uchun juda muhim ahamiyatga ega. Bu jarayon bir necha asosiy jihatlarni o'z ichiga oladi:

1. Maxsus maqsadlarda chet tilini o'qitish: Harbiy sohada ishlovchi talabalar uchun chet tilini o'qitish ularning professional faoliyatlari bilan bevosita bog'liq bo'lgan terminologiya va kontekstga asoslangan bo'lishi kerak. Bu, o'z navbatida, talabalarga xalqaro muloqotda muvaffaqiyatli ishtirok etish imkoniyatini beradi.

2. Terminologiya va ilmiy-texnik adabiyotlar: Harbiy mutaxassislar uchun ingliz tilida gapirish ko'nikmalarini rivojlantirishda, sohalariga mos keluvchi terminlarni o'rganish juda muhimdir. Talabalar o'z sohalariga oid ilmiy-texnik adabiyotlardan foydalanish qobiliyatini rivojlantirishlari lozim, bu esa ularning bilimlarini kengaytiradi va professional sohada samarali ishlashlariga yordam beradi.

3. Nutq faoliyatining to'rt turi: Chet tilini o'qitishda nutq faoliyatining to'rt turi — tinglash, gapirish, o'qish va yozish - dastur mavzulari doirasida o'rganilishi zarur. Har bir faoliyat turi o'ziga xos metod va texnikalarga ega bo'lib, talabalarni muloqot jarayonida yanada samarali qilishga yordam beradi.

4. Vaqt me'yorlari: Oliy ta'lim muassasalarida ingliz tilini o'qitishda vaqt me'yorlarining cheklanganligi, o'quv jarayonini samarali tashkil etish va talabalar uchun kerakli bilim va ko'nikmalarni yetkazish masalasini yanada dolzarb qiladi. Bu shuni anglatadiki, o'qitish jarayonida innovatsion metodlarni qo'llash va intensiv kurslar tashkil etish zarur.

5. Kasbiy malakalarni shakllantirish: Talabalarining kasbiy malakalarini shakllantirishda interaktiv o'qitish metodlari, simulyatsiyalar va real hayotiy vaziyatlarga asoslangan mashg'ulotlar katta ahamiyatga ega. Bu usullar talabalarni amaliy tajribaga tayyorlashda yordam beradi.

Xulosa qilib shuni ta'kidlash mumkinki, Oliy ta'lim muassasalarida chet tilini o'qitish jarayonida ushbu jihatlarni hisobga olish orqali harbiy mutaxassislarning professional kommunikativ kompetensiyasini rivojlantirish mumkin. Bu esa nafaqat ularning kasbiy faoliyatida muvaffaqiyatli bo'lishlariga, balki xalqaro miqyosda ham samarali muloqot qilishlariga yordam beradi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

[1] Ivanova M.A. Формирование учебных умений студентов вне аудиторной самостоятельной работе на примере иностранного языка на неязыковом факультете: кан. пед. наук... дисс.: - РФ. 2005.— С 157.

[2] Canale M. and Swain M. «Theoretical bases of communicative approaches to second language teaching and testing» Applied Linguistic, 1, 1980. pp. 1 – 47

- [3] Homskiy.N. Аспекты теории синтаксиса [Электронный ресурс] /Н. Хомский. - Москва: Изд-во Московского университета, 1972. – 129 с.
- [4] Gmurman.V.E Уточнение и систематизация понятий и терминов в педагогике // Интегративные процессы в педагогической науке и практике воспитания и образования. М.:АПН СССР, 1983. – С 29 - 36.
- [5] Yemelyanov, Yu.N. Активное социально-психологическое обучение: монография / Ю.Н. Емельянов. - JL: Изд - во Ленингр. Ун - та, 1985. – 166 с
- [6] Zeyer.E.F. Личностно-ориентированное профессиональное образование / Э.Ф. Зеер, Г.М. Романцев // Педагогика. 2002. №3. – С. 16 – 21.
- [7] Zeyer.E.F. Саморегулируемое учение как психолого дидактическая технология формирования компетенции у обучаемых // Психологическая наука и образование. 2004. № 3. – С. 5 – 40.
- [8] Zimnya.I.A. Социальная работа как профессиональная деятельность //Социальная работа / Отв. ред. И.А.Зимняя. Вып. 2. М., 1992. 9. Zotova I.N. Психолого-педагогическая поддержка развития коммуникативной компетенции студентов технического вуза: автореф. дис.канд. психол. наук: 19.00.07/. Ставрополь, 2006. – 22 с
- [9] Yo'ldosheva D.Sh. "Taqlid so'zlarda lingvistik kompetensiyaviy yondashuvni shakllantirish turlari" «Science and Education» Scientific Journal, August 2020// Volume 1, Issue 5.
- [10] Kadirova M.R. Tillarga ixtisoslashmagan oliy ta'lim muassasalari talabalariga chet tilini o'rgatishda ijodiy faollikni medernizasiyalash: ped.fan. nom. Diss. T., 2008. – 64 b.
- [11] Красильникова Т.Д. Иноязычная коммуникативная компетенция в исследованиях отечественных и зарубежных ученых. // Ярославский педагогический вестник. 2009. № 4. – 179-185 с.
- [12] Petrovskaya L.A. Компетентность в общении. Социально психологический тренинг / Л.А. Петровская - М.: Изд.-во МГУ, 2016. – 216 с.
- [13] Слобин Г. Предпосылки развития грамматики [Текст] /. - М.:Наука, 1984. – с. 192.
- [14] Хуторской А. Ключевые компетенции как компонент личностно-ориентированной парадигмы образования // Народное образование. 2003.№2. – С. 58-64.

HARBIY PEDAGOGIK MAHORAT ASOSLARI

dotsent. A.Sh. XUDAYAROV, dotsent X.U. YAKUBOV*O'R MV Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti*

Annotatsiya. “Pedagogik mahorat” – oliy ta’lim muassasalarida o‘qitiladigan pedagogik turkum fanlarning biri sanaladi. Fanning asosiy maqsadi – talabalarda pedagogik jarayonni mustaqil, tashkiliy, ilmiy-metodik jihatdan to‘g‘ri tashkil eta olish va kasbiy-pedagogik faoliyatda yuqori samaradorlikka erishishni kafolatlovchi bilim, ko‘nikma va malakalarini shakllantirishdan iborat.

Kalit so‘zlar: Harbiy pedagogik mahorat, kasbiy (pedagogik) bilim, pedagogik qobiliyat, pedagogik ta’sir ko‘rsatish, pedagogik muloqot, pedagogik odob, pedagogik madaniyat, pedagogik hamkorlik, pedagogik nazokat (takt), pedagogik texnika, pantomimika, mimika, o‘qituvchining nutq texnikasi.

Аннотация. “Педагогическое мастерство” – одна из педагогических категорий дисциплин, преподаваемых в высших учебных заведениях. Основная цель дисциплины – формирование у обучающихся знаний, умений и навыков, гарантирующих самостоятельную, организационную, научно-методическую правильную организацию педагогического процесса и достижение высокой эффективности в профессионально-педагогической деятельности.

Ключевые слова: военно-педагогическое мастерство, профессиональные (педагогические) знания, педагогические способности, педагогическое воздействие, педагогическое общение, педагогический этикет, педагогическая культура, педагогическое сотрудничество, педагогическая грация (такт), педагогическая техника, пантомимика, мимика, речевая техника учителя.

Abstract. “Pedagogical skill” is one of the pedagogical category of subjects taught in higher educational institutions. The main goal of the science is the formation of knowledge, skills and qualifications in students that guarantee the ability to independently, organizational, scientifically – methodically correctly organize the pedagogical process and achieve high efficiency in professional and pedagogical activity.

Keywords: military pedagogical skill, professional (pedagogical) knowledge, pedagogical ability, pedagogical influence, pedagogical communication, pedagogical etiquette, pedagogical culture, pedagogical cooperation, pedagogical femininity (ICT), pedagogical technique, pantomimics, mimics, teacher's speech technique.

“Harbiy pedagogik mahorat” fanini o‘qitish jarayonida belgilangan maqsadga erishish uchun quyidagi vazifalarni ijobiy hal qilish talab etiladi:

kursatlarni pedagogik mahoratning tarkibiy qismlariga doir nazariy bilimlar bilan qurollantirish;

ularda pedagogik faoliyatni oqilona tashkil etish, pedagogik jarayonni samarali yo‘lga qo‘yish ko‘nikma, malakalarini rivojlantirish;

kursatlarning pedagogik hamkorlikni qaror toptirish texnologiyasi borasidagi bilimlarni egallashlarini ta’minlash;

ularda pedagogik odob va madaniyat sifatlarini tarkib toptirish, pedagogik qobiliyatni shakllantirish;

kursatlar tomonidan pedagogik muloqot, pedagogik nazorat (takt), texnika va pedagogik ta’sir ko‘rsatish ko‘nikma, malakalarini yetarli darajada o‘zlashtirilishini ta’minlash;

bo‘lajak mutaxassis sifatida talabalarda pedagogik madaniyatni shakllantirish [1].

Mohiyati nuqtai nazardan pedagogik mahorat pedagogga xos kasbiy sifatlarning majmui sifatida ko‘zga tashlanadi. Pedagogik mahorat “pedagogik san’at” sifatida ham talqin etiladi. Tushunchaning mohiyatini chuqur anglash uchun dastlab uning lug‘aviy ma’nosini tushunib olish

lozim. Manbalarda “mahorat” tushunchasi arab tilidan tarjima qilingandamohirlik, ustalik, epchillik ma’nolarini anglatishi ko’rsatiladi. Mantiqan esa “biror ish, kasb uchun zarur yoki shu sohada orttirilgan ustalik, san’at, mohirlik” deya ta’riflanadi. “Mahorat” tushunchasini pedagogik sohaga tatbiq etilganda mazkur tushuncha quyidagi holatni yoritishga xizmat qiladi:

Ta’lim jarayonining faol ishtirokchisi bo’lgan o’qituvchining pedagogik mahorati pedagog shaxsi, uning ish tajribasi, fuqarolik maqomi, mutaxassis sifatidagi mavqei, u tomonidan pedagogik texnikaning yetarli darajada egallanganligi, kasbiy faoliyatning individualligidan dalolat beradi. Pedagogik mahorat yaxlit tizim bo’lib, uning tarkibida bir qator sifatlar ko’zga tashlanadi [2].

Pedagogik mahoratning muhim tarkibiy qismlari.

“Pedagogik mahorat” tushunchasi “Pedagogika”, “Pedagogik texnologiya”, “Pedagogik mahorat” kabi fanlarga xos muhim tushuncha bo’lib, u o’tgan asrning 80-90-yillarida ilmiy-pedagogik jihatdan asoslangan.

Pedagogik manbalarda pedagogik mahoratning asosiy, muhim kategoriyalari sifatida quyidagilar e’tirof etiladi:

Mahorat – muayyan ish, xatti-harakat yoki kasbiy faoliyatning ustalik, mohirlik bilan, san’atkorona tashkil etilishiga imkon beradigan bilim, ko’nikma va malakalar majmui.

Pedagogik mahorat – pedagog tomonidan kasbiy faoliyatning ustalik, mohirlik bilan, san’atkorona tashkil etilishini ta’minlovchi bilim, ko’nikma va malakalar majmui.

Pedagogik ijod – pedagogning kasbiy jarayonni samarali tashkil etishga yo’naltirilgan yaratuvchanlik faoliyati.

Pedagogik novatorlik – pedagogik faoliyatda ilg’or tamoyil, g’oyani asoslash, yangi yo’l, usul yoki vositalarni tavsiya qilish, ularning amaliyotga tatbiqini ta’minlashga qaratilgan ijodiy yondashuv.

Pedagogik bilimdonlik – pedagogning kasbiy faoliyatni mavjud ijtimoiy talab, huquqiy me’yor, standartlarga muvofiq tashkil etishga bo’lgan qobiliyati; kasbiy tayyorgarlik darajasi.

Pedagogik faoliyat – pedagog tomonidan kasbiy maqsadga muvofiq tashkil etiladigan tizimli harakatlarning muayyan shakli.

Pedagogik texnika – pedagogik faoliyatda orttirilgan ko’nikma, malakalar yig’indisi bo’lib, u pedagogik jarayon samaradorligini ta’minlaydi.

Pedagogik tajriba – kasbiy faoliyatni tashkil etish jarayonida pedagog tomonidan o’zlashtirilgan, orttirilgan bilim, ko’nikma va malakalar majmui.

Pedagogik madaniyat – pedagogning shaxs va mutaxassis sifatida muayyan xulq-atvor, odob, muomala, xatti-harakat ko’nikma, malakalarini o’zlashtirish darajasi.

Pedagogik bilimdonlik – pedagogning kasbiy faoliyatni mavjud ijtimoiy talab, huquqiy me’yor, standartlarga muvofiq tashkil etishga bo’lgan qobiliyati, kasbiy tayyorgarlik darajasi [3].

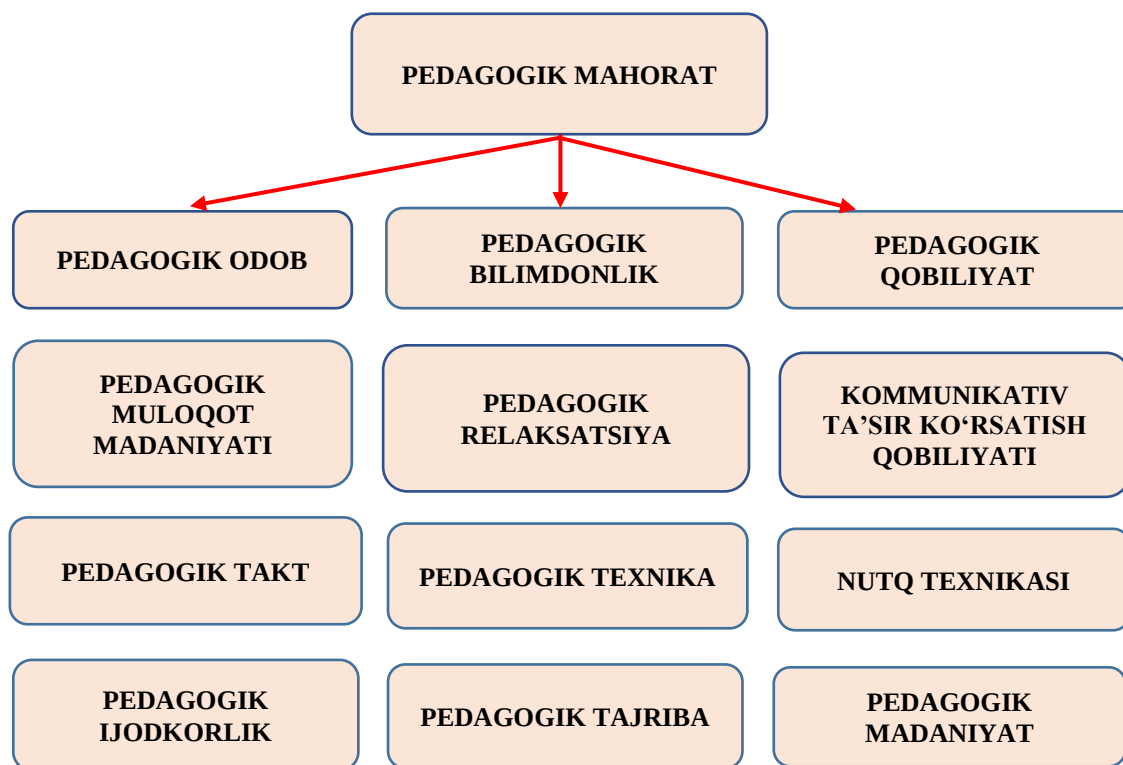
Pedagogik bilimdon shaxs mutaxassis sifatida pedagogik jarayon va munosabatlarni maqsadga muvofiq samarali shakl, usul hamda vositalarini yetarli darajada o’zlashtira olgan bo’lishi zarur. Bilimdon o’qituvchi quyidagi sifatlarini o’zlashtira olish imkoniyatiga ega bo’lishi darkor:

ijtimoiy sub’ektlar bilan o’zaro aloqada, madaniy muloqotda bo’la olish;

mutaxassislik yo’nalishi bo’yicha axborotlarni izlash, topish, ularni ta’lim mazmuniga tayangan holda qayta ishlash, kasbiy faoliyat jarayonida ulardan samarali foydalana bilish;

o’quv axborotlarini ta’lim oluvchi (o’quvchi, talaba)larga yetkazib bera olish.

Pedagogning kasbiy bilimdonligida o’quvchi bilan sub’ektiv munosabat o’rnatish; pedagogik jarayonlar mohiyati, pedagogik voqelikni izchil idrok qila bilish; jahon pedagogik madaniyati asoslarini, milliy pedagogik tajribani o’rganish, ularni integratsiyalashtirish asosida o’z faoliyatiga tatbiq etish; innovatsion yangiliklardan doimiy xabardor bo’lish; shaxsiy tajribalarni umumlashtirish, ta’lim oluvchilarga uzatish; kasbiy fidoiylik hamda pedagogik texnologiyalarni egallash borasidagi bilim, ko’nikma, malakalarning o’zlashtirilganligida namoyon bo’ladi.



1-rasm. Pedagogik mahorat tarkibiy qismlari

Pedagogik kreativlik – pedagogning an'anaviy pedagogik fikrlashdan farqli ravishda ta'lim, tarbiya jarayonining samaradorligini ta'minlashga xizmat qiluvchi yangi g'oyalarni yaratish, mavjud pedagogik muammolarni ijobiy hal qilishga bo'lgan tayyorgarligini tavsiflovchi qobiliyati.

Pedagogik bilimdonlik negizida, pedagogik refleksiya (lotinchadan "reflexio" – ortga qaytish, aks etish) ham ko'zga tashlanadi. Manbalarda "refleksiya" tushunchasi "kishining o'z xatti-harakatlari va ularning asoslarini tushunib yetishi, fahmlashiga qaratilgan nazariy faoliyati; bilishning alohida faoliyati", "shaxsiy kechinmalari, his-tuyg'ulari va o'yxayollari mohiyatini fikrlash orqali anglash" sifatida talqin etiladi.

Pedagogik refleksiya – pedagogning shaxs ongi (uning funksiyalari), qadriyatlari, qiziqishlari, rag'batlantiruvchi omillari, fikrlash, idrok, qarorlar qabul qilish, hissiy ta'sirlanish, xatti-harakatlari va b.ning mohiyatini anglab yetishi.

O'qituvchi pedagogik bilimdonlik, kreativlik, refleksiyaga ega bo'lish bilan birga pedagogik madaniyatni ham o'zlashtira olishi zarur. Pedagogik madaniyat kasbiy nuqtai nazardan pedagogik faoliyatni olib boruvchi mutaxassis umumiy madaniyatining tarkibiy qismi hisoblanadi [4].

Pedagogik madaniyat – bu pedagogning kasbiy vazifalarni hal qilish usul, vositalarini o'zlashtirganlik, pedagogik bilimdonlik, takt, texnika va madaniyatni namoyon qila olishning yuqori darajasi.

Ta'lim va tarbiya jarayonini tashkil etish uchun mas'ul va yetakchi sub'ekt bo'lgan pedagogning pedagogik madaniyati negizida quyidagilar aks etadi:

1) uning umumiy madaniyati, u tomonidan e'zozlanadigan moddiy va ma'naviy qadriyatlar, ijodiy pedagogik faoliyati;

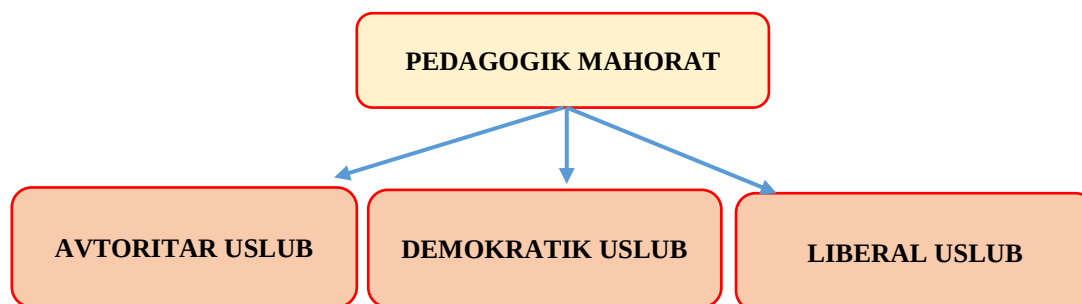
2) pedagog shaxsining tavsifi;

3) pedagogik qadriyatlar, pedagogning faoliyati, kasbiy xulq-atvorini o'z ichiga oluvchi dinamik tizim: pedagogik pozitsiya va shaxsiy sifatlar; kasbiy bilimlar, pedagogik tafakkur madaniyati; kasbiy malaka, pedagogik faoliyatning ijodiy xususiyati; shaxsning o'z-o'zini boshqarishi va pedagogning kasbiy hatti-harakatlari madaniyati.

Pedagogga xos madaniyat negizida quyidagi sifatlar namoyon bo'ladi:

- 1) o'quvchi (talaba, tarbiyalanuvchi)ning qiziqishlari, ehtiyojlarini tushuna olish, ularga hamdardlik bildirish qobiliyati;
- 2) ta'lim va tarbiya jarayonini shaxsan boyita olish ko'nikmasi;
- 3) o'quvchi (talaba, tarbiyalanuvchi) shaxsida ijobiy "men"lik (o'zlik)ni rivojlantirish uchun ijobiy rag'bat bildirish, yo'naltira olish;
- 4) o'zini o'zi va o'quvchi (talaba, tarbiyalanuvchi)larni boshqara olish;
- 5) o'quvchi (talaba, tarbiyalanuvchi)lar bilan rasmiy va norasmiy muloqotni tashkil etishning turli uslublarini o'zlashtira olganlik;
- 6) hissiy barqarorlik, o'zini tuta bilish, o'z-o'ziga ishonch, hayotsevarlik;
- 7) hech qanday majburiyatlarsiz, ixtiyoriy ravishda pedagogik ziddiyatlarni boshqarish;
- 8) turli diniy g'oyalar va an'analarga e'tiqod qiluvchi o'quvchi (talaba, tarbiyalanuvchi)larga hurmat bilan munosabatda bo'lish;
- 9) yaratuvchilik;
- 10) pedagogik refleksiya qobiliyatiga egalik.

O'qituvchi pedagogik muloqotni tashkil etishda yordamga muhtoj o'quvchilarga alohida e'tibor berishi, har bir o'quvchida turli o'quv fanlari asoslarini o'zlashtirishga nisbatan qiziqtirish usullaridan foydalanishi, hamkorlik va ijodkorlikka asoslangan mehnatni tashkil etishni oldindan o'ylab qo'yish lozim. Mutaxassis sifatida o'qituvchi tomonidan jamoa bilan muloqotni uyushtirish texnikasini doimiy ravishda tahlil qilib borish maqsadga muvofiqdir. Ma'lum vaziyatlarda o'qituvchi rahbar sifatida o'quvchilar, tarbiyalanuvchilar faoliyatlarini boshqaradi. Xuddi shu jarayonda ham muloqot yetakchi omil hisoblanadi. Biroq, muloqotning samaradorligi rahbar sifatida namoyon bo'layotgan o'qituvchi tomonidan qanday uslub (muloqot uslubi)ning tanlanganligi bilan belgilanadi. Odatda, o'qituvchining rahbar sifatidagi muloqot usullari quyidagi uch turga ajratiladi [5].



1-rasm. Pedagogik mahorat uslublari

Avtoritar uslub. Bunga ko'ra o'quvchilarning barcha turdagi faoliyatlarining tashkil etilishi, mazmuni, shakli, metod va vositalarining barchasi faqat o'qituvchi tomonidan belgilanadi. O'quvchilarning har qanday tashabbuslari rag'batlantirilmaydi, aksincha, buyruq, ko'rsatma, yo'llanma berish, jazolash choralari ko'rish orqali o'quvchilarga ta'sir etiladi. Hatto o'quvchilarning faoliyatlari ijobiy baholangan vaqtda ham ularga bo'lgan ta'sir turli kesatqlar bilan bayon etiladi. Ya'ni: "Sendan ijobiy xatti-harakatni kutmagan edim?!", "Buni qara-ya, nahotki o'zgargan bo'lsang!?", "Qaraya, birgina a'lo baho olish bilan o'zingni yaxshi inson bo'lib qolgan deb hisoblaysanmi!?"

va h.k. mazmundagi rag'batlar ijobiy holatni e'tirof etishga yo'naltirilgan bo'lsa-da, o'quvchini yangi yutuqlarga ilhomlantirmaydi. Aksincha, unda ta'lim olishga, ta'lim muassasasiga va o'qituvchilarga nisbatan sovuqqonlikni yuzaga keltiradi.

Demokratik uslub. Unga ko'ra o'qituvchi pedagogik faoliyatni tashkil etishda jamoaning fikriga tayanib ish ko'radi. O'quv mashg'ulotlari va tarbiyaviy ishlarni tashkillashtirishda har bir

o'quvchining fikrini inobatga olishga, ularni umumlashtirgan holda eng samaralisini tanlab olishga intiladi. Muhokamalar chog'ida barcha o'quvchilarning ishtiroklari ta'minlanadi. O'quvchilar tomonidan bildirilayotgan tashabbuslar qo'llabquvvatlanadi, mavjud imkoniyatlardan kelib chiqqan holda

bu tashabbuslar amaliyotga tatbiq etiladi. Demokratik uslubdan foydalanayotgan o'qituvchi zimmasidagi vazifa faqatgina o'quvchilarning faoliyatini nazorat qilish, tuzatishlar kiritishdan iborat emasligini anglab yetadi. Asosiy e'tiborni o'quvchilarning yutuqlarini e'tirof etgan holda yoki ularning xatolarinio'zlariga anglatgan holda samarali ta'sir chorasini ko'rishga qaratadi. Har bir o'quvchining yutug'i alohida e'tirof etiladiki, bu yangi zafarlarga erishishga ruhlantiradi. Ushbu uslubga asoslanib ish ko'radigan o'qituvchi har bir o'quvchining qiziqishlari, qobiliyatlarini hisobga olgan holda bajariladigan ishlarni to'g'ri taqsimlashga harakat qiladi, faol o'quvchilarni taqdirlab borishni faoliyatining asosiy yo'nalishi sifatida belgilaydi. Bu kabi demokratik uslubga ega o'qituvchi o'quvchilar bilan muloqotni o'rnatishda iltimos, maslahatga tayanib ish ko'radi [6].

Liberal uslub. Odatda bu uslub o'qituvchi va o'quvchi munosabatlarining kelishuvchanlikka asoslanishini ta'minlaydigan uslub sifatida e'tirof etiladi. Liberal uslubga ko'ra ish yuritadigan o'qituvchi pedagogik jarayonlarda o'quvchilar tomonidan sodir etilayotgan salbiy holatlarga ham e'tibor bermaslikka intiladi. O'quvchilarni tartibga chaqirish, vaziyatdan kelib chiqqan holda ularning faoliyatini to'g'ri baholab, jazolash zarur bo'lgan vaziyatlarda ham indamaslikni odat qilib oladi. Bu esa o'quvchilarning odobsiz, yalqov, mas'uliyatsiz bo'lishlariga olib keladi. Liberal uslubni ma'qul ko'radigan o'qituvchi o'quvchilar hayoti bilan mutlaqo qiziqmaydi, ularning faoliyatlariga aralashmaydi, hal qiluvchi vaziyatlarda mas'uliyatni o'z zimmasidan soqit qiladi. Ayrim holatlarda bir-biriga zid bo'lgan fikrlarni ham birdek ma'qullaydi. Natijada bu taxlitda ish ko'radigan o'qituvchi hech qanday obro'ga ega bo'lmaydi. Chunki unga ishonish mumkin emas[7].

Xulosa qilib aytganda, pedagogik jarayonda o'qituvchining ta'sirini kuchaytiradigan omillardan biri – bu uning ovozi, unga xos bo'lgan xususiyatlar sanaladi. O'qituvchi ovozining yoqimli va jarangdor bo'lishi o'quvchilar e'tiborini o'ziga to'la qarata olishini ta'minlaydi. Ta'sirchanligini aniqlash uchun o'qituvchi ovozining qanchalik darajada kuchli, shirador va yoqimli ekanligini bilishi, zarur vaziyatlarda ovozning bu kabi xususiyatlaridan unumli foydalana olishi zarur. O'z ovozida ma'lum kamchiliklar borligini sezgan o'qituvchi ularni bartaraf etishga harakat qilishi kerak. Buning uchun ovozdan foydalanish, uni yaxshilash texnikasi ustida izchil, doimiy mashq qilib borishi talab etiladi. Binobarin, bir yoki ikki marta qilingan mashq bilan ovoz xususiyatlarini yaxshilab bo'lmaydi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

- [1] Kan-Kalik V.A., Nikandrov N.D. Pedagogicheskoe tvorchestvo. – Moskva: Pedagogika. 1990. – 144 s.
- [2] Kuxarev N.V. Na puti k professionalnomu sovershenstvu. – Moskva: Prosveshchenie, 1990. – 159 s.
- [3] Muhiddinov A.G. O'quv jarayonida nutq faoliyati. – Toshkent: O'qituvchi, 1995. – 65 bet.
- [4] Основы педагогического мастерства / Под ред. A.Zyuzina. – Moskva: Prosveshchenie, 1989. – 302 s.
- [5] Pedagogik mahorat va pedagogik texnologiyalar / Ma'ruzalar matni. Tuzuvchilar: A.X.Qosimov, F.A.Holikova. – Toshkent: TATU, 2004. – 132 bet.
- [6] Sayidahmedov N. Pedagogik mahorat va pedagogik texnologiya. – Toshkent: Oliy pedagogika instituti, 2003. – 125 bet.

**ХАРБИЙ БЎЛИНМА ШАХСИЙ ТАРКИБНИНГ ЖАНГОВОР ҚОБИЛИЯТИНИ
АНИҚЛАШДА БЕЛГИЛАР МАЖМУАСИНИ ШАКЛЛАНТИРИШ ВА УЛАРНИНГ
ТАҲЛИЛИ****З.Р. ИМИНОВ***Ўзбекистон Республикаси Мудофаа вазирлиги*

Аннотация. Ушбу мақолада ҳарбий бўлинма шахсий таркибининг жанговор қобилиятини аниқлашда белгилар мажмуасини шакллантириш масалалари ҳамда ҳарбий хизматчининг жанговор тайёргарлиги, жисмоний ва руҳий ҳолатини баҳолаш усуллари муҳокама қилинади. Шу билан бирга, баҳолаш мезонлари ва тизимларининг такомиллашуви орқали ҳарбий қисмлар самарадорлигини ошириш имкониятлари ёритиб берилади.

Калит сўзлар: жанговор қобилият, ҳарбий хизматчи, шахсий таркиб, таҳлил, белгиловчи омиллар, баҳолаш мезонлари, тайёргарлик, ҳарбий психология, жисмоний ҳолат, стратегик кўрсаткичлар, самарадорлик, баҳолаш тизими, ҳарбий салоҳият.

Аннотация. В статье рассматриваются вопросы формирования совокупности признаков для определения боеспособности личного состава военного подразделения, а также методы оценки боевой подготовки, физического и психологического состояния военнослужащих. Особое внимание уделяется усовершенствованию системы оценки с целью повышения эффективности воинских частей.

Ключевые слова: боеспособность, военнослужащий, личный состав, анализ, определяющие факторы, критерии оценки, подготовка, военная психология, физическое состояние, стратегические показатели, эффективность, система оценки, военный потенциал.

Abstract. This article discusses the formation of a set of indicators for determining the combat capability of military unit personnel, as well as methods for assessing the combat training, physical and psychological condition of servicemen. Particular attention is paid to improving evaluation systems to enhance the effectiveness of military units.

Keywords: combat capability, serviceman, personnel, analysis, determining factors, assessment criteria, training, military psychology, physical condition, strategic indicators, efficiency, evaluation system, military potential.

Бўлинма шахсий таркибининг жанговор қобилиятини аниқлашда белгилар мажмуаси бир нечта гуруҳга бўлиб ўрганилади. Белгиларни ўрганиш Ҳарбий хизматчига қўйиладиган умумий, унинг касбига қўйилган, техник жиҳозлар ва алоқа воситалардан фойдаланиш маҳоратига қўйилган талаблардан ва ҳар хил ҳарбий ҳолатларда жанг санъатини мантикий олиб боришга қўйиладиган интеллектуал талаблар базасида шакллантирилади. Дастлаб, барча ҳарбий хизматчи бўлинма аскарларининг ҳар бири учун белгилар мажмуаси шакллантирилади, сўнгра ҳарбий хизматчи бўлинмалар қобилиятини аниқлашнинг математик модели қурилиб, ҳар хил жанговор ҳолатлар учун бўлинмаларнинг жанговор қобилиятини баҳоланади.

Жанговор салоҳият белгиларининг номланиши.

Юқорида баён қилинган барча масалаларни ечиш учун қуйидагича белгилашлар киритилади:

x_{pi} – ҳарбий хизматчи, $X_p, p = \overline{1, r}$ бўлинманинг $x_{pi} = (x_{pi}^1, x_{pi}^2, \dots, x_{pi}^N), i = \overline{1, m_p}$, ҳарбий хизматчиси. Демак, ҳарбий хизматчиларнинг хизмат вазифаларига кўра m_p та бўлиб, одатда бўлинмаларда 6-10 та аскарлардан ташкил топган бўлади.

Ҳар бир ҳарбий хизматчи тадқиқот ҳарбий хизматчиси деб олиниб, уларни қуйидагича ифодаланиб, $x_{pi} = (x_{pi}^1, x_{pi}^2, \dots, x_{pi}^N), i = \overline{1, m_p}$, N - ўлчовли белгилар орқали ифодаланган. Бу

ерда x_{pi}^1 - $X_p, p = \overline{1, r}$, бўлинманинг $i = \overline{1, m_p}$ чи ҳарбий хизматчининг биринчи белгиси деб ўқилади. Қуйида ҳарбий хизматчиларнинг умумий белгилари мажмуаси:

x_{pi}^1 - номзодни дастлабки ўрганиш; x_{pi}^2 - ҳарбий кўрик; x_{pi}^3 - психологик ўрганиш (интеллектуал ривожланганлик даражаси ва психоэмоционал барқарорлиги баҳоланади); x_{pi}^4 - жисмоний тайёргарлик даражаси; x_{pi}^5 - номзоднинг касбий нуктаи назардан ҳарбий хизмат учун муҳим сифатларини ўрганиш бўйича вазирлик томонидан белгиланувчи бошқа турдаги синов (текширув) турлари.

Ҳарбий хизматчилар билан жанговор тайёргарлиги қуйидаги фанлар кесимида баҳоланиб, улар асосида белгилар шакллантирилади, улар Ҳарбий хизматчиларнинг касбий белгилари деб тушунилади:

x_{pi}^6 - Тактик тайёргарлик; x_{pi}^7 - Отиш тайёргарлиги; x_{pi}^8 - Тоғ тайёргарлиги; x_{pi}^9 - Ҳаво-десант тайёргарлиги; x_{pi}^{10} - Разведка тайёргарлиги; x_{pi}^{11} - Тактик тайёргарлик; x_{pi}^{12} - Жанговор машиналарни бошқариш; x_{pi}^{13} - Муҳандислик тайёргарлик; x_{pi}^{14} - Оммавий қирғин куролларидан ҳимояланиш; x_{pi}^{15} - Жисмоний тайёргарлик; x_{pi}^{16} - Ҳарбий топография; x_{pi}^{17} - Алоқа тайёргарлиги; x_{pi}^{18} - Ҳарбий тайёргарлик; x_{pi}^{19} - Саф тайёргарлиги; x_{pi}^{20} - Умумҳарбий низомлар; x_{pi}^{21} - Информатика асослари.

Мазкур фанлар бўйича машғулотлар ташкиллаштирилади, ҳамда ўтилган машғулот ва мейёрлар бўйича ҳарбий хизматчилар баҳоланади ва олинган натижалар асосида фанларни ўзлаштириш даражалари аниқланади. Фанларни ўзлаштириш даражалари кесимида белгилар шакллантирилади.

Ҳарбий хизматчиларнинг жанговор салоҳиятини аниқлашда интеллектуал ва жанговор тайёргарлик бўйича ўтилган фанлар асосий ва асосий бўлмаган фанларга ажратилади. Бунда ҳарбий хизматчиларнинг жанговор салоҳиятини баҳолашда асосий бўлган фанларнинг ўзлаштириш даражаси, асосий бўлмаган фанларни ўзлаштириш даражасига нисбатан муҳимлик даражаси юқори ҳисобланади. Ушбу таҳлилларни инобатга олиниб экспертлар томонидан белгиларнинг муҳимлик даражалари коэффиценти ишлаб чиқилади [48-58].

Ҳарбий хизматчиларнинг техник жиҳоз ва алоқа воситаларидан фойдаланишнинг маҳорат белгилари мажмуаси:

x_{pi}^{22} - Исталган куролдан фойдаланиш кўникмаси; x_{pi}^{23} - Жанговор тажриба.

Ҳарбий хизматчиларнинг интеллектуал белгилари мажмуаси:

x_{pi}^{24} - Ихтиёрий ҳолатлардан хулоса чиқариш; x_{pi}^{25} - Қарор қабул қилиш. x_{pi}^{26} - Умумҳарбий низомлар; x_{pi}^{27} - Критик ҳолатларда вазифа белгилаш.

Демак, Ҳарбий хизматчиларнинг салоҳиятини аниқловчи белгилар мажмуаси тўрт гуруҳга ажратилиб таҳлил қилинди ва барча белгилар номланди. Энди қуйида ушбу белгиларнинг қийматлар соҳаси аниқланади [59-61].

Ҳарбий хизматчиларнинг жанговор салоҳиятларини аниқловчи белгиларни шакллантириш

Ҳарбий хизматчилар таркибини номинал белгилар ёрдамида ифодаланиши. Яъни, ҳар бир аскарнинг белгиларини рақамлаштириш масаласини қараб чиқайлик. Белгилар ва уларни номланиши ҳамда қийматлар соҳаларини аниқлаш қуйидагича амалга оширилади.

x_{pi}^1 - номзодни дастлабки ўрганиш белгиси қабул қиладиган қийматлар. Бу белги орқали ҳарбий хизматчининг дастлабки ўрганиш натижасида унинг ҳарбий хизматга лойиқлик даражаси аниқланади. Бу номинал белгилар асосида шакллантирилади: $x_i^1=1$ бўлса, у ҳолда ҳарбий хизматга лойиқлик даражаси энг юқори ва уни исталган лавозига тайинлаш мумкин, агар, $x_i^1=2$ бўлса, у ҳолда ҳарбий хизматга лойиқлик даражаси юқори ва яхши, ҳамда $x_i^1=3$ бўлса, у ҳолда ҳарбий хизматга лойиқлик даражаси қониқарли. Демак, x_i^1 белги уч хилдаги

кийматлар қабул қилади, айрим вақтлари бу белгиларга қийматлар экспертлар томонидан аниқланади..

x_{pi}^2 - ҳарбий кўрик белгиси қабул қиладиган қийматлар ҳарбий экспертлар томонидан аниқланади. x_i^2 - белги эса ҳарбий хизматчининг ҳарбий маълумоти бўлиб, у тўрт хил кўринишда ифодаланган бўлади қониқарли, яхши, аъло ва қониқарсиз. Демак, унинг белгилари қуйидаги шкала кўринишида ифодаланиб, $x_i^2 = 1$ (аъло); $x_i^2 = 2$ (яхши); $x_i^2 = 3$ (қониқарли); $x_i^2 = 4$ (қониқарсиз) қийматлар қабул қилиши мумкин.

x_{pi}^3 - психологик ўрганиш (интеллектуал ривожланганлик даражаси ва психоэмоционал барқарорлиги баҳоланади). Бу белги қуйидаги қийматлардан бирини $x_i^3 = 1$ (аъло); $x_i^3 = 2$ (яхши); $x_i^3 = 3$ (қониқарли); $x_i^3 = 4$ (қониқарсиз) қабул қилиши мумкин. Албатта, баҳо эксперт мутахассислар томонидан аниқланади, ёки мутахассислар ишлаб чиққан компьютер тестлари орқали аниқланиши мумкин.

x_{pi}^4 - жисмоний тайёргарлик даражаси.

Ҳарбий хизматчининг жисмоний тайёргарлик даражаси уч хил хусусиятга эга бўлади. Бу хусусият аскарнинг чидамлилиқ, тезкорлик ва кучлилиқ даражалари билан белгиланади. Агар $x_{pi}^4 = 1$ бўлса, у ҳолда ҳарбий хизматчининг жисмоний тайёргарлик даражаси аъло деб тушунилади, Агар $x_{pi}^4 = 2$ бўлса, у ҳолда ҳарбий хизматчининг жисмоний тайёргарлик даражаси яхши деб тушунилади, Агар $x_{pi}^4 = 3$ бўлса, у ҳолда ҳарбий хизматчининг жисмоний тайёргарлик даражаси қониқарли деб тушунилади, Агар $x_{pi}^4 = 4$ бўлса, у ҳолда ҳарбий хизматчининг жисмоний тайёргарлик даражаси қониқарсиз деб тушунилади, Демак, x_{pi}^4 - тўрт хил қиймат қабул қилади.

Қолган барча параметрлар ҳам $x_i^j, j = \overline{5,27}$ - қуйидаги қийматлардан бирини $x_i^j = 1$ (аъло); $x_i^j = 2$ (яхши); $x_i^j = 3$ (қониқарли); $x_i^j = 4$ (қониқарсиз) $j = \overline{5,27}$ қабул қилиши мумкин эканлиги таҳлили қилинди. Албатта, қўйилиши лозим бўлган баҳо эксперт мутахассислар томонидан аниқланади, ёки мутахассислар ишлаб чиққан компьютер тестлари орқали қўйилади.

Демак, юқорида келтирилган биринчи рақамлаштириш масаласи, ўз ечимини топади.

Юқорида шакллантирилган ҳар бир белги ҳарбий хизматчининг салоҳиятини характерловчи элементлар бўлиб, аскар ўз фаолияти давомида уларни ўзлаштириб, такомиллаштириб ва ривожлантириб боради. Бу жараён дастлаб ҳарбий хизматчининг қобилияти, тажрибаси ва маҳорат, кўрсаткичлари бўлиб, сўнгра буларнинг барчаси салоҳиятни ташкил этувчи белгилар мажмуасига айланади. ҳарбий хизматчи бўлинма шахсий таркибининг жанговор салоҳияти таърифига кўра шахсий таркибнинг комплектланганлигига, жанговор малака ва ахлокий-жанговор сифатларига, йўқотишлар ва уларни тўлдиролушига, моддий воситалар билан таъминланганлигига ва бошқа омилларга боғлиқ [62-64]. Агар бўлинма таъминоти идеал ҳолатда деб баҳоланса, бўлинманинг жанговор салоҳияти шахсий таркибнинг комплектланганлигига, жанговор малака ва ахлокий-жанговор сифатларига боғлиқ бўлиб қолади. Мазкур сифат кўрсаткичларни юқори бўлиши шахсий таркибнинг жанговор вазифанинг бажарилишида муҳим аҳамиятга эга. Бўлинмадаги ҳар бир ҳарбий хизматчининг жанговор салоҳиятини аниқланади, сўнг бўлинманинг жанговор салоҳиятига баҳо берилади.

Ҳарбий хизматчининг жанговор қобилияти деганда, аскар томонидан жанговор салоҳият белгилар мажмуаларини берилган вақтга нисбатан ўзлаштириш даражаларининг тезлиги тушунилади.

Ҳарбий хизматчининг жанговор салоҳияти деганда аскар томонидан жанговор салоҳият белгилар асосида эгаллаган билимлари ва кўникмаларидан фойдаланиб аниқ берилган кўрсатмани, топширикни амалда бажара олиш даражаси тушунилади. Одатда, бажара олиш даражалари аъло, яхши, қониқарли ва қониқарсиз деб баҳоланади.

Харбий хизматчининг жанговор қобилияти, ҳар хил ҳолатларда берилган топшириқларни бажара олиш жанговор салоҳиятлари доирасида, тажриба ва маҳоратларини ошириши унинг жанговор салоҳиятини белгилайди.

Харбий хизматчиларнинг жанговор салоҳиятларини аниқлашнинг ҳозирги ҳолати таҳлили.

АҚШ, Россия Федератсияси, Хитой, Англия, Франция ва бошқа ривожланган давлатлар армиялари сафида ҳарбий хизматга ўтишлари учун фуқоролар қуйидаги талаблар бўйича ўрганиб чиқилади:

- a) фуқороларни ўрганиш (хужжатларни йиғиш, ўрганиш ва суҳбат);
- b) ҳарбий кўриқдан ўтказиш (ҳарбий хизматга яроқлиги ва жисмоний ҳолати);
- c) психологик ўрганиш;
- d) жисмоний тайёргарлигини ўрганиш;
- e) интеллектуал салоҳиятини ўрганиш.

Фуқоролар мазкур талаблар бўйича ўрганиб чиқилади ва олинган натижалар асосан ҳарбий хизматчи сифатида ҳориж армияларига қабул қилинади.

Ўзбекистонда Ўзбекистон Республикаси пр.езидентининг 2019 йил 12 сентябрдаги 4447 сонли қарори билан тасдиқланган Ўзбекистон Республикаси фуқароларининг ҳарбий хизматни ўташ тартиби тўғрисидаги низомга кўра контракт бўйича ҳарбий хизматга номзодларни ҳарбий-касбий саралаш тартиби қуйидагиларни ўз ичига олади [1]:

- a) номзодни дастлабки урганиш (хужжатларни йиғиш ва ўрганиш, суҳбат);
- b) ҳарбий курик;
- c) психологик ўрганиш (интеллектуал ривожланганлик даражаси ва психоэмоционал барқарорлиги баҳоланади);
- d) жисмоний тайёргарлик даражасини баҳолаш;
- e) номзоднинг касбий нуктаи назардан ҳарбий хизмат учун муҳим сифатларини ўрганиш бўйича вазирлик томонидан белгиланувчи бошқа турдаги синов (текширув) турлари.

Мазкур босқичлардан юқори кўрсаткичлар билан ўтиш ҳарбий хизматнинг кейинги фаолиятида вазифаларни сифатли бажарилиши таъминлашда муҳим аҳамият касб этади.

Ривожланган давлатлар армияларида хусусан миллий армияларимиз сафида хизмат қилаётган ҳарбий хизматчилар ҳарбий-касбий сифат кўрсаткичларининг юқори бўлиши вазифаларни самарали бажарилишида муҳим деб ҳисобланади. Шунинг учун ҳам ҳарбий-касбий кўрсаткичлар доимий равишда ривожлантирилиб, ҳарбий хизматчиларнинг жанговор қобилиятлари баҳоланиб борилади.

Хулоса. Ҳарбий бўлинмалар жанговор салоҳиятларини аниқлаш усуллари таҳлили бўйича қуйидаги натижалар олинди. Бўлинма куруқликда душманни тор-мор этишга мўлжалланган қуроллар, танклар, пиёдаларга мослашган жанговор транспорт воситалари, бронотранспортёрлар, артиллерия ва миномётлар, танкларга қарши бошқариладиган ракетапар, зенит - ракета тизимлари ва қурилмалари, бошқарув ва разведканинг самарали воситалари билан жиҳозланганлиги ўрганилди. Ҳарбий бўлинмалар салоҳиятини аниқлаш, шахсий таркибнинг жанговор қобилияти ҳамда жанговор техника ва қуролларидан самарали фойдаланиши маҳорати билан белгиланади. Одатда, қўшин салоҳияти таркибдаги ҳар бир аскарнинг шахсий қобилияти, имкониятлари ва техник жиҳоз ва қуроллардан самарали фойдаланиш маҳорати тушунилади. Ҳарбий бўлинмаларнинг жанговор - техник имкониятларини аниқлаш усуллари таҳлили баён қилинди.

Фойдаланилган адабиётлар рўйхати:

[1] Mirshohid Aslanov. Reassessing Uzbekistan's military power: a case of underestimated strength // Defense.info (analiz maqola). — 2025.—Highlights reserve forces, budget, logistics for military readiness.

[2] President of the Republic of Uzbekistan. Issues of strengthening the country's defense capability discussed // Official press release. — 2025.—Feb 3 meeting on increasing combat readiness and personnel morale.

[3] Arslon APC introduction and troop modernization // Institute for Strategic and Regional Studies under the President of the Republic of Uzbekistan. — 2025.—Discusses modern equipment and doubling combat power.

[4] Reassessing Uzbekistan's military power... (Rossiya talqinida) // Daryo.uz rus versiyasi. — 2025.—Analysis in Russian of military potential.

[5] Armed Forces of the Republic of Uzbekistan (Wikipedia, includes Russian-language details) — 2025.—Covers structure, manpower, conscription

[6] Vulnerability Assessment Laboratory // Wikipedia. — Describes US Army's vulnerability analysis methods including combat systems.

[7] Center for Army Analysis // Wikipedia. — US Army organization for evaluating combat capability and force effectiveness.

[8] Joint Deployable Analysis Team // Wikipedia. — Covers US military joint analysis exercises to improve combat identification.

**CHET TILLARNI O'QITISH METODIKASINI TAKOMILLASHTIRISH: NAZARIY
ASOSLAR VA INNOVATSION YONDASHUVLAR****U.A. ALIBAYEVA***Oliy ta'lim tizimi kadrlarini qayta tayyorlash va malakasini oshirish instituti*

Annotatsiya. Ushbu ilmiy maqolada zamonaviy ta'lim sharoitida chet tillari o'qituvchilarining metodik tayyorgarligini takomillashtirishning nazariy asoslari tahlil qilingan. Tadqiqot metodik kompetentlikning dolzarb masalalarini, chet tillarni o'qitishning zamonaviy usullari va ularni amaliyotga tatbiq etish mexanizmlarini o'rganishga qaratilgan. Ilmiy jihatdan asoslangan xulosalar va pedagogik innovatsiyalarning samaradorligi haqida ma'lumotlar keltirilgan.

Kalit so'zlar: O'qitish metodikasi chet tillari, kasbiy kompetentlik raqamli pedagogika, CLIL texnologiyasi, refleksiv o'rganish.

Аннотация. В данной научной статье анализируются теоретические основы совершенствования методической подготовки преподавателей иностранных языков в условиях современного образования. Исследование посвящено актуальным проблемам методической компетентности, современным методам преподавания иностранных языков и механизмам их внедрения в практику. Приводятся научно обоснованные выводы и данные об эффективности педагогических инноваций.

Ключевые слова: методика преподавания, иностранные языки, профессиональная компетентность, цифровая педагогика, CLIL-технология, рефлексивное обучение.

Abstract. This scientific article examines the theoretical foundations of enhancing the methodological training of foreign language teachers in modern educational contexts. The study focuses on current issues in methodological competence, contemporary foreign language teaching methods, and implementation mechanisms. It presents research-based conclusions and data on the effectiveness of pedagogical innovations.

Keywords: teaching methodology, foreign languages, professional competence, digital pedagogy, CLIL technology, reflective learning.

Globalizatsiya sharoitida chet tillarini o'rganish ahamiyati ortib bormoqda. Bu esa o'qituvchilarning metodik tayyorgarligini sifat jihatidan yangi bosqichga ko'tarishni talab qiladi. Mazkur tadqiqot chet tillari o'qituvchilarining kasbiy kompetentligini oshirishning nazariy va amaliy jihatlarini kompleks o'rganishga bag'ishlangan.

Metodik tayyorgarligini rivojlantirishning nazariy asoslarini takomillashtirish degar mavzu ta'lim jarayonlarining samaradorligini oshirish, o'qituvchilarning kasbiy mahoratini rivojlantirish va o'quvchilarning bilim sifatini yaxshilash uchun metodik tayyorgarlikning ilmiy va amaliy asoslarini yangilash va takomillashtirishni ko'zda tutadi. Bu jarayonda zamonaviy ta'lim texnologiyalari, pedagogik tadqiqotlar va amaliy tajribalarning yangi natijalaridan foydalaniladi [2:50].

Metodik tayyorgarligini rivojlantirishning nazariy asoslarini takomillashtirishning asosiy yo'nalishlari:

1. Pedagogik nazariyalarni yangilash:

- Zamonaviy pedagogika nazariyalarini (masalan, konstruktivizm, interaktiv metodlar, individualashtirilgan ta'lim) metodik tayyorgarlikka tatbiq etish.

- O'qituvchilarning ijodiy fikrlashini rivojlantirishga yo'naltirilgan metodikalarni ishlab chiqish.

2. Ta'lim texnologiyalarini joriy etish:

- Axborot-kommunikatsiya texnologiyalari (AKT)ni metodik tayyorgarlikka keng joriy etish.

- Onlayn ta'lim, aralash ta'lim va distantsion ta'lim usullarini takomillashtirish.

3. Metodik materiallarni takomillashtirish:

- O'quv dasturlari, metodik qo'llanmalar va o'quv materiallarini zamonaviy talablarga moslashtirish.

- O'quvchilarning turli darajadagi tayyorgarligini hisobga olgan holda differensiallashtirilgan metodikalarni ishlab chiqish.

4. Tajriba va innovatsiyalarni tatbiq etish:

- Ilmiy tadqiqotlar va innovatsion tajribalarni metodik tayyorgarlikka tatbiq etish.

- O'qituvchilarning yangi metodikalarni o'zlashtirishi uchun malaka oshirish kurslarini tashkil etish.

5. Baholash tizimini takomillashtirish:

- O'quvchilarning bilim va ko'nikmalarini baholashning yangi metodlarini ishlab chiqish.

- Formativ va summativ baholash usullarini metodik tayyorgarlikka keng joriy etish.

6. Shaxsiy rivojlanishni qo'llab-quvvatlash:

- O'qituvchilarning shaxsiy va kasbiy rivojlanishini ta'minlash uchun metodik yordam ko'rsatish[6:30].

- O'qituvchilarning refleksiya qilish va o'z ishini takomillashtirish qobiliyatini rivojlantirish.

Ta'lim sifatini oshirish:

- Metodik tayyorgarlikni takomillashtirish orqali

- o'quvchilarning bilim va ko'nikmalarining sifatini oshirish.

O'qituvchilarning kasbiy mahoratini rivojlantirish:

- Yangi metodlar va texnologiyalarni o'zlashtirish orqali o'qituvchilarning kasbiy mahoratini oshirish.

Innovatsiyalarni joriy etish:

- Ta'lim jarayoniga yangilik va innovatsiyalarni kiritish.

Interaktiv metodlarni joriy etish:

- O'quvchilarning faol ishtirokini ta'minlash uchun interaktiv metodlardan foydalanish.

AKTni tatbiq etish:

- Virtual laboratoriyalar, onlayn platformalar va multimedia vositalarini metodik tayyorgarlikka kiritish.

Differensiallashtirilgan ta'lim:

- O'quvchilarning turli darajadagi tayyorgarligini hisobga olgan holda metodikalarni ishlab chiqish.

Tez o'zgarib turgan dunyo va ilg'or texnologiyalarning rivojlanishi sharoitida uzluksiz ta'lim chet tillari o'qituvchilarining kasbiy hayotining ajralmas qismiga aylanmoqda. Uslubiy tayyorgarlikni takomillashtirish bilim, ko'nikma va o'qitish uslublarini doimiy yangilashni talab qiladi. Chet tillari o'qituvchilarining uslubiy tayyorgarligini takomillashtirishda uzluksiz ta'limning o'rnini o'rganish, shuningdek, bu jarayonning asosiy shakllari, usullari va muammolarini aniqlashdir.

Uzluksiz ta'lim – bu butun kasbiy hayot davomida bilim, ko'nikma va kompetensiyalarni doimiy yangilash va kengaytirish jarayonidir. Texnologiyalar va o'qitish usullari tez rivojlanayotgan zamonaviy dunyoda uzluksiz ta'lim o'qituvchilar uchun muvaffaqiyatning asosiy omilidir. Bu eng so'nggi tendentsiyalar bilan tanishish, o'zgarishlarga moslashish va o'qitish sifatini oshirish imkonini beradi.

Uzluksiz ta'lim orqali uslubiy tayyorgarlikni takomillashtirish:

1. Nazariy bilimlarni yangilash:

Uzluksiz ta'lim o'qituvchilarga lingvistika, pedagogika va o'qitish metodikasi sohasidagi eng yangi tadqiqotlar bilan tanishishga yordam beradi. Bu nazariy bazani boyitish va zamonaviy yondashuvlarni amaliyotda qo'llash imkonini beradi.

2. Amaliy ko'nikmalarni rivojlantirish:

Malakani oshirish kurslari va amaliy seminarlar yangi usullar va texnologiyalarni amaliyotda o'zlashtirish imkonini beradi. Bu ta'lim jarayonida interaktiv va raqamli vositalarni joriy etish uchun ayniqsa muhimdir.

3. Yangi texnologiyalar va usullarni joriy etish:

Uzluksiz ta'lim raqamli platformalar, mobil ilovalar va boshqa texnologiyalarni o'zlashtirishga yordam beradi, bu esa o'quvchilar uchun ta'limni samaraliroq va qiziqarliroq qiladi.

Uzluksiz ta'limning shakllari va usullari:

1. Malakani oshirish kurslari:

Ushbu dasturlar o'qitishning alohida jihatlari, masalan, kommunikativ yondashuv, texnologiyalardan foydalanish yoki madaniyatlararo kommunikatsiyani chuqurroq o'rganishni taklif qiladi.

2. Vebinar, onlayn kurslar va MOOCs:

Onlayn formatlar o'qituvchilarga qulay vaqtda va istalgan joyda o'qish imkonini beradi. Ochiq massiv onlayn kurslar (MOOCs) dunyoning yetakchi universitetlari materiallariga kirish imkonini beradi.

3. Konferensiyalar va seminarlarda ishtirok etish:

Kasbiy tadbirlar tajriba almashish, yangi tendentsiyalar haqida bilim olish va hamkasblar bilan aloqalar o'rnatish imkonini beradi.

4. O'z-o'zini o'qitish va kasbiy hamjamiyatlar:

O'qituvchilar mustaqil ravishda adabiyot o'rganishi, forumlar va ijtimoiy tarmoqlardagi munozaralarda qatnashishi, shuningdek, o'z ishlanmalarini hamkasblari bilan baham ko'rishi mumkin[5:30].

Uzluksiz ta'limning amaliy jihatlari.

1. Malakani oshirishning muvaffaqiyatli dasturlari misollari:

Ko'plab universitetlar va ta'lim markazlari nazariy bilimlarni amaliy vazifalar bilan birlashtirgan dasturlarni taklif qiladi. Masalan, sun'iy intellektdan foydalanish bo'yicha kurslar.

2. O'z-o'zini o'qitish uchun raqamli platformalardan foydalanish:

Coursera, EdX va FutureLearn kabi platformalar o'qitish metodikasi, raqamli texnologiyalar va pedagogik dizayn bo'yicha kurslarni taklif qiladi.

3. Professional o'sishda fikr-mulohaza va o'z-o'zini baholash roli:

Hamkasblar va o'quvchilardan muntazam ravishda fikr-mulohaza olish va o'z-o'zini baholash o'qituvchilarga kuchli va zaif tomonlarini aniqlashga va ularni yaxshilash uchun ishlashga yordam beradi.

Uzluksiz ta'limdagi qiyinchiliklar va muammolar.

1. Vaqt va resurslarning yetishmasligi

Ko'plab o'qituvchilar ta'lim dasturlarida ishtirok etish uchun vaqt yetishmasligi va moliyalashtirishning cheklanganligi bilan duch kelishadi.

2. O'zgarishlarga qarshilik

Hammasi o'qituvchilar yangi texnologiyalar va usullarni joriy etishga tayyor emas, bu ularning professional rivojlanish jarayonini sekinlashtirishi mumkin.

3. Ta'lim resurslariga tengsiz kirish

Ba'zi hududlarda malakani oshirishning sifatli dasturlari va raqamli resurslarga kirish cheklangan, bu professional o'sish uchun tengsiz sharoitlarni yaratadi.

Uzluksiz ta'lim chet tillari o'qituvchilarining uslubiy tayyorgarligini takomillashtirishda hal qiluvchi rol o'ynaydi. Bu bilimlarni yangilash, ko'nikmalarni rivojlantirish va yangi texnologiyalarni joriy etish imkonini beradi, bu esa ta'lim sifatini oshirishga yordam beradi. Biroq, bu jarayonni muvaffaqiyatli amalga oshirish uchun resurslarning yetishmasligi va ta'lim imkoniyatlariga tengsiz kirish kabi muammolarni hal qilish kerak. Kelajakda har bir o'qituvchining so'nggi tendentsiyalar bilan tanishishi va professional kompetensiyalarini takomillashtirishi uchun moslashuvchan va qulay ta'lim formatlarini rivojlantirish muhimdir.

Ta'lim sifatini ta'minlashda o'qituvchilarning uslubiy tayyorgarligi asosiy o'rin tutadi. U o'qituvchilarning kasbiy kompetensiyalarini shakllantirish, zamonaviy texnologiyalarni o'zlashtirish va shaxsiy fazilatlarini rivojlantirishga yo'naltirilgan bo'lishi kerak. Tez o'zgarib borayotgan dunyoda o'qituvchilar zamonaviy ta'lim muammolarini muvaffaqiyatli yengishlari uchun metodik tayyorgarlik moslashuvchan, innovatsion va amaliyotga yo'naltirilgan bo'lishi kerak. O'qituvchilarning metodik tayyorgarligini oshirishda uzluksiz ta'lim asosiy o'rin tutadi. Bu o'qituvchilarga ta'lim sohasidagi so'nggi tendensiyalardan xabardor bo'lish, kasbiy kompetensiyalarni rivojlantirish va o'qitishning innovatsion usullarini joriy etish imkonini beradi. Tez o'zgarib borayotgan dunyoda uzluksiz ta'lim nafaqat zarurat, balki muvaffaqiyatli kasbiy faoliyat garoviga ham aylanmoqda.

Zamonaviy dunyoda informatsion texnologiyalar (IT) ta'lim sohasida muhim rol o'ynab, o'qitish uslublari va pedagoglarning metodik tayyorligini tubdan o'zgartirmoqda. Bu, ayniqsa, chet tillar o'qituvchilari uchun muhim ahamiyatga ega, chunki ularning faoliyati aloqa, madaniy almashinuv va ta'lim samaradorligini oshirish uchun zamonaviy vositalardan foydalanish bilan bevosita bog'liq. ITni chet tillar o'qituvchilarining metodik tayyorligiga joriy etish yangi imkoniyatlarni ochadi, bu esa ularning kasbiy ko'nikmalarini oshirish, ta'lim sifatini yaxshilash va raqamli davr talablariga moslashishga yordam beradi[1:40].

Informatsion texnologiyalar o'qituvchilarga ko'plab ta'lim resurslariga kirish imkoniyatini beradi: onlayn kurslar, vebinar, elektron kutubxonalar, ma'lumotlar bazalari, tillarni o'rganish uchun maxsus platformalar va boshqalar. Bu pedagoglarga doimiy ravishda bilimlarini yangilash, yangi metodika va yondashuvlarni o'rganish, shuningdek, butun dunyo bo'ylab hamkasblari bilan tajriba almashish imkoniyatini beradi. Masalan, Coursera, EdX kabi platformalar yoki chet tillar o'qituvchilari uchun mo'ljallangan resurslar metodika, raqamli vositalardan foydalanish va ta'limda innovatsion yondashuvlar bo'yicha kurslarni taklif etadi.

Zamonaviy chet tillar o'qituvchilari ta'lim jarayonini samaraliroq qilish uchun raqamli vositalar bilan tanishishi kerak. Bular quyidagilarni o'z ichiga oladi:

Interaktiv platformalar (masalan, Duolingo, Quizlet, Kahoot), qiziqarli topshiriqlar va testlar yaratish imkoniyatini beradi.

Virtual sinflar (Zoom, Microsoft Teams, Google Classroom), onlayn formatda dars o'tish imkoniyatini yaratadi.

Multimedia resurslar (audio, video, podkastlar), tinglash va gapirish ko'nikmalarini rivojlantirishga yordam beradi.

Sun'iy intellekt va chatbotlar, topshiriqlarni avtomatik tekshirish va fikr-mulohazalar berish uchun ishlatilishi mumkin.

Metodik tayyorlik dasturlari o'qituvchilarga ushbu vositalar bilan ishlashni o'rgatishni o'z ichiga olishi kerak, shunda ular ularni o'quv jarayoniga samarali integratsiya qilishlari mumkin[4:20].

Raqamli savodxonlik o'qituvchilarning kasbiy kompetensiyasining ajralmas qismiga aylanmoqda. Bu nafaqat texnologiyalardan foydalanish qobiliyatini, balki ularning ta'lim jarayoniga ta'sirini tushunishni ham o'z ichiga oladi. O'qituvchilar quyidagilarga qodir bo'lishlari kerak:

Raqamli resurslarning sifatini baholash.

O'quvchilar ma'lumotlarini himoya qilish va ITdan foydalanishda axloqiy me'yorlarga rioya qilish.

Texnologiyalarni o'quvchilarning individual ehtiyojlariga moslashtirish.

Metodik tayyorlik raqamli savodxonlikni rivojlantirishga bag'ishlangan modullarni o'z ichiga olishi kerak, shunda o'qituvchilar texnologiyalarni ishda ishonchli tarzda qo'llashlari mumkin[6:40].

Informatsion texnologiyalar o'quvchilar uchun shaxsiylashtirilgan ta'lim yo'nalishlarini yaratish imkoniyatini beradi. O'qituvchilar raqamli vositalar orqali olingan ma'lumotlardan

foydalanib, talabalarning progressini tahlil qilish, ularning zaif tomonlarini aniqlash va individual topshiriqlar taklif qilishlari mumkin. Bu pedagoglardan analitik vositalar bilan ishlash va metodikalarni muayyan vazifalarga moslashtirish qobiliyatini talab qiladi.

IT geografik chegaralarni yo'qotib, o'qituvchilarga xalqaro loyihalar, konferensiyalar va tadqiqotlarda ishtirok etish imkoniyatini beradi. Bu tajriba almashish, eng yaxshi amaliyotlarni joriy etish va madaniyatlararo aloqani rivojlantirishga yordam beradi. Masalan, o'qituvchilar boshqa mamlakatlardagi hamkasblari bilan onlayn seminarlarda qatnashishlari mumkin, bu ularning metodik qurol-yarog'ini boyitadi [3:60].

Xulosa qilib shuni ta'kidlash joizki, Informatsion texnologiyalar chet tillar o'qituvchilarining metodik tayyorligining ajralmas qismiga aylanmoqda. Ular kasbiy rivojlanish, ta'lim sifatini yaxshilash va zamonaviy dunyo talablariga moslashish uchun yangi imkoniyatlar ochadi. Biroq, ITni muvaffaqiyatli joriy etish tizimli yondashuvni talab qiladi, shu jumladan raqamli savodxonlikni o'qitish, zamonaviy vositalar bilan ishlash ko'nikmalarini rivojlantirish va bog'liq qiyinchiliklarni yengish. Bu o'qituvchilarga nafaqat texnologiyalarni samarali qo'llash, balki o'qituvchilarini chet tillarini o'rganishda yangi yutuqlarga erishishga ilhomlantirish imkoniyatini beradi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

[1] Abdullayeva, N. S. (2020). Lexical-semantic and cognitive specifics of political discourse (based on Si Jinping's speeches). *ACADEMICIA: An International Multidisciplinary Research Journal*, 70(5), 1086-1092.

[2] Anderson T. va Boye J. (2021). Til ta'limida virtual haqiqatdan foydalanish: innovatsion yondashuvlar va eng yaxshi amaliyotlarni o'rganish. *Ta'lim texnologiyasi jurnali*, 28(3), 87-104.

[3] Martinez S. va boshqalar. (2018). Til o'rgatishda onlayn platformalarning o'rni: o'qituvchilar faolligini va ta'lim natijalarini oshirish. *Kompyuter yordamida til o'rganish jurnali*, 25(4), 301-315.

[4] European Commission (2022). *Raqamli ta'lim bo'yicha harakatlar rejasi*.

[5] Richards, J.C. (2023). *Til o'qitish usullari va yondashuvlari*. Cambridge University Press.

[6] Verma, S. (2019). *Til o'qitishdagi zamonaviy pedagogik texnologiyalar*. London: Routledge.

HARBIY XIZMATCHILARNI TA'LIM-TARBIYA JARAYONIDA MUSTAQIL
FIKRLASH VA ILMIY DUNYOQARASHNI SHAKLLANTIRISH**dotsent A.Sh. XUDAYAROV, dotsent X. J. QOSIMOV***O'R MV Axborot kommunikatsiya texnologiyalari va aloqa harbiy instituti*

Annotatsiya. Ilmiy dunyoqarash tushunchasi va ilmiy dunyoqarashga ega bo'lishning ahamiyati. Shaxs kamolotida u tomonidan moddiy, ijtimoiy borliqni qabul qilish asosida muayyan dunyoqarashga ega bo'lib borishi muhim ahamiyatga ega. Dunyoqarashga ega bo'lish shaxsda atrof-muhit, ijtimoiy munosabatlar, mehnat faoliyati va ishlab chiqarish jarayoni, sub'ektlarga nisbatan ma'lum munosabatning qaror topishi, shaxs tomonidan zimmasidagi ijtimoiy burchlarini to'laqonli anglash va ularni bajarishga nisbatan mas'uliyat tuyg'usiga ega bo'lishi uchun zamin yaratadi.

Kalit so'zlar: atrof-muhit, ijtimoiy munosabatlar, mehnat faoliyati va ishlab chiqarish jarayoni, sub'ektlarga nisbatan ma'lum munosabatning qaror topishi, shaxs, o'rniga, o'z-o'ziga, qarashlari, e'tiqodi, falsafiy dunyoqarash, estetik dunyoqarash.

Аннотация. Понятие научного мировоззрения и значение научного мировоззрения. Немаловажное значение в созревании личности имеет то, что она приобретает определенное мировоззрение, основанное на принятии ею материального, социального бытия. Мировоззрение закладывает основу для того, чтобы у человека сложилось определенное отношение к окружающей среде, общественным отношениям, трудовой деятельности и производственному процессу, к субъектам, было полное осознание индивидом своих социальных обязанностей и чувство ответственности за их выполнение.

Ключевые слова: окружающая среда, общественные отношения, трудовая деятельность и производственный процесс, определение определенного отношения к субъектам, личность, место, я, взгляды, убеждения, философское мировоззрение, эстетическое мировоззрение.

Abstract. The concept of an ordinary worldview and the importance of having a scientific worldview. In the maturation of a person, it is important that he acquires a certain worldview on the basis of the acceptance by him of a material, Social being. Having a worldview sets the stage for an individual to have a sense of responsibility for the environment, social relations, labor activity and the production process, the decision-making of a certain attitude towards the subjects, a full-fledged understanding of his social duties on the part of the individual and their fulfillment

Key words: environment, social relations, labor activity and the production process, decision-making of a certain attitude towards subjects, personality, instead, self, views, beliefs, philosophical worldview, aesthetic worldview.

Dunyoqarashga ega bo'lish shaxsda atrof-muhit, ijtimoiy munosabatlar, mehnat faoliyati va ishlab chiqarish jarayoni, sub'ektlarga nisbatan ma'lum munosabatning qaror topishi, shaxs tomonidan zimmasidagi ijtimoiy burchlarini to'laqonli anglash va ularni bajarishga nisbatan mas'uliyat tuyg'usiga ega bo'lishi uchun zamin yaratadi.

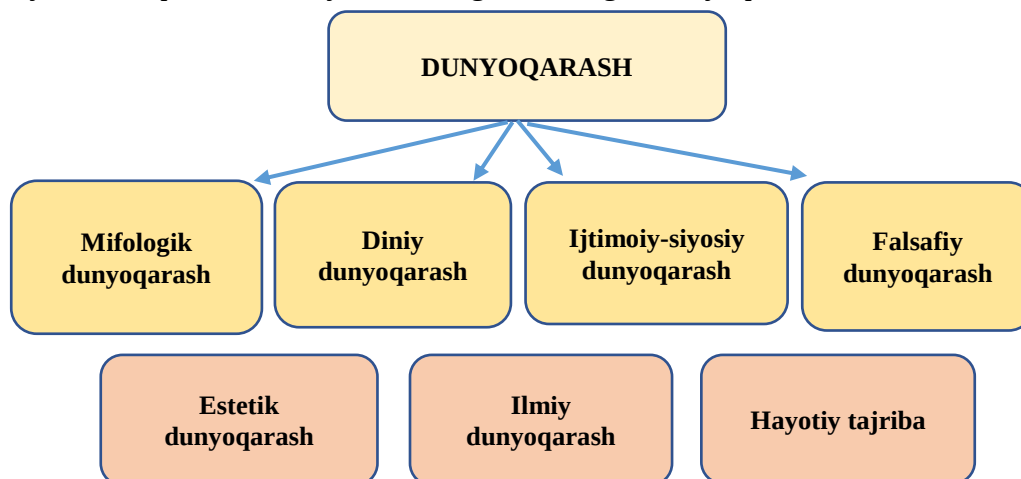
Yosh avlod dunyoqarashining shakllanishida tabiiy, ijtimoiy va gumanitar fanlar asoslarining ular tomonidan puxta o'zlashtirilishi muhim ahamiyatga ega. Dunyoqarashning boyib borishi shaxsiy sifat va fazilatlarni boyitadi, barqarorlashtiradi [1].

Mifologik dunyoqarash – ibtidoiy jamoa tuzumida borliqni obrazli qabul qilish asosida shakllangan tasavvurlar majmuasini ifodalovchi dunyoqarash. “Mifologiya” tushunchasining o'zi (yunonchadan “mythos” – afsona, rivoyat, “logos” – fan, ta'limot) biror xalqqa tegishli afsonalar ma'nosini anglatadi. Diniy dunyoqarash – borliqni ilohiy kuchga, Xudoga ishonish asosida qabul qilishni ifodalovchi tasavvurlar, urf-odatlar va marosimlar majmui. Arab tilidan tarjima qilinganda “din” tushunchasi “ishonch”, “e'tiqod” ma'nolarini anglatadi.

Ijtimoiy-siyosiy dunyoqarash – kishilarning ob'ektiv mavjud bo'lgan siyosiy hayotga nisbatan siyosiy qarashlarining, siyosiy faoliyatga nisbatan munosabatlarining umumlashtirilgan tizimi.

Falsafiy dunyoqarash – tabiiy va ijtimoiy borliqni nazariy qabul qilish, shaxsning borliqqa nisbatan falsafiy munosabatiga asoslangan dunyoqarash. “Falsafa” tushunchasining o'zi qadimgi grek tilidan tarjima qilinganda “φιλία” – muhabbat, intilish, ishtiyoq, “σοφία” – donishmandlik, so'zma-so'z tarjima qilinganda esa “filosofiya” “donishmandlikka intilaman” ma'nosini anglatadi.

Estetik dunyoqarash – tabiiy va ijtimoiy borliqqa estetik qadriyatlar – go'zallik, xunuklik, kulguli, fojiaiy va boshqalar asosida yondashishga asoslangan dunyoqarash.



1-rasm. Dunyoqarash turlari

Ilmiy dunyoqarash uzluksiz, izchil ravishda insoniyat tomonidan orttirilgan, mavjud ilmiy bilimlarni puxta o'zlashtirish, hayotiy tajribani orttirish asosida shakllanadi. Shaxs dunyoqarashini shakllantirish uzoq muddatli, dinamik xususiyatga ega jarayon sanaladi.

Hayotiy tajriba – shaxsning umri davomida orttirgan tajribalari. Shaxs ilmiy dunyoqarashining shakllanishida aqliy tarbiya muhim o'rin tutadi [2].

Aqliy tarbiya o'quvchilarni ilm-fan, texnika, texnologiya va ishlab chiqarishda qo'lga kiritilayotgan yutuqlar bilan tanishtirish, ularda ijodiy, erkin, mustaqil fikrlash ko'nikmalarini hosil qilishga zamin yaratadi. Aqliy tarbiya jarayonida quyidagi vazifalarni hal etish orqali shaxsda dunyoqarash, ilmiy dunyoqarash shakllantiriladi:

Aqliy ta'lim va tarbiya birligi asosida shaxsda tafakkur (ijtimoiy voqea-hodisalarning ongda to'laonli aks etishi, inson aqliy faoliyatining yuksak shakli) rivojlanadi. Aqliy tafakkurning mavjud darajasini belgilash bir qadar murakkab bo'lib, quyidagi belgi (mezon)larga ko'ra aniqlanishi mumkin: 1. Ilmiy bilimlar tizimining mavjudligi. 2. Mavjud ilmiy bilimlarni o'zlashtirib olish jarayoni. 3. Fikrlash ko'nikmasiga egalik. 4. Bilimlarni egallashga bo'lgan qiziqish hamda ehtiyojning yuzaga kelganligi. Aqliy tafakkur uzoq muddat hamda tinimsiz izlanish natijasida yuzaga kelib, uning negizida ilmiy qarash va e'tiqod yotadi [3].

Aqliy tarbiyani samarali tashkil etish shaxsda ilmiy tafakkurni rivojlantiradi. Ilmiy tafakkur inson aqliy faoliyatining yuksak shakli sanalib, ijtimoiy voqea-hodisa

va jarayonlarga ilmiy yondashuvni anglatadi. E'tiqod dunyoqarash negizida aks etuvchi ijtimoiy-falsafiy, tabiiy, iqtisodiy, huquqiy, ma'naviy-axloqiy, estetik va ekologik bilimlarning takomillashgan ko'rinishi; muayyan g'oyaga cheksiz ishonchdir. U bir necha bosqichda shakllanadi: 1) bilimlar beqaror va vaziyat taqozosiga ko'ra o'zgaruvchanlik xususiyatini kasb etadi; 2) ma'naviy-axloqiy qarashlar barqaror tamoyillarga aylanadi;

3) barcha vaziyatlarda ham ustuvor ma'naviyaxloqiy tamoyil bo'lib qoladi.

Shaxsning ilmiy dunyoqarashga ega bo'lishi, ilmiy bilimlarni o'zlashtirib borishi katta ahamiyatga ega. Buning afzalliklari quyidagilarda ko'rinadi:

- 1) tabiat, jamiyatda ro'y berayotgan voqea, hodisalar mohiyatini to'g'ri talqin eta oladi;
- 2) o'ziga va atrofdagilarga nisbatan oqilona munosabatda bo'la oladi;
- 3) hech qachon dalillar bilan isbotlanmagan voqelik va hodisalarni haqiqat sifatida qabul qilmaydi;
- 4) ilmiy dunyoqarashga egalik shaxsda mustaqil fikrlash qobiliyatini rivojlantiradi;
- 5) zamonaviy sharoitda inson ongini boshqarish ilinjida yurgan turli oqimlar, ularning missionerlik faoliyatlari ta'siriga, mistik g'oyalarga berilmaydi;
- 6) shaxsiy hayotida, ijtimoiy jamiyatda ro'y berayotgan o'zgarishlarning muayyan qonuniyatlarga asoslanishiga ishonadi va ularni tabiiy qabul qiladi;
- 7) o'zining va jamiyat hayotida sodir bo'layotgan salbiy hodisalarni o'tkinchi sifatida qabul qiladi hamda kelajakka ishonch bilan qaraydi [4].

Ta'lim muassasalarida tashkil etiladigan ta'lim-tarbiya jarayonida asosiy e'tibor shaxsda dunyoqarashni shakllantirishga qaratiladi. Zero, dunyoqarashga ega shaxsgina tabiiy va ijtimoiy borliqni borligicha qabul qila oladi, o'ziga va atrofdagilarga nisbatan to'g'ri munosabatda bo'ladi. Mustaqillik sharoitida O'zbekiston Respublikasida o'quvchilarda dunyoqarashni shakllantirish, ularda yuksak ma'naviy-axloqiy sifatlarni tarbiyalash shaxsni har tomonlama kamol toptirish, komil inson, malakali mutaxassisni tarbiyalashdek ijtimoiy maqsad bilan bevosita bog'liq. Ta'lim muassasalarida ijtimoiy, gumanitar va texnik fanlar asoslarini o'qitish, o'quvchilarning texnik, badiiy ijodkorlik qobiliyatlarini tarbiyalash, turli ijtimoiy faoliyat turlarini tashkil etishga mantiqiy yondashish, har bir jarayonning ilmiy asoslarini izlashga o'rgatish ularning dunyoqarashlarini boyitishga yordam beradi.

Dunyoqarashni shakllantirishda o'quvchilarni badiiy asarlar, milliy va umuminsoniy qadriyatlarni ulug'laydigan san'at namunalari – kinofilmlar, teatr tomoshalari, konsert dasturlari bilan yaqindan tanishtirish ularda o'ziga, atrof-muhitga ijobiy munosabatni qaror toptiradi. Binobarin, san'at asarlari, xususan, rassomlik namunalari o'quvchilarda estetik his-tuyg'ularni shakllantirishga, badiiy asarlar esa ular tomonidan hayot, uning asl mazmunini anglab yetishga xizmat qiladi. Fantastik janrdagi asarlar esa o'quvchilarda bir necha o'n yillardan so'ng ro'y berishi mumkin bo'lgan hayotiy voqeliklar bilan avvaldan tanishish imkoniyatini yaratadi. Bu o'rinda o'quvchilarga J.Vern asarlarida yoritilgan hodisalar qariyb yuz yildan so'ng hayotiy haqiqatga aylanganligini e'tirof etib o'tish lozim. Ayni o'rinda o'quvchilarga zamonaviy texnologiyalar – kompyuterlar va mobil telefonlarning shaxslararo munosabatlarda axborot almashish borasidagi rolini inkor etmagan holda ulardan to'g'ri, maqsadli foydalanishga oid tavsiyalarni berish ularda dunyoqarashini boyitishni ta'minlaydi [5].

Shaxs dunyoqarashini shakllantirishda mehnat omilining roli beqiyos. Shu sababli o'quvchilarni yoshlikdanoq mehnat va turli ko'rinishdagi mehnat faoliyatlari bilan yaqindan tanishtirib borish, ular tomonidan mehnatni tashkil etishga ilmiy yondashish ko'nikma, malakalarining samarali o'zlashtirilishiga erishish oila, ta'lim muassasalarida tashkil etilayotgan tarbiya samaradorligini baholash imkoniyatini yaratadi.

Ta'lim muassasalarida o'quvchilarni Islom dinining muqaddas manbalari – Qur'oni karim, Hadisi shariflarda ilgari surilgan ma'naviy-axloqiy g'oyalar bilan yaqindan tanishtirib borish ham ular tomonidan g'oyaviy e'tiqod mohiyatining to'g'ri anglanishini ta'minlaydi. Qolaversa, o'quvchilarni turli millat va elatlarning milliy madaniyatiga tobora kuchli tahdid solayotgan – “ommaviy madaniyat” ta'siridan himoyalash imkoniyatini yaratadi. O'quv fanlari bo'yicha tashkil etiladigan mashg'ulotlar bilan sinfdan, ta'lim muassasasidan tashqarida uyushtiriluvchi tadbirlar o'rtasida o'zaro aloqadorlikka erishish, oila, ta'lim muassasalari va jamoatchilik hamkorligini qaror toptirish asosida ma'naviy-ma'rifiy ishlarni uyushtirish o'quvchilarda dunyoqarashni shakllantirishga nisbatan tizimli yondashuv mohiyatini ifodalaydi.

Dunyoqarash, uning mohiyati, shaxsda dunyoqarashni shakllantirishga oid qarashlar o'quvchilarda dunyoqarashning shakllanganligini quyidagi mezonlar asosida aniqlash mumkin, degan xulosaga kelish imkonini beradi:

1. Tabiiy jarayonlar mohiyatini tushuna olish, tabiatda ro'y berayotgan o'zgarishlarning asosi tabiiy qonuniyatlar ekanligini anglash orqali unga nisbatan oqilona munosabatda bo'lish.

2. Jamiyatda sodir bo'layotgan o'zgarishlarga to'g'ri baho bera olish, ijtimoiy voqeliklarning asosida mustaqil davlatning ijtimoiy, iqtisodiy va madaniy taraqqiyot yo'lini belgilab beruvchi milliy istiqlol g'oyasi, uning tamoyillari yotganligini anglab yetish.

3. O'zining shaxs sifatida jamiyatda tutgan o'rniga munosib baho bera olish, o'quvchi sifatida zimmasidagi burch, majburiyatlarni chuqur anglash.

4. O'z shaxsiga baho bera olish, ijobiy va salbiy sifatlarini ko'ra bilish, imkon qadar salbiy sifatlarini bartaraf etish uchun o'z ustida ishlash.

5. O'quv fanlarining asoslarini, ilmiy bilimlarni puxta o'zlashtirish, zamonaviy texnika va texnologiyalardan xabardor bo'lish, ijtimoiy voqeliklarga to'g'ri yondashib, turli buzg'unchi oqimlar ta'siriga berilmaslik orqali shaxs sifatida o'zini-o'zini takomillashtirish.

6. O'zlashtirgan ilmiy bilimlarini amaliyotda bevosita qo'llay olish ko'nikma, malakalarini o'zlashtirib borish.

Noana'anaviy dars shakllari, xususan, bahs-munozara, davra suhbat, debat, axloqiy mavzulardagi ma'ruza, uchrashuv, muammoli vaziyatlarni yaratish, interfaol metodlarga asoslangan mashg'ulotlarni tashkil etish shaxs dunyoqarashini samarali shakllantirishga yordam beradi [6].

O'quvchilarni vatanparvarlik ruhida tarbiyalash. Fuqarolik tarbiyasini tashkil etish jarayonida shaxsda vatanparvarlik (lotincha "patriots" – vatandosh, "patris" – vatan, yurt) tuyg'usini shakllantirishga e'tibor qaratiladi. Zero, fuqaro davlatning a'zosi sifatida uning sha'ni, obro'e'tiborini ta'minlashi, manfaatlari uchun kurasha olishi zarur.

Harbiy vatanparvarlik tarbiyasi yoshlarni vatan himoyasi, harbiy mudofaaga tayyorlash, ularda favqulotda holatlarda harbiy mudofaani tashkil etish ko'nikma, malakasini shakllantirishga yo'naltirilgan pedagogik jarayon.

Harbiy-vatanparvarlik tarbiyasining maqsadi yoshlarni vatan himoyasi hamda harbiy mudofaaga tayyorlash, ularda favqulotda holatlarda harbiy mudofaani tashkil etish ko'nikma, malakalarini shakllantirishdan iborat bo'lib, mazkur jarayonda quyidagi vazifalar amalga oshiriladi:

Harbiy-vatanparvarlik tarbiyasini tashkil etishda ta'lim muassasalarida o'qitilishi yo'lga qo'yilgan boshlang'ich harbiy tayyorgarlik mashg'ulotlari muhim ahamiyatga ega. O'quvchilar o'rtasida Chaqiriqqa qadar boshlang'ich tayyorgarlik (ChQBT) fani bo'yicha o'zlashtirilgan nazariy va amaliy bilimlarni namoyish etish imkonini beruvchi musobaqaning tashkil etilishi bu borada ijobiy natija bera oladi. O'qituvchi rahbarligida "Shon-shuhrat" muzeylariga uyushtiriladigan ekskursiyalar ham o'quvchilarda harbiy– vatanparvarlik tuyg'usini shakllantirishda muhim rol o'ynaydi.

Shaxsda o'zlikni anglash hissining namoyon bo'lishi va uning ma'naviy qadriyatlarga ega bo'lishini ta'minlash. "O'zlikni anglash" tushunchasi psixologik kategoriya sanalsa-da, biroq, shaxs ma'naviyati va uni shakllantirish masalalari o'ziga xos dolzarblik kasb etgan mavjud sharoitda falsafiy, ma'naviy-axloqiy tushuncha sifatida ham keng qo'llanilmoqda. O'zlikni anglash o'z-o'zini anglash, o'z-o'zini bilish kabi tushunchalar orqali ham ifodalanadi. Psixologik nuqtai nazardan o'zlikni anglash – bu shaxsning o'z-o'zini tushunishi orqali shaxsiy psixologik va fizik xususiyatlarini o'rganishi³³ sanaladi. Boshqacha aytganda, o'zlikni anglash shaxs tomonidan o'z "meni"ni tushunish, o'z xarakteri, xulq-atvori, hatti-harakatlari va qobiliyatlarini baholay olishdir. Shu bilan birga pedagogik nuqtai nazardan o'zlikni anglash – bu shaxs tomonidan o'z qadr-qimmatini, g'ururini baholay olishi, jamiyatda, oilada, bolalar jamoasi (umuman jamoada, mehnat jamoasida va b.)da tutgan o'rnini belgilay bilishi, atrofdagilarning unga, uning atrofdagilarga, qolaversa, tabiatga bo'lgan munosabatini ham anglab yetishi demakdir. O'zlikni anglash jarayoni shaxsda juda yoshlikdan boshlanib, butun hayoti davomida kechadi, ongda tashqi dunyoning aks etishi kabi jarayonlar ham bosqichma-bosqich ro'y beradi [7].

Axloqiy his-tuyg'ular va axloqiy ong. Shaxs dunyoqarashining shakllanishida ma'naviy-axloqiy tarbiya ham muhim o'ringa ega bo'lib, uni samarali tashkil etish o'quvchida ma'naviy-

axloqiy ongni shakllantirishga yordam beradi. Axloq va axloqiy me'yorlar axloqiy tarbiyaning asoslaridir.

Axloq (lotincha "moralis" – xulq-atvor) ijtimoiy munosabatlarni, shaxs xatti-harakatini tartibga soluvchi, jamiyat tomonidan tan olinib, rioya qilinishi zarur bo'lgan xulq-atvor qoidalari yig'indisi. Axloqiy tarbiyaning natijasi o'quvchilarda axloqiy ong va faoliyat ko'nikmalari, axloqiy madaniyat shakllanishida ko'rinadi.

Shaxsning axloqiy xulq-atvori. Xulq-atvor – shaxsning fe'li, xarakteri bilan bog'liq ma'naviy hodisa, fe'lining axloqiylik doirasida namoyon bo'lishi³⁴. Ijtimoiy munosabatlar jamiyat tomonidan tan olingan, garchi majburiy bo'lmasa-da, biroq, omma fikri bilan tartibga solinadigan axloqiy me'yorlarga muvofiq tashkil etiladi. Shaxsning xulq-atvori axloqiy me'yorlarga muvofiq shaxslararo munosabatlarni tashkil etish vaqtida namoyon bo'ladi. Shaxs xulq-atvori uning ijobiy yoki salbiy sifatlarga egaligini ko'rsatadi. Agarda shaxs ijobiy ma'naviy-axloqiy sifatlarga ega bo'lsa, u holda uning xulq-atvorida tabiatga to'g'ri munosabat, atrofda qilargaga g'amxo'rlik, yaqinlariga mehribonlik, shaxslararo munosabatlarda xushmuomalalik, mehnat jarayonida mehnatsevarlik, jismoniy mashqlarni bajarishda kuchlilik, epchillik, chaqqonlik, o'z shaxsini baholashda kamtarinlik, o'jizlarga nisbatan saxovatlilik, Vatanga nisbatan vatanparvarlik, haqiqatga nisbatan haqiqatgo'ylik, har bir ishni bajarishda vijdonan ish ko'rish kabi hodisalar ro'y bersa, salbiy sifatlarga ega shaxs xulq-atvorida esa yuqorida qayd etilgan holatlarning aksi namoyon bo'ladi. Ijobiy xulq-atvorga ega bo'lish insonga ko'rk bag'ishlaydi. Chunki, u tomonidan tashkil etilayotgan xatti-harakatlar, uning o'zini tutishi jamiyat tomonidan tan olingan axloq me'yorlariga zid bo'lmaydi, shu sababli o'zgalarning g'ashini keltirmaydi. Shunga ko'ra xulq-atvor suhbatdoshlarning dilini ravshan qilish, kayfiyatini xushnud etish, ko'ngilga taskin berish uchun xizmat qiladi.

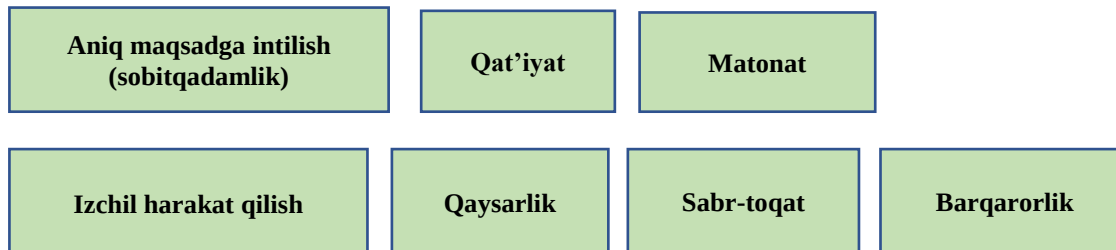
Axloqiy xulq-atvorni tarbiyalash axloqiy xatti-harakat va axloqiy odatlarni tarbiyalashni nazarda tutadi. Xatti-harakat yoki harakat kishining o'zini o'rab turgan voqealikka munosabatini tavsiflaydi. Axloqiy xatti-harakatni tashkil etish uchun tegishli sharoitni vujudga keltirish, tarbiyalanuvchilarning hayoti va faoliyatini aniq bir tartibda tashkil etish kerak³⁵. Zarur sharoitni yaratish ota-onalar, pedagoglar, tarbiyachilar hamda mas'ul shaxslardan pedagogik, psixologik bilimlarga ega bo'lishni, vaziyatni to'g'ri baholay olishni taqozo qiladi. Bolalar jamoasining ijtimoiy faoliyatini tashkil etish, bu jarayonda o'quvchilarning bir-birlariga ko'maklashishlarini ta'minlash, yordamga muhtoj kishilar, xususan, keksalarga xo'jalik yumushlarini bajarish, fanlardan o'zlashtira olmayotgan yoki bemor tengdoshlariga mavzularni tushuntirish, turistik sayohatlarda qiz bolalar, yoshi kichiklarning safar xaltalarini ko'tarish, ular uchun qulay dam olish joylarini ajratish va b. shu kabi xatti-harakatlarning yoshlar tomonidan tashkil etilishini ta'minlash ularda axloqiy xulq-atvorni shakllantirishga xizmat qiladi. "Biroq, xatti-harakatning o'zi axloqiy tarbiyalanganlik degan so'z emas, hali. Bunda xatti-harakatlarga qo'zg'otuvchi kuchlar, asoslar muhimdir" Axloqiy tarbiyani tashkil etishda o'quvchilarning xudbinlik sifatlarini o'zlashtirishlariga imkon bermaslik ham muhimdir. Aksincha, har qanday vaziyatda ham jamoa manfaati, tengdoshlarining umumiy yutuqlari muhim ekanligini ularning ongiga singdirib borish lozim. Axloqiy xatti-harakatlarning ijobiy mazmundagi qo'zg'atuvchi motiv (rag'bat)lar yordamida doimiy takrorlanishi ularning sekin-asta odatga aylanishini ta'minlaydi.

Shaxsda irodaviy harakatlarning namoyon bo'lishi, umumiy tarzda aytganda, quyidagi bosqichlarda kechadi:

- 1) maqsadni aniqlashtirish;
- 2) maqsadga erishish vositalarini belgilash;
- 3) motivatsiyalash (sabablarni asoslash);
- 4) motiv (rag'bat, sabab)lar kurashi;
- 5) qaror qabul qilish (unda qat'iyat va qat'iyatsizlik namoyon bo'ladi);
- 6) qarorni ijro etish;
- 7) ichki qarshiliklarni yengish;

- 8) tashqi qarshiliklarni yengish;
9) bajarilgan ishga baho berish.

Yuqorida aytib o'tilganidek, iroda ma'lum bir qarorga kelishda hamda bu qarorni ijro etishda namoyon bo'ladi. Inson hayotining barcha davrlarida go'daklikdagi ixtiyorsiz faollik shaxs taraqqiyotining keyingi bosqichlarida yuzaga keladigan irodaviy harakatlarga turlicha ta'sir qiladi. Bu ta'sir irodaviy harakatlarni yanada faollashtirishi ham, susaytirishi ham mumkin.



2-rasm. Iroda zaminida namoyon bo'ladigan sifatlar

Iroda go'daklik davrida ko'zga tashlanadigan ixtiyorsiz faollik negizida shakllanadi. Bu davrda go'dak tashqi ta'sirlarga ixtiyorsiz ravishda, o'ylab o'tirmagan holda qarshilik ko'rsatadi. Uning salbiy tashqi ta'sirlarga nisbatan harakatlari o'z-o'zidan paydo bo'ladi. Maktabgacha ta'lim yoshidan boshlab bolalarda ixtiyorsiz faollik asosida irodaviy faollik taraqqiy eta boshlaydi. Bu davrda u o'yinlar chog'ida albatta g'olib bo'lishga, tengdoshiga yordam berishga intiladi, garchi jismonan kuchi yetmasa-da, ayrim yumushlar (m: ukasini yoki og'ir sumkani ko'tarishni, yuqorida turgan buyumni olishni va h.k.)ni bajarishga intiladi. Bu kabi yumushlar uning imkoniyatlari darajasida bo'lmasa-da, biroq, bolaning bunday yondashuvini rag'batlantirish lozim. Zero, ana shunday intilishlarning uzluksiz, izchil sodir etilishi bolalarda irodaviy faollikni kuchaytiradi [8].

Xulosa qilib aytganda, har bir shaxsda iroda darajasi turlicha bo'ladi. Bir hayotiy faoliyatni tashkil etayotgan shaxslarda iroda yuqori darajada bo'lishi mumkin. Bu o'rinda Genri Fordning to'rt silindrli motorni yaratish jarayonidagi irodasini misol qilib keltirish mumkin. Genri Ford mutaxassislar bunday motorni yaratishning iloji yo'q deyishganda ham o'z qaroridan qaytmay, "Toki uni yaratmaguncha, ishni to'xtatmanglar! Qancha mablag', qancha vaqt sarflanishi meni qiziqitirmaydi" deb javob bergan. Aslida buyuk ixtirolarning kashf etilishi ana shunday jarayonda kechadi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

- [1] Ibragimov X.I., Abdullaeva Sh.A. Pedagogika nazariyasi / Darslik. - Toshkent: Fan va texnologiyalar, 2008. – 286 bet.
- [2] Ivanov P.I., Zufarova M.E. Umumiy psixologiya / Oliy ta'lim muassasalari uchun darslik. – Toshkent: "O'zbekiston faylasuflari milliy jamiyati" nashriyoti, 2008. – 308-332-betlar.
- [3] Mavlonova R., To'raeva O., Xoliqberdiyev K. Pedagogika / Kasb-hunar kollejlari ushun darslik. – Toshkent: "O'qituvchi" nashriyot-matbaa ijodiy uyi, 2010. – 495 bet.
- [4] Pedagogika / Bakalavriat yo'nalishi uchun darslik. Prof. M.X.Toxtaxodjayevaning umumiy tahriri ostida. – Toshkent: "O'zbekiston faylasuflari milliy jamiyati" nashriyoti, 2010. – 400 bet.
- [5] Pedagogika / O'quv qo'llanma. Sh.A.Abdullaeva, D.A.Axatova, B.B.Sobirov, S.S.Sayitov. – Toshkent: Fan, 2004. – 214 bet.
- [6] Tarbiya / Ota-onalar va murabbiylar uchun ensiklopediya. Tuzuvchi: M.N.Aminov. Mas'ul muharrir A.Majidov. – Toshkent: "O'zbekiston milliy ensiklopediyasi" Davlat ilmiy nashriyoti, 2010. – 528-bet.
- [7] Tursunov I., Nishonaliev U. Pedagogika kursi. – Toshkent: "O'qituvchi", 1997. – 188 bet.
- [8] G'oziyev E.G'. Psixologiya / Kasb-hunar kollejlari uchun darslik. – Toshkent: "O'qituvchi" nashriyot-matbaa ijodiy uyi, 2008. – 130-154-betlar.

CHET TILI O'QITUVCHILARINING METODIK TAYYORGARLIGINI TASHKIL
ETISHNING ZAMONAVIY TENDENTSIYALARI

U.A. ALIBAYEVA

Oliy ta'lim tizimi kadrlarini qayta tayyorlash va malakasini oshirish instituti

Annotatsiya. Maqolada chet tili o'qituvchilarini metodik tayyorgarligini tashkil etishdagi ba'zi zamonaviy tendentsiyalar tahlili keltirilgan. Zamonaviy jamiyatga xos bo'lgan ko'plab o'zgarishlar, shu jumladan, oliy pedagogik ta'lim tizimiga ta'sir ko'rsatdi. Chet tili o'qituvchilarining o'ziga xos parametrlarga ega bo'lgan, bir-biriga bog'liq va o'zaro bog'liq jihatlardan iborat bo'lgan kasbiy tayyorgarligi emas, ular orasidagi uslub muhim rol o'ynaydi. Zamonaviy tendentsiyalardan biri chet tili o'qituvchilarini uslubiy tayyorlashni tashkil etishga yondashuvlarni qayta ko'rib chiqishdir, ular orasida amaliyotga yo'naltirilgan, modulli va vaziyatni ajratib ko'rsatish maqsadga muvofiqdir. Maqolada har bir yondashuvning ishlash mexanizmlari va ularning chet tili o'qituvchilarini metodik tayyorlash kontekstidagi o'rni ko'rsatilgan.

Kalit so'zlar. chet tili o'qituvchilarini metodik tayyorgarligi; amaliyotga yo'naltirilgan yondashuv; modulli yondashuv; situatsion yondashuv; sinfdan tashqari ishlar

Chet tili o'qituvchilarining kasbiy tayyorgarligi nuqtai nazaridan uning uslubiy jihati asosiy o'rinlardan birini egallaydi. Ushbu qoida, birinchi navbatda, belgilangan fan sohasining zamonaviy o'qituvchisi nafaqat kommunikativ va psixologik-pedagogik kompetentsiyaning etarli darajasiga ega bo'lishi, balki zamonaviy ta'lim haqiqatining barcha xususiyatlari va tendentsiyalarini hisobga olgan holda har xil turdagi ta'lim muassasalarida chet tilini o'qitish jarayonini optimal tarzda tashkil eta olishi bilan belgilanadi. Hozirgi vaqtda chet tili o'qituvchilarining uslubiy tayyorgarligi o'rnatilgan va ijobiy tasdiqlangan an'analarning mavjudligi bilan ham, ba'zi bir dolzarb lingvometodik yo'nalishlarni shakllantiradigan rivojlanayotgan innovatsion jarayonlar bilan ham tavsiflanadi.

Ushbu maqola doirasida chet tili o'qituvchilarini metodik tayyorlashning innovatsion yo'nalishlarini umumlashtirilgan tahlil qilishga to'xtalamiz, ularning namoyon bo'lishi va faoliyatining xususiyatlari va qonuniyatlarini ko'rib chiqamiz, samaradorlik sabablarini belgilaymiz. Bo'lajak chet tili o'qituvchilarini metodik tayyorlashni tashkil etishning turli tarkibiy qismlari A. V. Dubakov, O. N. igna, S. N. Makeyeva, E. S. Nadtocheva, I. V. Rahmanova, E. N. Solovova, O. L. Felde, T. V. Xilchenko va boshqalarning tadqiqotlarida aks ettirilgan. [1, 3-7, 9, 10].

Ushbu maqolada o'qituvchilarni zamonaviy linguometodik tayyorlashning umumlashtirilgan xususiyatlari va uning o'ziga xos jihatlari keltirilgan. Shuni ham ta'kidlash kerakki, yaqin vaqtgacha chet tili o'qituvchilarini uslubiy tayyorlashni tashkil etish to'g'ridan-to'g'ri chet tilini o'qitish metodikasi intizomi doirasida amalga oshirildi. I.V. Rahmonov bir necha o'n yilliklar davomida shakllangan lingvometodik an'analarni belgilab, oliy o'quv yurtlari va til fakultetlarida fanni o'qitishning o'ziga xos xususiyatlarini tahlil qilib, fanni o'qitishni tashkil etishda tuzatishni talab qiladigan turli kamchiliklar mavjudligini ta'kidladi. Metodika boyicha ma'ruzalar kurslari ma'lum bir mavhumlik bilan ajralib turishi mumkin edi, seminar va amaliy mashg'ulotlar esa mazmunining etarli emasligi sababli talabalarning qiziqishini uyg'otmadi.

Qoida tariqasida, fanni o'rganishning asosiy maqsadlari tilning turli jihatlarini qanday o'qitish haqida g'oyalarni shakllantirish bilan bog'liq edi, ammo ma'lum bir sinfda ta'limni qanday qilib aniq qurish kerakligini va nima uchun buni shu tarzda amalga oshirish kerakligini aniq anglashga yo'naltirilmagan. Seminar mashg'ulotlarini qurish ham bir-biriga zid edi. Ushbu darslar to'g'ridan-to'g'ri nazariy bo'lishi kerakmi yoki muayyan mavzularni ishlab chiqishning amaliy yo'naltirilgan

illyustratsiyasiga xizmat qilishi kerakmi yoki nazariy va amaliy organik to'plamga ega bo'lishi kerakmi degan savolga yagona javoblar olinmadi [6]. Bugungi kunda chet tili o'qituvchilarini metodik tayyorlashni tashkil etish turli yo'nalishlarda o'zgardi. O'zgarishlarning asosiy sababi zamonaviy inson hayotida chet tilining rolining o'zgarishi.

Ta'limning haqiqiyliigi va kommunikativ yo'nalishi printsiplarining ustunligi, chet tilini o'qitishning amaliyotga yo'naltirilgan xorijiy metodologiyasi g'oyalarining intensiv integratsiyasi tufayli mahalliy uslubiy tayyorgarlikni tashkil etish yondashuvlari ko'p jihatdan o'zgardi. Innovatsion yondashuvlarning mantig'i va muhim xususiyatlari chet tili o'qituvchilarini metodik tayyorlashda sinf ishlarini tashkil etishda yangi xususiyatlarning paydo bo'lishini belgilaydi. Bundan tashqari, chet tili o'qituvchilarini zamonaviy metodik tayyorlashning o'ziga xos xususiyatlaridan biri bu darsdan tashqari ishlarni tashkil etishda namoyon bo'ladigan qo'shimchalik tamoyilini amalga oshirishdir.

O. L. Felde o'qituvchining uslubiy tayyorgarligini takomillashtirish uchun eng muhim yondashuvlar ekanligini ta'kidlaydi, chunki ular talabalarning mazmuni, o'qitish yo'nalishlari, talabalar bilan ishlash turlari va ish turlarini belgilaydi. Yondashuvlar asosida zarur o'quv ta'minotining mazmuni va tarkibiy tarkibi qurilgan. Chet tili o'qituvchilarini metodik tayyorlashni tashkil etishning zamonaviy yondashuvlariga kompetentsion, aks ettiruvchi, integrativ yondashuvlarni kiritadi. Ushbu yondashuvlarning har birini amalga oshirish ma'lum xususiyatlar va imkoniyatlarga ega [9]. Taqdim etilgan nuqtai nazarni baham ko'rish orqali biz ushbu yondashuvlarga zamonaviy ta'lim sharoitida tobora kuchayib borayotgan mavqeini hisobga olgan holda amaliyotga yo'naltirilgan, modulli va vaziyatni qo'shish maqsadga muvofiq deb hisoblaymiz.

Chet tili o'qituvchilarini metodik tayyorlashni tashkil etishda amaliyotga yo'naltirilgan yondashuvning ahamiyati bugungi kunda metodik tayyorgarlikni tashkil etish jarayonida jarayonning amaliy tarkibiy qismi to'g'ridan-to'g'ri birinchi o'ringa chiqishi bilan bog'liq. Kelajakdagi chet tili o'qituvchilari nafaqat kerakli miqdordagi uslubiy bilimlarga ega bo'lishlari, balki ularni haqiqiy kasbiy faoliyatda oqilona qo'llashlari, buni qanday qilish kerakligini bilishlari va shakllangan uslubiy ko'nikmalarga ega bo'lishlari kerak. Ushbu qoidaga asoslanib, chet tili o'qituvchilarining zamonaviy uslubiy tayyorgarligi amaliyotga yo'naltirilgan bo'lishi kerak degan xulosaga kelishimiz mumkin. Chet tili o'qituvchilarini metodik tayyorlashni tashkil etishning mavjud xususiyatlari va ko'rsatmalarini qayta ko'rib chiqish tabiiydir.

Chet tili o'qituvchilarini metodik tayyorlashni tashkil etishga amaliyotga yo'naltirilgan yondashuvni amalga oshirish modulli yondashuv bilan o'zaro bog'liqdir. Bu, boshqa narsalar qatori, amaliyotga yo'naltirilgan yondashuvni amalga oshirish samaradorligini modullikni ta'minlash, ya'ni umumta'lim maktabida chet tilini o'qitish bosqichlarini aks ettiruvchi bloklarga tarkibiy va mantiqiy reytingni oshirish orqali oshirish mumkinligi bilan izohlanadi. Modulli amaliyotga yo'naltirilgan tayyorgarlikni tashkil etish kelajakdagi o'qituvchilarning e'tiborini chet tilini o'qitishning ma'lum bir bosqichiga qaratishga, har bir bosqichning o'ziga xos xususiyatlarini tahlil qilish va anglashga, tilshunoslik ko'nikmalarining yaxlit tizimini shakllantirishga yordam beradi.

Tayyorgarlikning har bir bosqichining finalida chet tili o'qituvchilari lingvometodik portfelni namoyish etishlari mumkin. Ushbu turdagi portfel nazariy tayyorgarlik jarayonida ham, pedagogik amaliyotni o'tashda ham kasbiy o'zini o'zi baholash va ularning faoliyatini aks ettirish vositasidir. Portfelga bo'lajak o'qituvchini ilmiy-uslubiy izlash natijalari (tahliliy ma'ruzalar, loyihalar, uslubiy insholar va boshqalar), original uslubiy ishlanmalar, darslarning parchalari, amaliy o'qituvchilarning saboqlarini tahlil qilish, o'z darslarini tahlil qilish, yakuniy malaka ishi doirasida olib borilayotgan ilmiy tadqiqotlar bo'yicha eksperimental ish natijalari va boshqalar kiradi.

Chet tili o'qituvchilarini metodik tayyorlash doirasida amaliyotga yo'naltirilgan va modulli yondashuvlarni amalga oshirish zamonaviy ta'lim tizimi sharoitida o'z vaqtida amalga oshiriladi. Amaliyotga yo'naltirilgan yondashuv kelajakdagi chet tili o'qituvchilarining uslubiy tayyorgarligini ularning keyingi kasbiy faoliyatiga yaqinlashtirishni o'z ichiga oladi va bir qator muhim uslubiy ko'nikmalarni shakllantirishga yordam beradi. Modulli yondashuvning xususiyatlarini hisobga olish

kelajakdagi o'qituvchilarda chet tilini o'qitishning har bir yosh bosqichi to'g'risida zarur uslubiy bilimlarni shakllantirishga, ularning xususiyatlarini ko'proq "yashashga" yordam beradi. Amaliyotga yo'naltirilgan va modulli yondashuvlarni amalga oshirish metodik fikrlashni shakllantirishga, metodik ko'nikmalarni kompleks rivojlantirishga va chet tili o'qituvchilarining kasbiy moslashuvchanligiga yordam beradi.

Vaziyatli yondashuv ekzistensializmning doimiy ravishda o'zgarib turadigan tanlov sharoitida odamning mavjudligi haqidagi pozitsiyalariga asoslanadi va shu sababli odam doimiy qarorlar qabul qilishga majbur bo'ladi. Falsafiy asosdan tashqari, pedagogik asosni ham ajratib ko'rsatish kerak, unga ko'ra vaziyat pedagogik muammo, o'quv jarayonining boshlang'ich nuqtasi, vositasi va maqsadi sifatida ko'rib chiqiladi. Vaziyatli yondashuv haqiqiy hayotiy vaziyatlarga asoslangan holda o'qitish va tarbiyalashni o'z ichiga oladi. Bu ta'lim va hayot o'rtasidagi yaqin aloqani ta'minlaydi, vaziyatlarni tahlil qilish asosida o'quv jarayonining mazmunini rejalashtiradi [8]. Chet tili o'qituvchilarini kasbiy tayyorlash jarayonida situatsion yondashuvni amalga oshirish umumiy pedagogik va lingvistik metodik darajalarda amalga oshiriladi.

Chet tili o'qituvchisi doimo oqilona tahlil va echimni talab qiladigan har qanday pedagogik va uslubiy vaziyatlarga duch keladi. Vaziyatli yondashuvni amalga oshirish variantlari ma'ruza va seminar mashg'ulotlarida turli xil uslubiy vaziyatlarni to'g'ridan-to'g'ri tahlil qilish, shuningdek uslubiy vaziyatlarni modellashtirishdir.

Amaliyot shuni ko'rsatadiki, bugungi kunda uslubiy vaziyatli muammolarni hal qilish va uslubiy vaziyatlarni tahlil qilish bo'yicha mavjud seminarlar ancha eskirgan va chet tilini o'qitish jarayonining zamonaviy xususiyatlari va tendentsiyalarini aks ettirmaydi. Bu erda zamonaviy ustaxonalarga alternativa sifatida ishlaydigan dars parchalari ko'rinishidagi video vaziyatlardan foydalanish tavsiya etiladi. Uslubiy video vaziyatlarning kamchiliklari ularning ma'lum bir cheklanganligi, dars davomida yuzaga kelishi mumkin bo'lgan aksariyat fikrlarni qamrab olishning mumkin emasligi. Bundan tashqari, video to'plamlarda motivatsion funktsiyani bajaradigan eng yaxshi darslar mavjud.

Zamonaviy ta'limning salbiy tendentsiyalaridan biri bu o'quv soatlarini sezilarli darajada qisqartirishdir. Shu sababli, qo'shimcha ish printsipini amalga oshirishga asoslangan sinfdan tashqari ishlar alohida rol o'ynaydi. Sinfdan tashqari ishlar sinf soatlarining pasayishi bilan bog'liq bo'shliqlarni to'ldirish, bo'lajak o'qituvchilarning kasbiy dunyoqarashini kengaytirish, ularning umumiy kasbiy va predmetli kompetentsiyalari darajasini oshirish imkonini beradi. Istisno, shuningdek, auditoriyadan tashqari tarkibiy qismi samarali imkoniyatlarga ega bo'lgan kelajakdagi chet tili o'qituvchilarining uslubiy tayyorgarligi emas.

Bugungi kunda chet tili o'qituvchilarini metodik tayyorgarligi kontekstida darsdan tashqari ishlarning quyidagi shakllarini belgilash maqsadga muvofiqdir:

1. axborot-hisobot rejasi tadbirlari (uslubiy mahorat darslari va ustaxonalar, ma'ruzalar va video ma'ruzalar, onlayn vebinarlar, muammoli seminarlar va boshqalar);
2. raqobatbardosh tadbirlar (chet tilini o'qitish metodikasi bo'yicha Olimpiada yoki Olimpiada sinovlari, yuqori kurs talabalari uchun uslubiy mahoratni rivojlantirish bo'yicha tanlovlar, eng yaxshi ilmiy yoki uslubiy ishlar uchun tanlov va boshqalar);
3. ilmiy-tadqiqot ishlari;
4. chet tilini o'qitish metodikasi bo'yicha muammoli guruhlar;
5. o'quv ekskursiyalarini tashkil etish va o'tkazish;
6. pedagogik amaliyot [2].

Sinfdan tashqari ishlarning barcha belgilangan shakllari o'zaro bog'liq va o'zaro bog'liqdir. Qo'shimcha printsipning o'ziga xos xususiyatlarini hisobga olgan holda shuni ta'kidlash kerakki, chet tilini o'qitish metodikasi fanidagi dastur faqat chet tilini o'qitishni tashkil etishning asosiy masalalarini qisqacha ochib berish bilan cheklangan. Ba'zida alohida ko'rib chiqishni talab qiladigan ko'plab muhim va innovatsion masalalar e'tiborga olinmaydi. Ushbu pozitsiyalardan ta'lim jarayoniga axborot-kommunikatsiya yo'nalishidagi qo'shimcha tadbirlarni ishlab chiqish va

joriy etish zarur. Yuqorida ta'kidlab o'tilganidek, bunday tadbirlarga uslubiy ustaxonalar va mahorat darslari, ma'ruzalar va video ma'ruzalar, onlayn vebinarlar, muammoli seminarlar va boshqalar kiradi [10].

Shadrin davlat pedagogika universitetining nemis tillari nazariyasi va amaliyoti (ingliz tili va uni o'qitish metodikasi) kafedrasida ham talabalar auditoriyasi, ham amaliyotchi o'qituvchilar uchun lingvometodik seminarlar va mahorat darslari o'tkazish bo'yicha foydali tajriba to'plangan. Qoida tariqasida, innovatsion tushunchalar va texnologiyalar batafsil ko'rib chiqiladi, ba'zida qarama-qarshiliklarga ega, ammo kelajakdagi o'qituvchilar uchun qiziqish uyg'otadi. Mahorat darslari doirasida texnologiyalarning xususiyatlari, ularni amalga oshirish algoritmlari ochib beriladi. Bu erda talabalar bahslari, davra suhbatlari va tematik munozaralar tashkil etiladi. Masalan, darsdan tashqari lingvometodik ishlarni tashkil etish yillarida quyidagi mavzularda seminarlar va mahorat darslari o'tkaziladi:

Chet tilini o'qitishda veb-qidiruv texnologiyasi, chet tilini o'qitishda Interaktiv texnologiyalar, chet tili darsida tanqidiy fikrlashni qanday shakllantirish kerak, Chet tilini o'qitishda texnologiyasini amalga oshirish va boshqalar, master-klass shakli chet tili o'qituvchilarining uslubiy tafakkurini shakllantirishga qaratilgan, ayniqsa uni muammoli qurishda.

Sinfdan tashqari linguometodik ish raqobatbardosh tadbirlarni tashkil etishga yo'naltirilishi mumkin. Chet tilini o'qitish metodikasi bo'yicha fakultet ichidagi tadbirlar umumiy madaniy va kasbiy kompetentsiyalarni shakllantirish darajasini aniqlash, chet tili o'qituvchilarining kasbiy moslashuvchanligini shakllantirish, o'qituvchilik kasbining obro'sini oshirish maqsadida o'tkaziladi. Sinfdan tashqari raqobatbardosh shaklning bir misoli sifatida turli bosqichlardan iborat chet tilini o'qitish metodikasi bo'yicha fakultet ichidagi Olimpiada bo'lishi mumkin. Lingvometodik Olimpiadani o'tkazish quyidagilarga qaratilgan

1. bo'lajak chet tili o'qituvchilarining kasbiy vakolatlarini rivojlantirish va ularning kasbiy o'zini o'zi anglashi uchun sharoit yaratish;
2. talabalarning fanlarni o'rganish uchun ijobiy motivatsiyasini rivojlantirish pedagogik tsikl va pedagogik amaliyotga;
3. bo'lajak o'qituvchilarning kasbiy o'zini o'zi anglashini shakllantirish; iqtidorli fakultet talabalarini aniqlash va rag'batlantirish [2].

Fakultet ichidagi uslubiy Olimpiada davomida iqtidorli talabalarni aniqlash, ularni professional qo'llab-quvvatlashni tashkil etish mumkin. Raqobatbardosh tadbirlar motivatsion funktsiyani bajaradi va talabalarni kasbiy rivojlanish bilan shug'ullanishga, oldinga siljishga, yangi narsalarni o'rganishga undaydi. Mualliflar tomonidan tashkil etilgan va o'tkazilgan tanlov xarakteridagi quyidagi tadbirlar samarali ekanligi isbotlandi: chet tilini o'qitish metodikasi bo'yicha madaniyatlararo olimpiadalar, mening uslubiy kredoim uslubiy mahorat tanlovi, amaliyotchilarning eng yaxshi talabalarini aniqlash bo'yicha tanlovlar va boshqalar, hozirgi vaqtda talabalar va amaliyotchi chet tili o'qituvchilari uchun xalqaro kompleks tanlovni tashkil etish bo'yicha ishlar olib borilmoqda. Auditoriyadan tashqari lingvometodik ishlarning keyingi yo'nalishi ilmiy-tadqiqot ishlari hisoblanadi. Bu sizga shaxsiy masalalarni o'rganish va tahlil qilish, ularni tanqidiy tushunish, belgilangan muammolarni hal qilishda ijodiy yondashish imkonini beradi. Tadqiqot natijalari ilmiy-amaliy konferentsiyalar doirasida taqdim etilgan kurs va tezislarda aks etadi

Chet tilini o'qitish metodikasi bo'yicha ilmiy-tadqiqot ishlarini tashkil etish shakllaridan biri muammoli guruhdir. Chet tilini o'qitish metodikasi bo'yicha ilmiy hamjamiyat yanada murakkab shakl sifatida ko'rib chiqilishi mumkin. Pedagogik amaliyot chet tili o'qituvchilari olgan bilimlarini qo'llashlari, kasbning turli xususiyatlarini ko'rishlari mumkin bo'lgan platformadir. Pedagogik amaliyot ko'p jihatdan o'qituvchining shakllanishiga, uning lingvometodik tafakkurining rivojlanishiga ta'sir qiladi. Amaliyot davomida ko'plab talabalar tanlangan professional yo'lning to'g'riligi yoki noto'g'riligini bilishadi. Dastlabki professional tajribalarning ba'zilar noto'g'ri. Chet tili o'qituvchilarining amaliyoti muvaffaqiyatli bo'lishi uchun ularning faoliyatini

muvoqilash, pedagogik qo'llab-quvvatlash va kasbiy qo'llab-quvvatlashni amalga oshirish zarur.

Umumiy xulosa sifatida chet tili o'qituvchilarini uslubiy tayyorlashni tashkil etishda bugungi kunda uning o'zgarishi va keyingi rivojlanishining mohiyatini belgilaydigan bir qator zamonaviy tendentsiyalar kuzatilmoqda. Ushbu tendentsiyalar amaliyotga yo'naltirilgan, modulli va vaziyatli yondashuvning jadal rivojlanishini o'z ichiga oladi. Bundan tashqari, zamonaviy uslubiy tayyorgarlikning eng muhim tarkibiy qismi uning sinfdan tashqari ishidir. Belgilangan barcha tarkibiy qismlar chet tili o'qituvchilarining uslubiy tayyorgarligini modernizatsiya qilish va takomillashtirishga qaratilgan.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

[1] Dubakov, A. V. oliy ta'limni modernizatsiya qilish sharoitida chet tili o'qituvchilarining uslubiy raqobatbardoshligini shakllantirish [matn] / A. V. Dubakov, T. V. Xilchenko // gumanitar va tabiiy fanlarning dolzarb muammolari. – №10 (69). – 2014. 336-344-betlar.

[2] Dubakov, A. V. chet tili o'qituvchilarini kasbiy uslubiy tayyorlash tizimida darsdan tashqari ishlarining imkoniyatlari [matn] / A. V. Dubakov, T. V. Xilchenko // Shadrin davlat pedagogika universitetining Axborotnomasi. – 2015. – №4(28). 131-135 betlar.

[3] Igna, O. N. chet tili o'qituvchisining uslubiy kompetentsiyasining tuzilishi va mazmuni [matn] // Yaroslavl pedagogik byulleteni. – 2010 – №1. 90-94 betlar.

[4] Makeyeva, S. N. chet tili o'qituvchisini metodik tayyorlashga kompetentsiyaga asoslangan yondashuv [matn] / S. N. Makeyeva // buryat gazetasi. davlat un-ta: o'qitish nazariyasi va metodikasi. – 2010. – №15. 201-205 betlar.

[5] Nadotcheva, E. S. chet tili o'qituvchilarini kasbiy va uslubiy tayyorlash jarayonini tashkil etish uchun asos sifatida refleksiv-faoliyat yondashuvi [matn] / E. S. Nadotcheva // Rossiyada pedagogik ta'lim. – 2012. – № 1. 111115-sahifa.

[6] Rahmonov, I. V. pedagogika institutlari va chet tillar fakultetlarida metodikani o'qitish to'g'risida [matn] / I. V. Rahmonov // maktabda chet tillari. – № 4. – 2010. 123-sahifa.

[7] Solovova, E. N. chet tili o'qituvchisini metodik tayyorlash va qayta tayyorlash: integrativ-reflektiv yondashuv: monogr. [Matn] / E.N. Solovov tomonidan. M.: Glossa-Press, 2004 yil. 336 b.

[8] Solovyov, G. E. o'qituvchilarini tarbiyalashda voqealarga asoslangan yondashuv [matn] / G. E. Solovyev // Udmurtiya universiteti gazetasi. Falsafa Seriyasi. Psixologiya. Pedagogika. – 2009. – №2. 103111-sahifa.

[9] Felde O. L. chet tili o'qituvchisini metodik tayyorlashni takomillashtirishning zamonaviy asoslari // ijtimoiy rivojlanish nazariyasi va amaliyoti. – 2012 – №11. 165-167-betlar.

[10] Xilchenko, T. V. chet tili o'qituvchilarini kasbiy uslubiy tayyorlash tizimida darsdan tashqari ishlar [matn] / T. V. Xilchenko, A. V. Dubakov // bugungi kunda til ta'limi – rivojlanish vektorlari: VI xalqaro ilmiy-amaliy konferentsiya-forum materiallari. Yekaterinburg, 2015 yil 14-18 aprel / FGBOU VPO Ural. davlat ped. un-t. Yekaterinburg, 2015 yil. 158-166 betlar.

**ZAMONAVIY OQIMLI SHIFRLASH ALGORITMLARINING
TAQQOSLAMA TAHLILI**

f-m. f. d., professor G.U. JURAYEV, Sh.S. ANVAROV
Mirzo Ulug'bek nomidagi O'zbekiston Milliy Universiteti

Annotatsiya. Ushbu maqolada zamonaviy oqimli shifrlash algoritmlarining arxitekturasini, xavfsizlik darajasi va amaliy jihatlari bo'yicha chuqur tahlil keltirilgan. RC4, A5/1 va E0 kabi an'anaviy algoritmlar xavfsizlik muammolari sababli yangi tizimlarda qo'llanilmayotgani asoslab berilgan. eSTREAM loyihasida tavsiya etilgan Salsa20, Trivium, Rabbit, Grain, SOSEMANUK va MICKEY 2.0 kabi algoritmlar qiyosiy tahlil qilingan. Ularning dasturiy va apparat ko'rinishdagi bajarilishi, quvvat sarfi, mantiqiy elementlar talabi va tezlik bo'yicha natijalari jadval asosida ko'rsatilgan. Oqimli shifrlar ustida olib borilgan hujumlar, xususan differensial, chiziqli, algebraik va korrelyatsion kriptotahlil usullari alohida yoritilgan. LWC (Lightweight Cryptography) muhitida qo'llashga mo'ljallangan Enocoro, WG-7/8 va ACORN kabi ixcham va samarali algoritmlar baholangan. Bundan tashqari, autentifikatsiyani ta'minlaydigan oqimli shifrlar (Hummingbird-2, Rabbit-MAC) tahlil qilinib, ularning xavfsizlik xususiyatlari ochib berilgan. Maqolada FPGA va ASIC muhitlarida bajarilgan amaliy testlar asosida algoritmlarning texnik ko'rsatkichlari solishtirilgan. Tadqiqot natijalari oqimli shifrlarning ilovaga mos tanlanishi va ularning amaliy xavfsizligi o'rtasidagi muvozanatni ta'minlash muhimligini ko'rsatmoqda.

Kalit so'zlar: oqimli shifr, kriptotahlil, RC4, A5/1, E0, eSTREAM, Salsa20, Trivium, Rabbit, Grain, MICKEY 2.0, Enocoro, SOSEMANUK, Hummingbird-2, autentifikatsiya, FPGA, ASIC, LWC, apparat amalga oshirish, xavfsizlik tahlili, psevdotasodifiylik, IV, ARX struktura, chiziqli registyor, tezkorlik, energiya samaradorligi.

Аннотация. В статье проведён всесторонний сравнительный анализ современных потоковых шифров с учётом их архитектурных особенностей, безопасности и применимости. Приведены причины, по которым устаревшие алгоритмы, такие как RC4, A5/1 и E0, более не используются в современных системах. Основное внимание уделено участникам проекта eSTREAM — Salsa20, Trivium, Rabbit, Grain, SOSEMANUK и MICKEY 2.0. Для каждого из алгоритмов рассмотрены параметры реализации на программном и аппаратном уровнях, такие как потребляемая мощность, количество логических элементов и пропускная способность. Раскрыты особенности атак на потоковые шифры: дифференциальный, линейный, алгебраический и корреляционный криптоанализ. Особое внимание уделено лёгким криптографическим решениям (LWC), включая алгоритмы Enocoro, WG-7/8 и ACORN. Также проанализированы аутентифицирующие потоковые шифры (например, Hummingbird-2, Rabbit-MAC) и их надёжность. Приведены результаты тестирования на FPGA и ASIC платформах.

Ключевые слова: потоковый шифр, криптоанализ, RC4, A5/1, E0, eSTREAM, Salsa20, Trivium, Rabbit, Grain, MICKEY 2.0, Enocoro, SOSEMANUK, Hummingbird-2, аутентификация, FPGA, ASIC, LWC, аппаратная реализация, стойкость, псевдослучайность, IV, структура ARX, сдвиговый регистр, производительность, энергоэффективность.

Abstract. This article presents a comprehensive comparative analysis of modern stream cipher algorithms with a focus on architecture, security, and implementation efficiency. Legacy ciphers such as RC4, A5/1, and E0 are discussed in terms of their vulnerabilities, making them unsuitable for modern applications. The study focuses on eSTREAM project finalists including Salsa20, Trivium, Rabbit, Grain, SOSEMANUK, and MICKEY 2.0. These ciphers are evaluated based on hardware and software performance, including power consumption, gate count, and throughput. Various cryptanalytic techniques — differential, linear, algebraic, and correlation attacks — are discussed in depth. Lightweight cryptographic (LWC) solutions like Enocoro, WG-

7/8, and ACORN are reviewed for constrained environments. Authenticated stream ciphers such as Hummingbird-2 and Rabbit-MAC are also examined for integrity protection. FPGA and ASIC-based performance tests are reported with comparative metrics. The findings highlight the importance of balancing theoretical security and practical efficiency. The study concludes that cipher selection should be context-driven, factoring in application type and platform limitations.

Keywords: stream cipher, cryptanalysis, RC4, A5/1, E0, eSTREAM, Salsa20, Trivium, Rabbit, Grain, MICKEY 2.0, Enocoro, SOSEMANUK, Hummingbird-2, authentication, FPGA, ASIC, LWC, hardware implementation, security evaluation, pseudorandomness, initialization vector, ARX structure, shift register, performance, energy efficiency.

Ana'naviy oqimli shifrlar va ularga aloqador xavfsizlik muammolari ko'plab adabiyotlarga keltirilgan [1,47]. Ularga misol qilib Rivest Cipher 4 (RC4), A5/1 va E0 algoritmlarini keltirish mumkin. Ushbu algoritmlarda xavfsizlik muammolari aniqlangani bois, undan yangi ilovalarda yoki tizimlarda foydalanilmaydi.

RC4 algoritmi. Rivest Cipher 4 yoki RC4 oqimli shifrlash algoritmi dasturiy vosita ko'rinishida amalga oshirishga qulay bo'lgan eng mashhur algoritmlardan biri bo'lib, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) va Secure Socket Layer (SSL) kabi protokollarda keng qo'llaniladi. Ushbu shifrlash algoritmi sodda tuzilishga egaligi bois, katta tezkorlik qayd etadi. U LFSR yondashuviga asoslangan bo'lib, undan farqli ravishda bit emas, balki, bayt ko'rinishda chiqish

qiymatini taqdim etadi. RC4 shifrlash algoritmi ham dasturiy ham apparat ko'rinishlarda amalga oshirish uchun qulay hisoblanadi. Biroq, ishlab chiqilganiga ancha muddat bo'lgani va kalitni almashtirishda muammolar mavjudligi sababli, xavfsiz emas deb qaraladi. Xususan, protokollarda nonce va kalitning alohida- alohida yuborilmasligi va ular asosida kalit ketma-ketligini yaratish jarayoni. Bu holda bo'lishi mumkin bo'lgan yechimlardan biri - kalit va nonce kattaliklarini bardoshli MAC algoritmlari asosida xeshlash hisoblandsada, mazkur holda turli kalit ketma-ketligi taqdim etish holati kuzatilgan [3]. Hosil bo'lgan kalit ketma- ketliklari asosiy kalitga bog'liq bo'lgani bois [4], WEP protokolini buzishga asos bo'lgan. RC4 algoritmini tahlil qilish bo'yicha olib borilgan eng samarali usul yordamida 224 ta ulanish bilan shifrlash kalitini topish mumkin bo'lgan [5]. Shifrn o'ziga bevosita qaratilgan amaliy hujumlar mavjud emas.

A5/1 algoritmi. A5/1 oqimli shifrlash usuli GSM (Global System for Mobile) standartining 2G texnologiyasi uchun havo muhitida aloqa konfidensialligini ta'minlash maqsadida ishlab chiqilgan. U o'zida uchta LFSRni birlashtirgan bo'lib, undagi *maj()* funksiyasi asosida registrlarning siljishi yoki siljimasligi aniqlanadi. Hozirgi kunda ham foydalanilayotgan bo'lishiga qaramay, A5/1 oqimli shifrlash algoritmi bevosita hamda GSM tarmog'ida qo'llanilgan holati uchun ham xavfsiz emas deb topilgan. Aksariyat kriptotahlil usullari katta hisoblash imkoniyatini talab qilib, shifrn qisqa vaqtda buzish imkonini bergan bo'lsa, 2003-yilda faqat shiftmatnga asoslangan dastlabki kriptotahlil amalga oshirilgan [6, 7]. 2007-yilda parallel ulangan FPGA (Field-programmable gate array)lar massivi asosida yaratilgan COPACOBANA loyihasi ishlab chiqilib, uning tijoriy shakllari ham keng tarqalgan [8, 9]. Ushbu vosita yordamida shifrn real vaqtda deshifrlash mumkin.

E0 algoritmi. E0 oqimli shifrlash algoritmi Bluetooth simsiz tarmoq standartida foydalanilgan bo'lib, u 4 ta siljitish registridan iborat [14]. Ushbu shifrlash algoritmi va standartda qo'llanilishi ham amaliy hujumga uchragan. Ushbu shifrlash algoritmda 128-bitli kalitdan foydalanilgan. Yetarlicha katta uzunlikdagi kalit foydalanilgan bo'lsada, hujum natijasida uning uzunligi 65

bitgacha tushurilgani aniqlangan [10, 11]. Bluetooth standartini statistik va ma'lum ochiq matnlar asosida hujum qilish natijasida kalit uzunligini 38 bitga tushurishga erishilgan [12, 13].

Bundan tashqari, simmetrik blokli shifrlardan foydalanib oqimli shifrlash algoritmlarini qurish mumkin. Masalan, NIST tomonidan simmetrik blokli shifrlarning CFB, OFB, CTR rejimlari yordamida oqimli shifrlarni yaratish mumkin [15].

Ularni hosil qilish uchun ko'rsatilgan rejimda faqat shifrlash amalga oshiriladi va rasshifrovkalash uchun ham aynan ushbu jarayoning o'zidan foydalaniladi. Loyihalashning mazkur turiga qaratilgan hujumlar va uning xavfsizlik tahlili [3] manbada amalga oshirilgan. Oqimli shifrlarni hosil qilishda eng ko'p foydalanilgan blokli shifrlash algoritmi bu AES standarti hisoblanadi. Xususan, sanoq rejimidagi AES-CTR algoritmi oqimli shifrlash algoritmi sifatida amalda keng qo'llaniladi [1]. AES-CTR algoritmida hosil qilingan oqimli shifrlash usuli 7-ildavda keltirilgan. Ushbu algoritmdan LWC (Lightweight cryptography) tizimlari uchun ham qo'llash bo'yicha ilmiy izlanishlar olib borilmoqda. Biroq, aksariyat holatlarda ularni cheklangan qurilmalar uchun mos emasligi aniqlangan.

Quyida esa eSTREAM loyihasi doirasida ishlab chiqilgan ko'plab oqimli shifrlash algoritmlarining tahlili bilan tanishib chiqiladi. eSTREAM bu – oqimli shifrlash algoritmlarining majmuasi bo'lib, European Network of Excellence for Cryptology II loyihasining bir qismi hisoblanadi [16]. Ushbu loyihada ikki turdagi: dasturiy vositalar va qurilmalar uchun mos bo'lgan oqimli shifrlash algoritmlari keltirilgan. Birinchi guruh algoritmlari dasturiy ko'rinishda qulay bo'lgan algoritmlardan iborat bo'lib, 128-bitli AES-CTR algoritmdan tezkor bo'lgan algoritmlardan tashkil topgan. Ushbu guruhga tegishli finalchi shifrlar: Salsa20/12 [17], Rabbit, HC-128 [18] va SOSEMANUK algoritmlaridan iborat. Ikkinchi guruhga tegishli shifrlar qurilma uchun mos bo'lgan algoritmlardan iborat bo'lib, 80-bitli AES algoritmdanda ko'ra qurilmada amalga oshirish qulay bo'lishi talab etilgan. Bu guruhda esa finalchi algoritmlar: Grain [2], Trivium [19] va MICKEY 2.0 [20] iborat bo'lgan. Ushbu loyihada ko'plab algoritmlar ishtirok etgan bo'lib, ularning ayrimlaridagi xavfsizlik muammolari sabab, konkursni tark etgan bo'lsa, ayrimlari uchun qurilma ko'rinishda amalga oshirishdagi qiyinchiliklar ishtirok etolmaslikka sabab bo'lgan. Ushbu konkursa qatnashgan 34 ta shifrlash algoritmdan faqat ikkitasi o'zi sinxronlanuvchi shifrlarga tegishli bo'lib, ularning har ikkalasi ham xavfsiz emas deb topilgan. Finalchi algoritmlar ham kalitni to'liq tanlash hujumiga qaraganda samarali bo'lgan usullar yordamida tahlil qilingan. Biroq, yangi kriptotahlil usullari finalchilar orasidan ayrimlari uchun jiddiy xavfsizlik muammolarini ko'rsatdi.

LWC muhiti uchun mos bo'lgan algoritmlar sifatida ikkinchi guruhga tegishli bo'lgan Grain va Trivium algoritmlari olindi. Shuning uchun ushbu ikki algoritm bilan yaqindan tanishib chiqiladi. Bundan tashqari, birinchi guruhga tegishli bo'lgan Salsa va Rabbit algoritmlari ham o'zining kam resurs talab qilishi bilan LWC muhitida foydalanishga mosligini ko'rsatdi.

Dasturiy ko'rinishda amalga oshirish uchun mos bo'lgan shifrlash algoritmlari. Salsa20/r deb (r – raund funksiyasidagi takrorlanishlar soni) umumiy nomlanuvchi algoritm eSTREAM loyihasining dasturiy ko'rinishda amalga oshirish bo'yicha final boshqichi qatnashchisi hisoblanib, ma'lumotni shifrlash uchun 256 bitli kalit va 128 bitli IV talab etiladi. Ushbu algoritmning amalda quyidagi variantlari keng qo'llaniladi:

- Salsa20/20 – yuqori xavfsizlik darajasini talab qilgan kriptografik ilovalarda;
- Salsa20/12 va Salsa20/8 variantlari yuqori tezkorlikni talab etuvchi, yuqori xavfsizlikni talab etmaydigan muhitlar uchun.

Ushbu algoritm dasturiy ko'rinishda amalga oshirishga qulay bo'lib, uning matematik asosini qo'shish, modul 232 bo'yicha qo'shish, bitlar bo'yicha siljitish va ARX amallari tashkil etadi. Shu sababli, ushbu algoritm ma'lumotni shifrlashda va rasshifrovkalashda yuqori tezkorlikni qayt etadi. Ushbu algoritmning yuqori keltirilgan barcha variantlari tezkor algoritm bo'lgani sababli, aksariyat kriptografik kutobxonalar (masalan, Crypto++) va dasturlash tillari tarkibiga kiritilgan.

Algoritmning 4 raundli funksiya asosida shifrlash jarayonining C/C++ dasturlash tilidagi ko'rinishi 8-ildav keltirilgan. Ushbu algoritmning eng optimal tarzda yozilgan dasturiy ko'rinishi 1452 bayt hajmga ega va shifrlash uchun 18400 takt (sikl) talab etiladi [21]. Eng optimal ravishda amalga oshirilgan qurilma ko'rinishida esa 12126 ta mantiqiy elementni (Gate equivalent, GE) talab qiladi [22]. Shu sababli ushbu algoritm LWC uchun mos kelmaydi (ko'plab izlanuvchilar tomonidan LWC uchun 300 GE talab qo'yilgan [23-25]) deb xulosa qilingan. Algoritmning 8-

raundli versiyasi uchun qator hujumlar amalga oshirilgani aytilgan bo'lsada, qolgan versiyalar uchun kalitni to'liq tanlash hujumidan boshqa hujum olib borilmagan [26].

Rabbit oqimli shifrlash algoritmi sinxronlanishgan turga tegishli bo'lib, dasturiy ko'rinishda amalga oshirishga mo'ljallangan. Algoritm dastlab 2003-yilda taqdim etilgan bo'lib, Martin Boesgaard, Mette Vesterager, Thomas Pedersen, Jesper Christiansen va Ove Scaveniuslar tomonidan loyihalangan. Ushbu shifrlash algoritmining asosini ARX va mod232 matematik amallari tashkil qilib, 128 bitli kalit va 64 bitli IVdan foydalanadi. Ushbu algoritm mualliflar tomonidan patentlangan bo'lsada, ochiq foydalanish uchun ham mavjud (masalan, ISO/IEC 18 033-4:2011 tarkibida standartlashtirilgan [27, 28]).

Rabbit algoritmda ichki holatni kuchli aralashtirish uchun foydalanilgan funksiya hisoblash qurilmasida mavjud sodda arifmetik amallarga asoslangani uchun ham apparat ham dasturiy amalga oshirishga qulay hisoblanadi. Xususan, Pentium 3 muhitida algoritm yordamida 1 bayt ma'lumotni shifrlashda 3.7 protsessor sikli talab etilgan bo'lsa, ARM7 uchun bu ko'rsatkich 9.7 ga teng [29]. Bundan tashqari algoritmni apparat amalga oshirish uchun eng minimal holatda 3800 ta mantiqiy element (GE) talab etilgan. Ushbu algoritmgga qaratilgan hujumlar asosan TMD oilasiga tegishli bo'lib, kichik uzunlikdagi IVdan foydalanilganda kalit uzunligini 96 bitgacha tushirishi aniqlangan [30]. Ushbu algoritmgga nisbatan qator hujumlar amalga oshirilgan bo'lsada, ularning natijasi kalitni to'liq tanlash hujumidan olingan natijalardan yuqori bo'lgan.

HC algoritmining ikki ko'rinishi: HC-128 va HC-256 mavjud bo'lib, ularda mos ravishda 128 va 256 bitli kalit va 128 bitli IV dan foydalanilgan hamda kichik kalit uzunligi variatni eSTREAM loyihasining dasturiy ko'rinishga mo'ljallangan yo'nalishi bo'yicha ishtirokchisi hisoblanadi. Mazkur algoritm 2004-yilda Hongjun Wu tomonidan birinchi marta taqdim etilgan bo'lib, muallif tomonidan patentlanmagan. Algoritm maxfiy bo'gan ikkita (P va Q) jadvaldan iborat bo'lib, ularning har biri 32 bitli 1024 ta elementdan iborat. Har bir qadamda jadvallar holati yangilanib, to'liq yangilanish uchun 2048 sikl talab etiladi. Mazkur algoritm aksariyat kriptografik kutubxonalarda (CyaSSL) mavjud bo'lib, 128 bitli varianti foydalanilgan jadvallar uzunligini kichikligi bilan farqlanadi.

Ushbu algoritmning 256 bitli varianti Pentium 4 muhitida ma'lumotning bir baytini shifrlash uchun 4 ta protsessor siklini talab qilgan bo'lib, mualliflar tomonidan initsializatsiya jarayoni uchun 74 000 sikl talab etilishi aytilgan [22]. Ushbu algoritmgga nisbatan kriptotahlillar deyarli amalga oshirilmagani bois, uni xavfsiz deb qarash mumkin.

SOSEMANUK sinxronlashgan oqimli shifrlash algoritmi yuqorida keltirilgan algoritmlar kabi dasturiy ko'rinishga qulay bo'lib, u Come Berbain va boshqalar tomonidan yaratilgan. Algoritmida 128 yoki 256 bitli kalitlar va 128 bitli IV dan foydalanilgan. Biroq, algoritmning bardoshligi barcha kalit uzunliklari holati uchun ham 128 bitga tengligi tahlillar natijasida aniqlangan. Ushbu algoritmni yaratishda mualliflar tomonidan SNOW 2.0 [31, 46] oqimli shifri va Serpent [57] blokli shifrlarining ayrim elementlaridan foydalanilgan. Shu sababli, algoritm SNOW 2.0 algoritmgaga qaraganda tezkor hisoblanib, bu initsializatsiya bosqichini tezkorligi bilan xarakterlanadi. eSTREAM loyihasi doirasida amalga oshirilgan nazariy tahlillar natijasi 2224 hisoblashga teng bo'lgan. Ushbu algoritmda kalitlarni o'rnatish bosqichi uchun 24 raundli Serpent algoritmi akslantirishidan foydalanilgani bois, algoritmni dasturiy tomondan amalga oshirishda 2000-5000 bayt xotira talab qilinadi. Ushbu algoritm qurilmada amalga oshirish uchun mo'ljallanmagan bo'lsada, 18819 ta mantiqiy elementlar yordamida algoritmni amalga oshirish mumkinligi isbotlangan [22].

Qurilmaga mo'ljallangan oqimli shifrlash algoritmlari. Grain oqimli shifrlash algoritmi qurilmaga amalga oshirish uchun mo'ljallangan bo'lib, 2004-yilda Martin Hell va uning jamoasi tomonidan yaratilgan. Ushbu algoritm LFSR va chiziqliq filterlash funksiyasidan iborat bo'lib, 80 bitli kalit va 64 bitli IV dan foydalanilgan. Mualliflar tomonidan har bir kalit va IV jufti uchun maksimal chiqish ketma-ketligining uzunligiga talab qo'yilmagan. LFSR minimal kalit ketma-ketlik davrini va chiqishdagi muvozanatni kafolatlab, algoritm 128 bilti xavfsizlik va autentifikatsiyani ta'minlashi mualliflar tomonidan aytilgan.

Grain oqimli shifrlash algoritmi qurilmada amalga oshirish uchun mos bo'lib, odatiy holda ma'lumotni bir bitini shifrlash uchun 1 protsessor siklini talab etadi. Biroq, ushbu algoritmni amalga oshirishning samarali usullarini ishlab chiqish mumkin bo'lib, buning natijasida tezkorlikni 16 protsessor sikligacha yetkazish mumkin. Ushbu algoritm kichik hisoblash muhitida A5/1 va E0 algoritmlaridan yuqori xavfsizlik darajasini ta'minlaydi [23]. Bundan tashqari algoritmning 128 bit kalit va 96 bitli IV dan foydalanilgan Grain 128 versiyasi ham mavjud.

Grain-128a algoritmi Grain 128 algoritmining xavfsizlik nuqtai nazaridan takomillashtirilgan versiyasi bo'lib, 2011-yilda Symmetric Key Encryption Workshop (SKEW) loyihasi doirasida taqdim etilgan. Algoritmi 128 bit kalit va 96 bitli IV dan foydalanib, yuqori xavfsizlik darajasini ta'minlaydi. Algoritmning chiqish oldi funksiyasining ichki holat o'lchami 256 bitga teng bo'lib, teng ravishda NLFSR va LFSR turidagi registrlarga bo'lib saqlanadi.

Grain 128a algoritmi tag o'lchamini 1 bitdan 32 bitgacha oshirish imkoniga ega bo'lib, algoritmning maksimal tag uzunligi holati dasturiy tomondan amalga oshirishga qulay hisoblanadi. Xususan, algoritmni 1 bitli tag holatida apparat ko'rinishda amalga oshirish uchun 1857 ta GE element talab qilingan bo'lsa, maksimal qiymat holati uchun 4617 GE ta element talab qilgan [34]. Grain va uning variantlari uchun qator kriptotahlilashlar amalga oshirilgan bo'lsada, qoniqarli natijalar qo'lga kiritilmagan [35].

Trivium shifrlash algoritmi ham ikkinchi guruhga tegishli algoritmi bo'lib, eSTREAM konkursining finalisti hisoblanadi va u yengil kriptografik algoritmlar standartida (ISO/IEC 29192-3:2012) qayd etilgan. Ushbu algoritmi mualliflari oqimli shifrlarni qanday qilib uning xavfsizligi, tezkorligi va moslashuvchanligini yo'qotmasdan soddalashtirish mumkin degan savolga javob topishga harakat qilgan. Ushbu algoritmi oqimli shifrlarni yaratishning sinxronlashgan turiga tegishli bo'lib, 80 bitli kalit va 80 bitli IV dan foydalanib, har bir kalit va IV juftligi uchun 264 chiqish qiymatini xavfsiz generatsiyalashga imkon beradi.

Apparat shaklda algoritmi standart CMOS (Complementary metal-oxide semiconductor) texnologiyasida amalga oshirish uchun 2017 ta mantiqiy element talab qilingan bo'lsa, C2MOS texnologiyasida bu ko'rsatkich 749 ga teng bo'lgan [36].

Ushbu algoritmi qurilmada amalga oshirish uchun mo'ljallangan bo'lsada, dasturiy vosita ko'rinishga ham amalga oshirishga qulay. Xususan, algoritmning initsializatsiya bosqichini amalga oshirish uchun 2050 ta, kalitni o'rnatish bosqichi uchun 55 ta va bir baytni shifrlash uchun 12 ta protsessor sikli talab etilgan [45].

Ushbu algoritmi sodda bo'lgani uchun unga qaratilgan ko'plab hujumlar amalga oshirilgan bo'lsada, ulardan olingan natijalar kalitlarni to'liq tanlash hujumidan olingan natijalardan yaxshi emas.

MICKEY 2.0 (Mutual Irregular Clocking KEYstream generator) algoritmi ham eSTREAMning qurilmalar uchun mos algoritmlar guruhidagi ishtirokchisi bo'lib, Steve Babbage va Matthew Dodd tomonidan 2006-yilda taqdim etilgan. Algoritmi 80 bitli kalit va [0, 80] oraliqdagi o'zgaruvchan uzunlikdagi IV lardan foydalanib, har bir kalit va IV juftligi uchun 240 ketma-ketlik bitini generatsiyalash imkonini beradi. Ushbu algoritmning qurilma ko'rinishda amalga oshirish uchun 3188 ta mantiqiy element talab qilinadi [38]. Grain va Trivium shifrlari kabi, ushbu algoritmi uchun ham 2013-yilda Subhadeep Banik va Subhamoy Maitra tomonidan differensial kriptotahlil amalga oshirilgan.

MICKEY-128 2.0 algoritmi MICKEY ning takomillashtirilgan versiyasi bo'lib, yuqori xavfsizlikni ta'minlashni maqsad qilgan. Shu sababli, 128 bitli kalit va [0, 128] oraliqidagi IV dan foydalanadi [41]. Ushbu algoritmi XOR-CHAIN strukturasi yordamida himoyalangan bo'lib, algoritmi qurilmada amalga oshirish uchun 5039 ta mantiqiy elementlar talab qilinadi [40].

Enocoro shifri. eSTREAM konkursidan tashqari, International Organization for Standardization/ International Electrotechnical Commission 29192-3:2012 [42] tomonidan ham LWC uchun oqimli shifrlar standartlashtirilgan. Xususan, ushbu standart ikki oqimli shifrni: Trivium va Enocoro [43] o'z ichiga olib, 9-ildoda ushbu ikki shifrning umumiy ko'rinishini keltirilgan.

Trivium shifri eSTREAM konkursida qurilmalar uchun mos bo'lgan algoritmlar doirasida finalchi hisoblansa, Encoro shifri esa 2007-yilda Hitachi tomonidan taqdim qilingan 4 ta algoritm qatorida standartlashtirilgan. Ushbu algoritm AES shifrlash algoritmining shifrlash jarayonida sarflagan quvvat sarfini 1/10 qayt etishi bilan xarakterlanadi. Shuning uchun ushbu algoritm hisoblash imkoniyati cheklangan qurilmalar va sensorlarda foydalanish uchun juda mos.

Encoro shifrlash oilasi Encoro-80 va Encoro-128 [44] shifrlaridan tashkil topgan bo'lib, ular mos holda 80 va 128 bitli kalitlardan foydalanadi. Encoro shifrida 64 bitli IV foydalanilib, algoritm xavfsizligini baytga asoslangan S-jadval ta'minlaydi. Ushbu algoritm akslantirishlari ham qurilma ham dasturiy ko'rinishda amalga oshirishga qulay bo'lib, har bir raundda 1 bayt hosil qilinadi. Har bir kalit/

IV juftligi bilan algoritm 264 bayt psevdotasodifiy ketma-ketlikni hosil qilish imkonini beradi.

Qurilma ko'rinishda Encoro-80 versiyasida 2700 mantiqiy elementlar talab qilinsa, Encoro-128 uchun bu ko'rsatkich 4100 ga teng [43, 44]. Dasturiy ko'rinishida esa Encoro-128 algoritmini ishga tushurishda 4869.5 ta protsessor sikli talab etilsa, bir baytni generatsiyalashda 46.3 sikl talab qilinadi. Ushbu algoritmdan olingan natijalar NIST statistik testlar to'plamidan o'tgan, olib borilgan tahlil natijalari kalitni barcha variantlarini hisoblash murakkabligidan yuqori bo'lgani bois algoritmni xavfsiz deb aytish mumkin.

Bundan tashqari, eSTREAM loyihasi ishtirokchisi bo'lmagan, biroq, yetarli xavfsizlik va samaradorlik ko'rsatkichlariga ega algoritmlar mavjud bo'lib, ularning tahlili bilan quyida tanishib o'tiladi.

BEAN oqimli shifrlash algoritmi Grain shifriga asoslangan bo'lib, apparat ko'rinishda amalga oshirishga qulay hisoblanadi. Ushbu algoritm 2009-yilda Navi Kumar va uning jamoasi tomonidan ishlab chiqilgan. Algoritm ikkita 80 bitli siljitish registori va chiqish funksiyasidan iborat. Grain algoritmidan ikkita, LFSR va NFSR registrlaridan foydalanilgan bo'lsa, Bean algoritmidan FCSR registridan foydalanilgan. Algoritm 80 bitli kalitdan foydalanib, xavfsizlik, narx va tezkorlik omillarining eng mos qiymatlarini o'zida qayt etgan. Algoritm mualliflari tomonidan 107 bit uzunlikdagi psevdotasodifiy qiymatni hosil qilishda Grain algoritmdan 1.5 marta kam vaqt sarflagani va 10% kam xotira hajmini talab qilgani ko'rsatilgan. Algoritm NIST testlar to'plamidan o'tgan bo'lsada, Martin Agren va Martin Hell tomonidan chiqish funksiyasining optimal emasligi natijasida algoritm bardoshligi 273 ga tushishi ko'rsatilgan [45].

Quadium oqimli shifrlash algoritmi Trivium algoritmining kengaytirilgan varianti bo'lib, 2012-yilda Yun Tian va boshqalar tomonidan yaratilgan. Algoritm 288 bit ichki holatga ega bo'lib, 80 bitli kalit va 80 bit dastlabki qiymatni talab qiladi. Ushbu algoritmda 4 raundli Trivium algoritmidagi kabi siljitish registridan foydalanilgan.

Ushbu shifrlash algoritmini to'liq apparat tarzda amalga oshirishda 3495 GE talab qilinsa, 3 raundli versiyasi uchun 2372 GE talab qilinadi. Dasturiy ko'rinishda esa Trivium kabi tezkorlik qayd etadi. Algoritmning 3 raundli versiyasining C++ dasturidagi shifrlash natijasi Triviumga nisbatan 30% ortiq tezkorlikni qayd etgan.

Cavium oqimli shifrlash algoritmi ham Trivium algoritmiga asoslangan bo'lib, CA dan foydalanib ham chiziqli ham chiziqli akslantirishlarga tayanadi. Ushbu loyiha LFSR va NFSR tuzilmalariga qaraganda tezkor bo'lgani sababli, Trivium algoritmidagi kalitlarni o'rnatish bosqichi raundlarini kamaytirgan. Ushbu shifrlash algoritmiga nisbatan kriptotahlil usuli amalga oshirilmagan.

A2U2 oqimli shifrlash algoritmi apparat amalga oshirishga mos algoritm bo'lib, juda ham cheklangan resurs muhiti uchun (masalan, RFID teglari uchun) mo'ljallangan. Mazkur holda amalga oshirish uchun 500 GE talab qilinadi. Ushbu shifrlash algoritmi sinxronlashgan shifrlash algoritmi hisoblanib, 56 bitli kalitdan foydalanadi. A2U2 shifri simmetrik oqimli va blokli shifrlash prinsiplarini o'zida mujassamlashtirgan. Kichik imkoniyatli qurilmalarda amalga oshirish uchun, A2U2 algoritmi kichik sondagi registrlardan qayta foydalanishga asoslanadi. Ushbu shifrlash algoritmini apparat amalga oshirishga mostlash uchun KATAN blokli shifrlash algoritmidan

qo'llanilgan texnologiyadan foydalanilgan. Bundan tashqari, A2U2 shifrlash algoritmi qayta aloqa va filter funksiyasidan doimiy bo'lmagan o'zgartirishlar asosida foydalanilgan.

A2U2 shifrlash algoritmini apparat amalga oshirilishi 284 ta mantiqiy elementlarni talab qiladi. Biroq, algoritmda kichik kalitdan foydalanilgani sababli tanlangan ochiq matnga asoslangan kriptotahlil usuli bilan maxfiy kalitni tiklash imkoniyati mavjud.

WG-7 shifri. 80 bitli kalit va 81 bitli IV dan foydalanuvchi WG-7 shifri eSTREAM konkursining ikkinchi guruhida qatnashgan WG oqimli shifrining yangilangan versiyasi hisoblanadi. Ushbu algoritm RFID qurilmalari uchun mo'ljallangan bo'lib, chekli F7 maydonida 23 qadamli LFSRdan foydalanadi. O'z

navbatida LFSR qiymati WG o'zgartirishiga asoslangan chiziqsiz filterlash funksiyasiga kiritiladi.

WG-8 shifri esa WG-7 shifrning yangilangan versiyasi hisoblanib, 80 bitli kalit va IV dan foydalanadi. Bundan tashqari, F8 o'lchamdagi chekli maydondan foydalanib qurilgan algoritm, WG oilasiga tegishli algoritmlarning barcha yaxshi

xususiyatlarini o'zida mujassamlashtirgan va oqimli shifrlarga qaratilgan hujumlarga bardoshli hisoblanadi. Ushbu algoritm kam quvvat talab qilib, yuqori tezkorlikni qayt etadi. Algoritmnining mualliflar tomonidan Atmega128L muhitida amalga oshirilgan versiyasi ma'lumotni shifrlashda 185.5Kb/sek natija qayt etgan.

CAR30 algoritmi CA loyihalash yondashuviga asoslangan bo'lib, 2013-yilda Sourav Das va Dipanwita Roy Chowdhurylar tomonidan taklif etilgan. Taklif etilgan algoritm kichik uzunlikdagi xabarlarni shifrlashda qulay bo'lib, algoritmni ham apparat ham dasturiy amalga oshirish imkoniyati mavjud. Algoritm 128 bitli kalit va

120 bitli IV lardan foydalanib, har bir iteratsiyada 128 bitli psevdotasodifiy ketma-ketlikni taqdim qiladi. Algoritm yordamida hosil qilingan ketma-ketliklar NIST testlar to'plamidan o'tgan bo'lib, algoritmni zamonaviy kriptotahlil usullariga bardoshligi mualliflar tomonidan ko'rsatilgan [46]. Algoritmni ham dasturiy ham apparat tarzda amalga oshirish mumkinligi mualliflar tomonidan ko'rsatilgan. Xususan, algoritmni dasturiy amalga oshirishda bir baytni shifrlash uchun 160 protsessor sikli talab etilgan.

TinyStream oqimli shifrlash algoritmi TinySec algoritmiga asoslangan bo'lib, 2010-yilda Tieming Chen va boshqalar tomonidan taklif etilgan. Algoritmida

128 bitli kalitdan foydalanilib, WSN tarmoq qurilmalarida foydalanish uchun mo'ljallangan. Algoritm loyihalash bo'yicha TPM yondashuviga asoslangan. Algoritmning har bir holat siljishida 128 bitli ketma-ketlik hosil bo'lib, ularni to'liq ENT testlar to'plamidan o'tganligi mualliflar tomonidan ko'rsatilgan. Ushbu algoritm TinyOS muhitida dasturiy ko'rinishda amalga oshirilganda ROMdan 65 024 bayt va RAMdan 1 659 184 bayt xotira talab qilishi mualliflar tomonidan qayt etilgan. TinyStream algoritmiga nisbatan jiddiy kriptotahlillar amalga oshirilmagan [46].

Autentifikatsiyani ta'minlovchi ixcham shifrlar. Autentifikatsiyani ta'minlovchi shifrlashda shifrmatnga qo'shimcha ravishda autentifikatsiya tegi hosil qilinib, uning asosiy maqsadi xabar yaxlitligi va autentifikatsiyasini ta'minlash hisoblanadi. Rasshifrovkalash jarayonida esa parallel ravishda yaxlitlikni tekshirish ham amalga oshiriladi hamda ochiq matn va autentifikatsiya tegi mos kelmasa yaxlitlik buzulgan deb hisoblanadi. Ushbu jarayonning umumiy sxemasi 10-ilovada keltirilgan. Bu turdagi shifrlash usullari onlayn ilovalar uchun juda muhim hisoblanib, aloqani uzish, qalbakilashtirish va shifrmatnni o'zgartirish kabi hujumlarni oldini olish imkonini beradi. Ilovalarda autentifikatsiyani ta'minlovchi shifrlashni ta'minlashda eng mos echim AES-GCM hisoblansada, bu cheklangan hisoblash imkoniyatli muhitlar uchun o'rinli hisoblanmaydi. Shuning uchun bunday muhitlar uchun maxsus yechimlarni topish talab etiladi. WG-7 shifrlash usuli RFID teglari va "ma'lumot o'quvchi" o'rtasida ikki tomonlama autentifikatsiyani ta'minlaydi. Shu sababli, WG-7 dan ushbu muammoning yechimi sifatida foydalanish mumkin.

Hummingbird-2 shifri ultra-ixcham oqimli shifrlash algoritmi bo'lib, 256-bitli kalit va 64 bitli IVdan foydalanib har bir xabar uchun autentifikatsiya tegi hosil qilinadi. Ushbu algoritmning ichki holati 128 bitgacha bo'lib, 4x4 o'lchamli S jadvaldan foydalanilgan. Bundan tashqari, so'zlar

o'rtasida XOR amali, mod 65536 bo'yicha qo'shishdan foydalanilgan. Mazkur algoritm mualliflari tomonidan differensial, chiziqli, algebraik kriptotahlil usullariga baholangan. Baholash natijalari algoritmni ushbu hujumlarga bardoshligini ko'rsatgan. Hummingbird-2 algoritmi ham dasturiy ham apparat tarzda amalga oshirishga qulayligi, mualliflar tomonidan turli muhitlarda o'tkazilgan testlash natijalari bilan ko'rsatilgan.

Rabbit-MAC shifrlash algoritmi autentifikatsiyani ta'minlovchi shifrlash guruhiga tegishli bo'lib, Rabbit shifri asosida 2008-yilda Ruhma Tahir va boshqalar tomonidan ishlab chiqilgan. Ushbu algoritm WSN tarmoq qurilmalari uchun mo'ljallangan bo'lib, kanal sathida autentifikatsiya, yaxlitlik va konfidensiyalikni ta'minlaydi. Ushbu algoritm WSN tarmog'ida ikki nuqta o'rtasida xavfsizlikni ta'minlab qolmasdan, nuqtalararo maxfiy aloqani o'rnatish imkonini beradi. Ushbu shifrlash algoritmiga ko'ra simmetrik shifrlash kaliti oldindan ochiq kalitli kriptografik tizimlar orqali yetkazilib, IV parametrini xavfsiz uzatishda sarflanuvchi tarmoq yuklamasini kamaytirish uchun ular paket sarlavhasiga biriktiriladi. Bundan tashqari, ushbu kattaliklar turli paketlar uchun turlicha bo'lib, xavfsizlikni madadlashda yordam beradi. MAC tashkil etuvchisi keyingi holat funksiyasi hisoblanib, talab qilinganda amalga oshiriladi va bunda "shifrlash – keyin – MAC" yondashuvidan foydalaniladi.

ACORN shifrlash usuli yangi oqimli shifrlash usuli bo'lib, autentifikatsiya imkoniyatiga ega shifr hisoblanib, Hongjun Wu tomonidan 2006-yilda yaratilgan va CEASAR konkursi ishtirokchisi hisoblanadi. ACORN shifri 128 bitli kalit va 128 bitli IV dan foydalanib, 264 bitgacha psevdotasodifiy ketma-ketlikni hosil qilish imkonini beradi. Algoritm yaxlitlikni ta'minlash uchun 128 bitgacha bo'lgan autentifikatsiya tegini hosil qiladi. ACORN-128 algoritmining ichki holati 293 bitga teng bo'lib, algoritmning ishga tushishi uchun 1792 qadam talab etiladi. Algoritm holat, umumiy qayta aloqa biti va holatni yangilash funksiyasi yordamida psevdotasodifiy ketma-ketliklarni hosil qiladi. Barcha ochiq matnlar shifrlanib bo'lganidan so'ng, autentifikatsiya tegini hosil qilish amalga oshiriladi. Rasshifrovkalash muolajasi ham xuddi shu tarzda amalga oshiriladi.

Sablier shifri ham CEASAR konkursida ishtirok etgan oqimli shifrlash algoritmi hisoblanib, 2014-yilda Bin Zhang va boshqalar tomonidan taklif etilgan. Algoritm autentifikatsiyalash imkoniyatiga ega shifrlash turiga tegishli bo'lib, 80 bitli kalit va IVlardan foydalanadi. Ushbu algoritm apparat tarzda amalga oshirishga qulay bo'lgan Trivium algoritmiga nisbatan 15 marta tezkor bo'lib, amalga oshirish uchun 1926 ta mantiqiy elementlarni talab qiladi. Ushbu algoritmga nisbatan kalitli to'liq tanlash hujumiga nisbatan samarali bo'lgan kriptotahlil amalga oshirilmagan [46].

ASC-1 algoritmi oqimli shifrlash algoritmi bo'lib, 2012-yilda Goce Jakimoski va Samant Khajurialar tomonidan autentifikatsiyani ta'minlovchi shifrlash algoritmi sifatida taqdim etilgan. Algoritm asosini 128 bitli kalitga ega AES tashkil etib, CFB rejimidan foydalanilgan. Ushbu algoritm blokli shifrga asoslangani bois, nisbatan sekin va yuqori hisoblash resursini talab qiladi.

ALE algoritmi AES algoritmiga asoslangan yana bir ixcham autentifikatsiyani ta'minlovchi shifrlash sxemasi bo'lib, 2013-yilda Andrey Bogdanov va boshqalar tomonidan taqdim etilgan. Ushbu algoritmning asosini AES raund akslantirishlari va AES-128 kalitni kengaytirish algoritmi tashkil qiladi. Ushbu algoritm 128 bitli kalit va 128 bitli IV dan foydalanib, algoritmni ASIC muhitida amalga oshirish uchun 2500 ta mantiqiy elementlar talab etiladi.

Yuqorida keltirilgan oqimli shifrlarning yakuniy tahlili haqidagi ma'lumotlar 11-ildavda keltirilgan bo'lib, tahlil natijasi RC4, A5/1, E0, Trivium, Rabbit, Sosemanuk, Mickey 2.0, Bean, WG-7, A2U2, ALE, Sablier, Grain va Hummingbird oilasiga tegishli shifrlardan yuqori xavfsizlik talab qilinuvchi ilovalar uchun foydalanish maslahat berilmaydi. Nisbatan yangi ishlab chiqilgan algoritmardan foydalanishdan oldin esa chuqur tahlil qilish talab etiladi.

Sanoq rejimida AES algoritmidan foydalanish oqimli shifrlash algoritmilarini yaratishga yaxshi namuna hisoblanadi. Shuningdek, ushbu shifrlash algoritmi qurilmalar uchun ham mos bo'lib, yangi ishlab chiqilgan algoritmarni solishtirish uchun etalon sifatida ham xizmat qiladi. Biroq, sanoq rejimidagi AES barcha muhitlar uchun ham tavsiya etilmaydi, masalan, quvvat manbai cheklangan va RFID tizimlari uchun. Bunday hollarda Enocoro algoritmidan foydalanish mumkin

bo'ladi. Ushbu algoritmi aynan sanoatda LWC muhiti uchun ishlab chiqilgan bo'lib, dasturiy vositada ham amalga oshirish imkoni mavjud.

AES-CTR algoritmi ham apparat ham dasturiy ko'rinishda amalga oshirishga qulay bo'lgani kabi, autentifikatsiyani amalga oshiruvchi oqimli shifrlar doirasida ACORN algoritmi eng yaxshi tanlov hisoblanadi. Bundan tashqari, ACORN algoritmini so'ngi paralellashtirish texnologiyalari asosida tezkorligini yanada oshirish imkoni mavjud. WSN va FRID muhitlari uchun WG-8 algoritmi ham xavfsizlik ham quvvat samaradorligi bo'yicha eng yaxshi tanlov hisoblanadi.

O'zi sinxronlashuvchi oqimli shifrlarga amaliyotda sinxronlashgan algoritmlar kabi talabning yuqori emasligi yuqorida aytib o'tildi. Xavfsiz sinxronlashgan shifrlar o'rnatilgan tizimlar, hisoblash imkoniyati cheklangan muhitlar, sensor tarmoqlar uchun asosiy tanlov hisoblanadi. Autentifikatsiyalash imkoniyatiga ega shifrlar ham muhim bo'lgan autentifikatsiya teglarini taqdim qiladi. Biroq, ushbu shifrlash sxemalari qator hujumlarga bardoshsizligi bois, amalda keng qo'llanilmaydi. Shuning uchun mazkur muammoni bartaraf etishda odatda "shifrlash-keyin-MAC" sxemasidan keng foydalaniladi va bu odatiy autentifikatsiyalash imkoniyatiga ega shifrlarga qaraganda yuqori xavfsizlikni ta'minlaydi.

Xulosa o'rnida shuni aytish mumkinki, xavfsiz algoritmi tanlash bilan butun ilovaning xavfsizligi ta'minlanmaydi. Boshqacha aytganda, butun ilovani loyihalash davomida nafaqat algoritmlarning xavfsizligiga, balki, ularning to'g'ri tanlanganligiga va to'g'ri birlashtirilganiga ham e'tibor berish kerak bo'ladi. Apparat ko'rinishda amalga oshirish natijalari. Tahlil qilingan oqimli shifrlarni apparat ko'rinishda amalga oshirish muhiti cheklangan bo'lib, [46] manbada mualliflar tomonidan Verilog tilida 5 ta oqimli shifrlash algoritmlari amalga oshirilgan. Bunda, Spartan-3 1.2V FPGA apparat muhiti tanlab olingan. Tahlil jarayonida baholash omillari sifatida o'tkazish qobiliyati (throughput, MBps), kutish qiymati (latency, sikl/blok), maksimal chastota (maximum frequency, MHz), quvvat (power, W) va talab qilingan triggerlar hamda qatlam (flip-flops va slices) parametrlari tanlangan hamda olingan tahlil natijalari 1-jadvalda keltirilgan.

1 – jadval

FPGA muhitida algoritmlarning omillar bo'yicha tahlili

Shifr	Kalit uzunligi (bayt)	Blok uzunligi (bit)	IV (bayt)	Kutish qiymati (sikl/ blok)	O'tkazish qobiliyati (MBps)	Mak. Chastota (MHz)	Quvvat (mW)	FF	Qatlamlar	O'tkazish qobiliyati/ qatlamlar
Yaxshisi				Pasti	Yuqorisi		Pasti	Pasti	Pasti	Yuqori
WG-8	10	1	10	1	2112	192	16	207	398	0.66
Enocoro 80	10	1	8	1	900	118	8	239	292	0.38
Enocoro 128	16	1	8	1	1200	149	8	362	442	0.33
AES-128	16	128	–	226	8754	77	78	781	5948	0.18
WG-8	10	11	10	1	190	190	5	85	137	0.17
Salsa20	32	32	8	2	990	19.4	12	1286	2036	0.06
HC,128	16	512	16	–	–	–	–	–	> 262000	–

Bundan tashqari, ushbu algoritmlarni ASIC (Application specific integrated circuit) muhitida amalga oshirish natijalari ham keltirilgan. Mazkur holda tahlillash omili sifatida o'tkazish qobiliyati, *GE* va yuqori sifatli FOM (figure of merit) lar tanlab olingan. Bunda, FOM kattaligi *GE* tarzida hisoblangan va algoritmning qurilmada amalga oshirishdagi sifat darajasini ko'rsatgan. Mazkur muhitda olingan tahlil natijalari esa 2 – jadvalda keltirilgan.

2– jadval

ASIC muhitida algoritmlarning omillar bo'yicha tahlili

Shifr	Kalit uzunligi (bayt)	Blok uzunligi (bit)	IV (bayt)	Kutish qiymati (sikl/ blok)	Har 100 KHz da o'tkazish qobiliyati (MBps)	Tex. (mm)	Maydoni (GE)	FOM
Yaxshisi				Pasti	Yuqorisi		Pasti	Yuqorisi
WG-8	10	1	10	1	100	650	1 786	0.00391
Enocoro 80	10	1	8	1	–	90	2 700	–
Enocoro 128	16	1	8	1	800	90	4 100	0.00594
AES-128	16	128	–	226	56.64	350	2 400	0.00122
WG-8	10	11	10	1	1 100	650	3 942	0.00884
Salsa20	32	32	8	2	99	130	12 126	0.00008
HC,256	16	512	16	–	–	130	> 524 000	–

Tahlillar o'rnatilgan tizimlar uchun eng mos algoritm sifatida WG-8, Enocoro va AES algoritmlarini ko'rsatgan. Bular orasida WG-80 eng ixcham va samarali algoritm hisoblansa, Enocoro algoritmi ham yaxshi amalga oshirilish darajasiga egaligini va LWC muhitida amalga oshirish mumkin bo'lgan standartlashtirilgan algoritm ekanligini ko'rsatgan. AES algoritmi yuqori xavfsizlik darajasini qayd qilishi, energiya sarfini ham yuqori sarflanishiga sabab bo'lgan. Salsa20 va HC algoritmlarini esa o'rnatilgan qurilmalarda foydalanish uchun mos emasligi tahlillar natijasida aniqlangan.

Dasturiy ko'rinishga amalga oshirish natijalari. Apparat ko'rinishda amalga oshirish kabi, manbada mualliflari tomonidan ayrim oqimli shifrlash algoritmlarini C dasturlash tilida kredit karta o'lchamidagi o'rnatilgan qurilma, BeagleBone muhitida testlash amalga oshirildi. Tanlab olingan algoritmlar va omillar 3-jadvalda keltirilgan bo'lib, ularni tanlashda tahlil uchun eng mosligiga, eng xavfsiz deb hisoblanishiga va eng samarali deb topilganligiga e'tibor berildi.

Dasturiy vosita ko'rinishda amalga oshirishda Salsa20 algoritmi tezkorlik va ishga tushurish vaqtining qisqaligi bilan qolganlaridan ajralib turgan. Enocoro va WG-8 algoritmlari ham kam kod hajmi va kam xotira hajmini talab qilishi bilan ajralib turgan. Eng tezkor shifrlash algoritmi HC bo'lgan bo'lsa, eng past tezkorlik qayt etgan algoritmi AES standarti bo'lgan.

3 – jadval

Dasturlash muhitida algoritmning omillar bo'yicha tahlili

Shifr	Kalit uzunligi (bayt)	Blok uzunligi (bit)	IV (bayt)	Ishga tushirish (sikli)	Shifrlash (sikli)	ROM (bayt)	RAM (bayt)	Har 720 MHz da o'tkazish qobiliyati (KBps)	CM
Yaxshisi				Pasti	Pasti	Pasti	Pasti	Yuqori	Pasti
Salsa 20	16	512	8	460	29 491	4800	8 270	12 500	276
Salsa 20	32	512	8	460	29 729	4800	8 350	12 400	278
Enocoro 128	16	1	8	4 870	138	3800	7 560	5 200	526
WG-8	10	1	1	1 379	69	6600	590	10 400	456
HC,128	16	512	16	2 082 876	17 388	77 200	16 580	21 200	2 621
AES	16	128	–	6 953	20 480	22 200	88 000	4 500	3 552
AES-CTR	16	128	16	469.6	21 942	22 300	88 500	4 200	3 822

Zamonaviy oqimli shifrlash algoritmning xavfsizligi va samaradorligi ularning arxitekturasida va foydalanish muhitiga bevosita bog'liq. RC4, A5/1, va E0 kabi an'anaviy algoritmning jiddiy kriptotahliliy zaifliklari sababli yangi ilovalarda qo'llanilmaydi. eSTREAM loyihasida tavsiya etilgan algoritm — Salsa20, Trivium, Rabbit, Grain va boshqalar — amaliy samaradorlik va xavfsizlik nuqtai nazaridan keng tahlil qilindi. Bu algoritmning apparat va dasturiy bajarilish natijalari (quvvat, tezlik, GE, ROM/RAM sarfi) asosida ularning real tizimlarda qo'llanilish darajasi baholandi. LWC muhitlar uchun Enocoro, WG-8 va ACORN algoritmning eng mos variant sifatida ajralib turadi. Avtorizatsiyani ta'minlovchi shifrlar (Hummingbird-2, Rabbit-MAC) xavfsizlikni oshirishga xizmat qilsa-da, ularning ayrimlari resurs cheklovlari tufayli kam qo'llaniladi. Salsa20 va Trivium kabi ARX asosidagi yengil algoritm dasturiy muhitda yuqori tezlikni ta'minlasa, WG-8 va Enocoro algoritmning apparat jihatdan ixchamlik va energiya samaradorligi bilan ajralib turadi. ASIC va FPGA platformalarida o'tkazilgan testlar natijasida ularning samaradorlik ko'rsatkichlari raqamli tarzda baholandi. Tahlillar shuni ko'rsatmoqdaki, oqimli shifrnin tanlashda faqat nazariy xavfsizlik emas, balki amaliy talablar, platforma cheklovlari va shifrlash tezligi ham hisobga olinishi kerak.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

- [1] Rueppel R. A. Analysis and design of stream ciphers. – Springer Science & Business Media, 2012.
- [2] Zhang H., Wang X. Cryptanalysis of stream cipher grain family //Cryptology ePrint Archive. – 2009.
- [3] Ohigashi T. et al. How to recover any byte of plaintext on RC4 //International Conference on Selected Areas in Cryptography.–Berlin: Springer Berlin Heidelberg, 2013.–C.155-173.
- [4] Paul G., Maitra S., Srivastava R. On non-randomness of the permutation after RC4 key scheduling //Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: 17th International Symposium, AAECC-17, Bangalore, India, December 16-20, 2007. Proceedings 17. – Springer Berlin Heidelberg, 2007. – C. 100-109.

- [5] AlFardan N. J. et al. On the security of RC4 in TLS and WPA //USENIX Security Symposium. – 2013. – T. 173.
- [6] Gomułkiewicz M. et al. Synchronization fault cryptanalysis for breaking A5/1 //Experimental and Efficient Algorithms: 4th International Workshop, WEA 2005, Santorini Island, Greece, May 10-13, 2005. Proceedings 4. – Springer Berlin Heidelberg, 2005. – C. 415-427.
- [7] Zhang B. Cryptanalysis of GSM encryption in 2G/3G networks without rainbow tables //International Conference on the Theory and Application of Cryptology and Information Security. – Cham : Springer International Publishing, 2019. – C. 428-456.
- [8] Guneyssu T. et al. Enhancing COPACOBANA for advanced applications in cryptography and cryptanalysis //2008 International Conference on Field Programmable Logic and Applications. – IEEE, 2008. – C. 675-678.
- [9] Perkov L., Klisura A., Pavković N. Recent advances in GSM insecurities //2011 Proceedings of the 34th International Convention MIPRO. – IEEE, 2011. – C. 1502-1506.
- [10] Lu Y., Vaudenay S. Faster correlation attack on Bluetooth keystream generator E0 //Advances in Cryptology–CRYPTO 2004: 24th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 2004. Proceedings 24. – Springer Berlin Heidelberg, 2004. – C. 407-425.
- [11] Shaked Y., Wool A. Cracking the bluetooth pin //Proceedings of the 3rd international conference on Mobile systems, applications, and services. – 2005. – C. 39-50.
- [12] Jakobsson M., Wetzel S. Security weaknesses in Bluetooth //Cryptographers' Track at the RSA Conference. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2001. – C. 176-191.
- [13] Armknecht F. A linearization attack on the Bluetooth key stream generator //Cryptology ePrint Archive. – 2002.
- [14] Antonioli D., Tippenhauer N. O., Rasmussen K. Low entropy key negotiation attacks on Bluetooth and Bluetooth low energy //Cryptology ePrint Archive. – 2019.
- [15] NIST Special Publication 800-38A. Recommendation for block cipher modes of operation methods and techniques, NIST, 2001. (Available from: <http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf>) [Accessed 1 July 2015].
- [16] Robshaw M. The eSTREAM project //New stream cipher designs: the eSTREAM finalists. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2008. – C. 1-6.
- [17] Bernstein D. J. et al. ChaCha, a variant of Salsa20 //Workshop record of SASC. – 2008. – T. 8. – №. 1. – C. 3-5.
- [18] Raizada S. Some results on analysis and implementation of HC-128 stream cipher : дис. – Indian Statistical Institute-Kolkata, 2015.
- [19] Feldhofer M. Comparison of low-power implementations of trivium and grain //The State of the Art of Stream Ciphers, Workshop Record. – 2007. – C. 236-246.
- [20] Stefan D., Mitchell C. On the parallelization of the MICKEY-128 2.0 stream cipher //Proceedings of the ECRYPT State of the Art of Stream Ciphers. – 2008. – T. 17.
- [21] Sadkhan S. B., Salman A. O. A survey on lightweight-cryptography status and future challenges //2018 International Conference on Advance of Sustainable Engineering and its Application (ICASEA). – IEEE, 2018. – C. 105- 108.
- [22] Galanis M. D. et al. Comparison of the Hardware Implementation of Stream Ciphers //Int. Arab J. Inf. Technol. – 2005. – T. 2. – №. 4. – C. 267-274.
- [23] Juels A., Rivest R. L., Szydlo M. The blocker tag: Selective blocking of RFID tags for consumer privacy //Proceedings of the 10th ACM conference on Computer and communications security. – 2003. – C. 103-111.
- [24] Ranasinghe D. C., Engels D. W., Cole P. H. Low cost RFID systems: confronting security and privacy //Paper Auto-ID Labs White Paper Journal. – 2005. – T. 1.
- [25] McKay K. et al. Report on lightweight cryptography. – National Institute of Standards and Technology, 2016. – №. NIST Internal or Interagency Report (NISTIR) 8114 (Draft).

- [26] Mouha N., Preneel B. A Proof that the ARX Cipher Salsa20 is Secure against Differential Cryptanalysis //IACR Cryptol. ePrint Arch. – 2013. – T. 2013. – C. 328.
- [27] wolfSSL. CyaSSL Embedded SSL Library, wolf - SSL Inc., 2014. <http://www.yassl.com/yaSSL/Products-cyassl.html>
- [28] ISO/IEC 18033-4:2011. International standard for IT Security techniques, ISO/IEC, 2011. http://webstore.iec.ch/preview/info_isoiec18033-4%7Bed2.0%7Den.pdf
- [29]. Boesgaard M. et al. The stream cipher rabbit //ECRYPT Stream Cipher Project Report. – 2005. – T. 6. – C. 28.
- [30] Lu Y., Wang H., Ling S. Cryptanalysis of rabbit //Information Security: 11th International Conference, ISC 2008, Taipei, Taiwan, September 15-18, 2008. Proceedings 11. – Springer Berlin Heidelberg, 2008. – C. 204-214.
- [31] Jiao L., Li Y., Hao Y. A guess-and-determine attack on SNOW-V stream cipher //The Computer Journal. – 2020. – T. 63. – №. 12. – C. 1789-1812.
- [32] Anderson R., Biham E., Knudsen L. Serpent: A proposal for the advanced encryption standard //NIST AES Proposal. – 1998. – T. 174. – C. 1-23.
- [33] Otte D. AVR-Crypto-Lib, AVR-Crypto-Lib, 2009. <http://www.das-labor.org/wiki/AVR-Crypto-Lib/en>
- [34] Ouafi K., Vaudenay S. Smashing squash-0 //Advances in Cryptology- EUROCRYPT 2009: 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings 28. – Springer Berlin Heidelberg, 2009. – C. 300-312.
- [35] Banik S., Maitra S., Sarkar S. A differential fault attack on the grain family of stream ciphers //International Workshop on Cryptographic Hardware and Embedded Systems. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2012. – C. 122-139.
- [36] SUZER M. H., BEŞLİ N. A New Software Implementation of TRIVIUM Stream Cipher //Harran Üniversitesi Mühendislik Dergisi. – 2020. – T. 5. – №. 1. – C. 1-8.
- [37] Dey P., Adhikari A. Improved multi-bit differential fault analysis of Trivium //International Conference on Cryptology in India. – Cham : Springer International Publishing, 2014. – C. 37-52.
- [38] Good T., Benaissa M. ASIC hardware performance //New Stream Cipher Designs: The eSTREAM Finalists. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2008. – C. 267-293.
- [39] Karmakar S., Chowdhury D. R. Differential fault analysis of MICKEY- 128 2.0 //2013 Workshop on Fault Diagnosis and Tolerance in Cryptography. – IEEE, 2013. – C. 52-59.
- [40] Karmakar S., Chowdhury D. R. Differential fault analysis of MICKEY family of stream ciphers //Cryptology ePrint Archive. – 2014.
- [41] Jattke P., Senker M., Wiesmaier A. MICKEY 2.0 & WG-8.
- [42] ISO/IEC 29192-3:2012. International standard for lightweight cryptographic methods, ISO/IEC, 2012.
- [43] Ding L., Jin C., Guan J. Slide attack on standard stream cipher Enocoro- 80 in the related-key chosen IV setting //Pervasive and Mobile Computing. – 2015. – T. 24. – C. 224-230.
- [44] Shibayama N., Igarashi Y. A New Higher Order Differential of Enocoro-128v2 //2021 Ninth International Symposium on Computing and Networking Workshops (CANDARW). – IEEE, 2021. – C. 379-384.
- [45] M Manifavas C. et al. A survey of lightweight stream ciphers for embedded systems //Security and Communication Networks. – 2016. – T. 9. – №. 10. – C. 1226-1246.
- [46] Z.T.Xudoykulov, I.R.Rahmatullayev, “Yangi oqimli shifrlash algoritmlari va uning kriptotahlili”, Milliy standart Ilmiy-texnik jurnali, 2023/2-son, 42-47 betlar.
- [47] I.R.Rahmatullayev, “Oqimli Shifrlash Algoritmlari”, Zamonaviy axborot texnologiyalari va ta’lim tizimini rivojlantirish istiqbollari, Xalqaro ilmiy- amaliy anjuman materiallar to’plami, Denov, 2023, 97-100 b.

EKSSENTRIK ROTATSION ISHQALAGICH YORDAMIDA ICHKI YONUV DVIGATELLARI DETALLARIGA ISHLOV BERISHNING KOMPYUTER DASTURI VA HISOBI

t.f.d. (DSc), dotsent A.I. XURRAMOV

Chirchiq Oliy tank qo'mondonlik muhandislik bilim yurti

Annotatsiya. Ushbu ilmiy maqolada ichki yonuv dvigatellari (IYoDi) detallarini ekstsentrik rotatsion ishqalagich yordamida silliqlash jarayoni kompyuter grafikasi vositasida o'rganilgan. "CATIA" va "NX" kabi muhandislik dasturlari yordamida ishqalagich va dvigatel detallarining 3D modellarini yaratish, ularning geometriyasini optimallashtirish hamda silliqlash samaradorligini baholash bo'yicha natijalar taqdim etilgan. Elastik tuklarning deformatsiyasi, kuchlanish holatlari va silliqlangan yuzalarning sirt sifati eksperimental va hisobiy usullar asosida tahlil qilinadi.

Kalit so'zlar: ichki yonuv dvigateli; ekstsentrik ishqalagich; rotatsion shyotka; 3D modelashtirish; kompyuter grafikasi; CATIA dasturi; NX muhiti; elastik tuklar; silliqlash samaradorligi; sirt sifati.

Аннотация. В данной научной статье рассматривается процесс шлифования деталей двигателей внутреннего сгорания (ДВС) с использованием эксцентриковой ротационной щетки на основе компьютерной графики. Приведены результаты моделирования 3D-геометрии щетки и деталей ДВС в инженерных программах «CATIA» и «NX», оптимизации конструкции и анализа эффективности шлифования. Деформации эластичных щетинок, напряжённые состояния и качество обработанных поверхностей оценены как экспериментально, так и расчётными методами.

Ключевые слова: двигатель внутреннего сгорания; эксцентриковый шлифовщик; ротационная щетка; 3D-моделирование; компьютерная графика; программа CATIA; среда NX; эластичные щетинки; эффективность шлифования; качество поверхности.

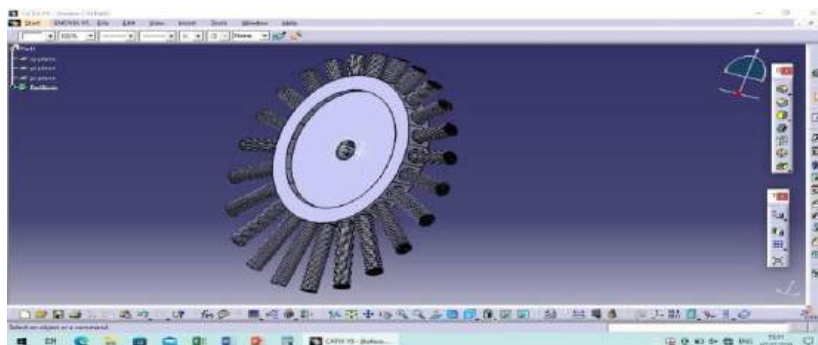
Abstract. This scientific article investigates the grinding process of internal combustion engine (ICE) components using an eccentric rotary brush, modeled through computer graphics. The study presents results of 3D modeling and geometric optimization of the brush and ICE components using engineering software such as CATIA and NX, as well as an evaluation of grinding efficiency. The deformation of elastic bristles, stress states, and the surface quality of the processed parts are analyzed using both experimental and computational approaches.

Keywords: internal combustion engine; eccentric grinder; rotary brush; 3D modeling; computer graphics; CATIA software; NX environment; elastic bristles; grinding efficiency.

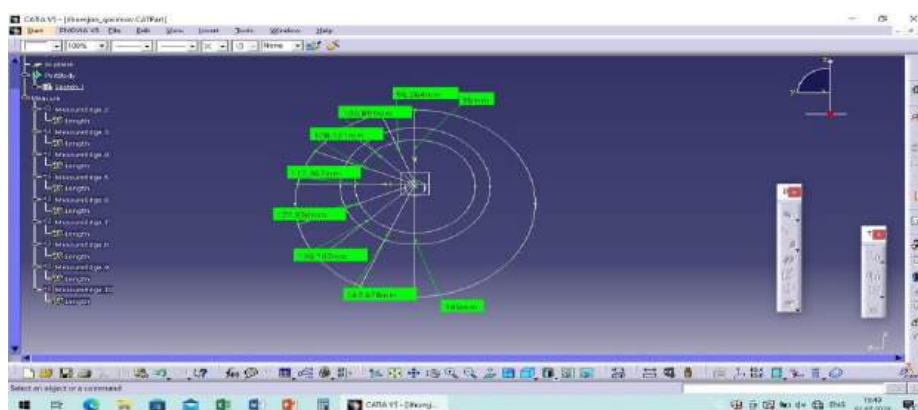
Tadqiqot predmeti bo'lgan ishqalagich detallari "CATIA" muhandislik grafikasi dasturida 3D formatda loyihalashtirildi. Loyihada ekstsentrikli rotatsion shyotkaning umumiy ko'rinishi, o'lchamli chizmasi, ekstsentrik valning 3D modeli va o'lchamlari, shuningdek, shyotka tuklarining uzunligi va radiusi bo'yicha o'zgaruvchan sxemalari ishlab chiqildi. 1 - 3- rasmlarda "CATIA", muhandislik grafikasi dasturida silliqlash uchun ekstsentrikli rotatsion ishqalagichning 3D tizimidagi chizmalari tasvirlangan.

"CATIA", muhandislik grafikasi dasturida silliqlash uchun ishqalagichning ekstsentrikli rotatsion shyotkasini 3D asosida ishqalagichning ekstsentrik valining ko'rinishidagi chizmasi, ishqalagich shyotkani elastik tuklarini o'zgaruvchan uzunlikdagi o'lchamlari hisoblanib ishlab chiqilgan.

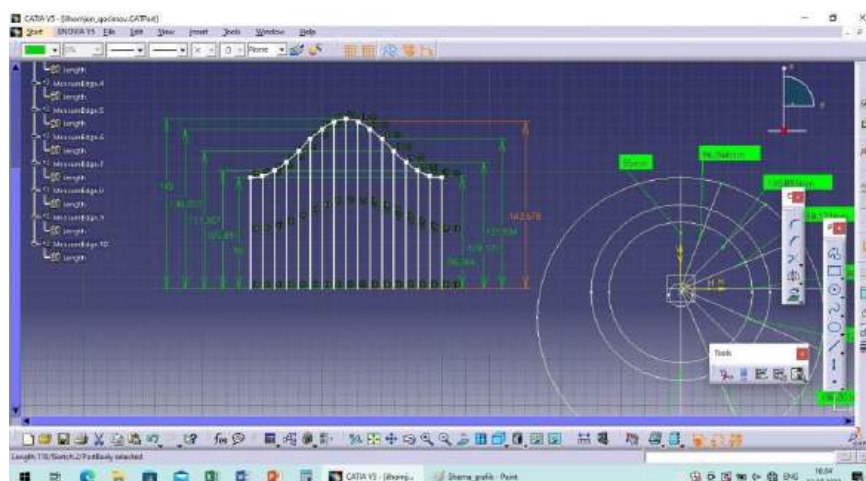
Kompyuterda tadqiqot predmeti detallarini 3D (uch ko'rinishi) "NX" muhandislik grafikasi dasturiy ta'minotida loyihalangan [1].



1- rasm. “CATIA”, muhandislik grafikasi dasturida silliqlash uchun ekstsentrikli rotatsion ishqalagichning 3D tizimidagi chizma



2- rasm. “CATIA”, muhandislik grafikasi dasturida silliqlash uchun ishqalagichning ekstsentrikli rotatsion shyotkasini 3D asosida o‘lchamlari qo‘yilgan ko‘rinishi chizma tasviri



3- rasm. “CATIA”, muhandislik grafikasi dasturida silliqlash uchun ishqalagichning ekstsentrikli rotatsion shyotkasini sterjen elastic tuk o‘lchamlari qo‘yilgan ko‘rinishi, ishqalagich shyotkani elastic tuklarini o‘zgaruvchan uzunlikdagi o‘lchamlarini sxema grafigi va tuklarni o‘zgaruvchan radiusli sxemalari hisoblanib ishlab chiqilgan

3- rasmda sterjen elastic tola uzunligining minimal va maksimal qiymatlariga mos keladigan, ekstsentrik ravishda qo‘yilgan R kuch bilan siqilgan ikkita tekis elastoplastik sterjen ko‘rsatilgan. Agar δ ekstsentriklik η ning ma’lum bir qiymatidan kam bo‘lsa (3- rasmga qarang), u holda ma’lum bir chegaraviy yuklanishda sterjen mustahkamligini yo‘qotadi. Agar $\delta > \eta$ (3- rasm.) yetarlicha

katta bo'lsa, mustahkamlik muammosi paydo bo'lmaydi. Belgilangan vazifalarni ajratib turadigan yuk $R \cdot (3\text{-rasm.})$ barqaror yuklash jarayonlarining yuklamasi deb atash mumkin.

Bu yerda eksentrisitet δ -tebranish, η esa uning chegarasi sifatida xizmat qiladi. Faqat $\delta < \eta$ bo'lganda tolaning uzunligi bo'ylab egilish jarayonining barqarorligi yoki beqarorligi haqida gapirish mumkin.

Elastik elementni uning barqarorligi bo'yicha hisoblash

Egiluvchan elastik tolaning doimiy ko'ndalang kesimi bo'ylab R kuch bilan siqilgan holatini ko'rib chiqaylik (3-rasm.) Tola o'qining boshlang'ich burilishini ω deb belgilaymiz. R kuchini qo'lanishi bilan sterjen darhol qisiladi. To'liq egilish bo'lsin, u holda tola o'qini egilishining o'zgarishi, dastlabki egirikni hisobga olgan holda quyidagicha bo'ladi:

$$X = (d^2\omega/dx^2) - (d^2\omega_0/dx^2) \quad (1)$$

Biz sterjenni pastki uchidan boshlab x masofagacha kesamiz va plastik tukning pastki kesilgan qismining muvozanatini ko'rib chiqamiz (3-rasmga qarang).

Muvozanat tenglamalari quyidagi shaklga ega:

$$\begin{aligned} N &= -R, & Q &= Q_0 = \text{const} \\ M &= M_0 + Q_0 x + P\omega \end{aligned} \quad (2)$$

bunda

R -aks tasir ettiruvchi kuch

N – umumiy kuch

Q_0 – ta'sir etuvchi kuch

M_0 - kesuvchi kuch ta'sirida vujudga keluvchi kuch moment (reaksiya-yani ichki ezuvchi moment). $N \cdot m$

P -birlik aylanish burchagi 1 teng bo'lganda yeyilish uchun energiya $\frac{Nmc}{rad}$

$$M = -EI[(d^2\omega/dx^2) - (d^2\omega_0/dx^2)] \quad (3)$$

(3) va (4) tenglamalar yordamida quyidagi formulani topamiz

$$EI[(d^2\omega/dx^2) + R\omega] = -M_0 - Q_0 x + EI(d^2\omega_0/dx^2)$$

X o'qi bo'yicha 2 marta differensiyalasak unda

$$\begin{aligned} EI(d^2\omega/dx^2) + P(d\omega/dx) &= -Q_0 + EI(d^2\omega_0/dx^2) \\ EI(d^2\omega/dx^2) + P(d\omega/dx) &= EI(d^2\omega_0/dx^2) \end{aligned}$$

Belgini kiritamiz

$$k^2 = P/EI$$

u holda bo'rtib chiqqan plastik tuklarning holat tenglamasini shaklda yozish mumkin.

$$(d^2\omega/dx^2) + k^2 (d\omega/dx) = (d^2\omega_0/dx^2)$$

Uning yechimi

$$\omega = C_1 \sin kx + C_2 \cos kx + C_3 x + C_4 + 1/k^2 \int (d^2\omega_0/dx^2) [\sin k(t-x) + \sin kt \cos kx + k(x-t)]$$

bunda k -fizik kattalik uning olchovi, $[k]=\text{rad/m}$;

x -masofa, metrlarda;

C_1, C_2, C_4 - birlik vaqt ichida siljish burchgi o'lchov biligi, rad/s;

C_3 – koefitsiyent birligi, radian/(s·m).

Valni silliqlash momentining kritik kuchga ta'sirini hisoblash.

Polimer materiallar uchun moment kritik kuchga sezilarli ta'sir ko'rsatishi mumkin. Sterjen o'zining ko'ndalang kesimida qisilganda kuch momenti quyidagicha topiladi:

O'R MV AKT VA ALOQA HARBIY INSTITUTI

$$M = P\omega + Q_0x + m_0 \quad (4)$$

Yuqoridagi tenglamadan korinadiki qo'shimcha ravishda kesish kuchi paydo bo'ladi(4- rasimga qarang).

$$\frac{dM}{dx} = Q_0 + Pd\omega/dx \quad (5)$$

Uning harakati tolalarning egilgan o'qining qo'shimcha γ -qiyaligiga olib keladi.

$$\gamma = d\omega/dx \quad (6)$$

Faraz qilaylik, ko'ndalang kesimda siljish kuchlanishlari bir tekis taqsimlangan. U holda

$$\gamma_{sr} = \tau_{sr}/G = Q/GF \quad (7)$$

Tangensial kuchlanishlarning notekis taqsimlanishi tufayli burchakning haqiqiy o'zgarishi biroz farq qiladi, shuning uchun (6) formulaga tuzatish koeffitsiyentini kiritamiz.

$$\gamma_{sr} = d\omega/dx = nQ/GF \quad (8)$$

Koeffitsient n , ko'ndalang kesmadagi yon kuchlanishlarining tasirini kamaytirish ularning yuza sirtidagi mikro notekisliklarni qirqib yuborish kuchi bilan tenglashtirish orqali aniqlanishi mumkin, ya'ni.

$$\int_0^X \left(\frac{\tau^2}{2G}\right) dF = 1/2 Q(Dw/dx) \quad (9)$$

yoki (7) dan foydalanib

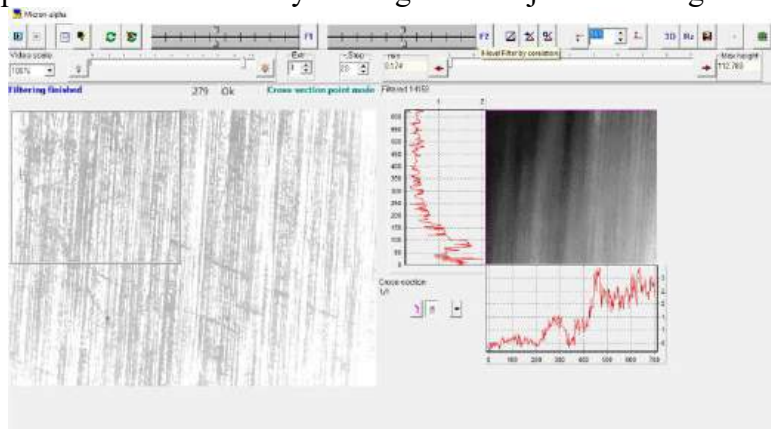
$$n = F/Q \int_0^X \tau^2 dF$$

Misol sifatida, to'rtburchaklar shaklidagi detalni kesimini ko'rib chiqamiz. Juravskiy formulasiga ko'ra, olamiz

$$\tau QS/hf = 3/2 Q (1/4 y^2/h^2)$$

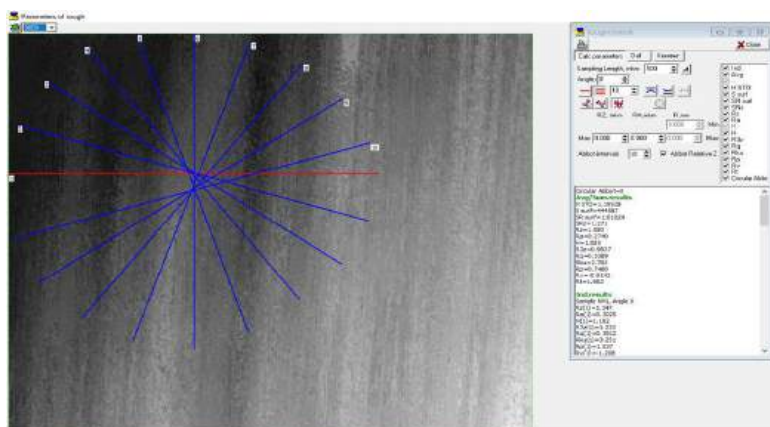
Bu qiymatini (5...65) ga almashtirib, integrallab, topamiz $n = 1,2$. Analogiya bo'yicha, dumaloq kesma uchun $n = 1,11$. Bu shuni anglatadiki, detallarni rotatsion aylanadigan shytka bilan silliqlashda shyotkaning asosiy parametrlari quyidagilar bo'lishi kerak [2-4].

Quyida (4 - 5- rasmlarga qarang) IYoDlari valsimon detallar materiallarining sirt g'adir-budirligini turli ekspluatasion ta'sirlar bo'yich o'zgarish natijalari keltirilgan.



4- rasm. Filtrlangan material yuzasi

3-rasmdagi grafikni filtrlash jarayoni ikkita protsedurani o'z ichiga oladi, birinchi filtrlash filtrlanmagan sirtlarning 50% ni olib tashlaydi va ikkinchi filtrlash butunlay filtrlanmagan sirtlarni olib tashlaydi va sirt gadir-budirligini tahlil qilish uchun faqat filtrlanadigan sirt qoladi.



5- rasm. Nuqtalarni tahlil qilish

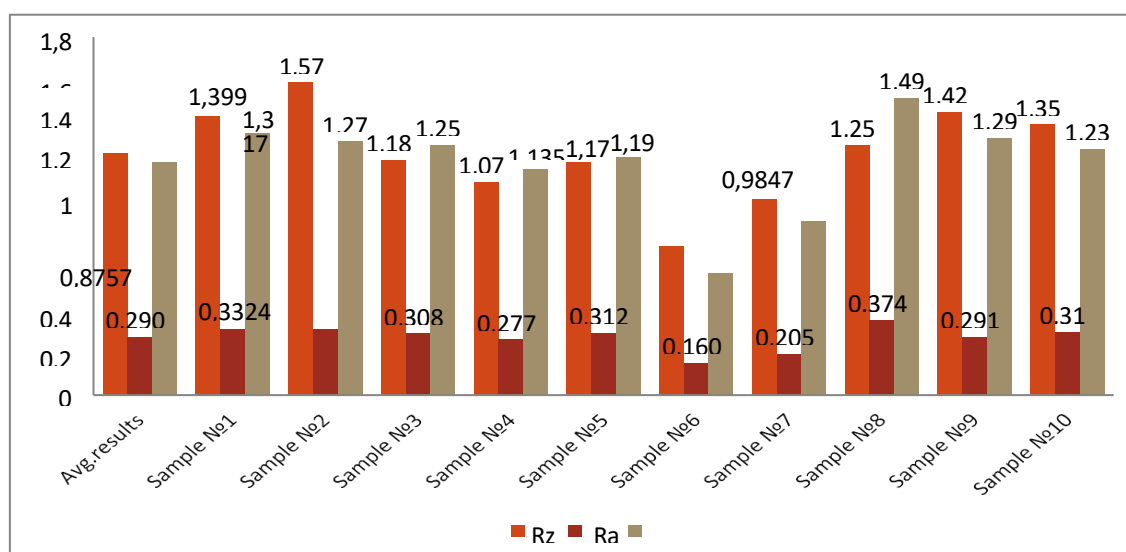
Ushbu tajribada biz turli sirt zonalaridan materialning sirt g'adir-budirligini farqini topish uchun 10 ta nuqtani tanladik. Material yuzasida boshqa o'n xil nuqtalar bilan birga sirt g'adir-budirligini o'rtacha qiymatini topdik. Quyida 1- jadval yordamida tajriba natijalarini tahlil qildik.

1-jadval

Materiallar sirtining parametrlarining eksperimental tahlil natijalari

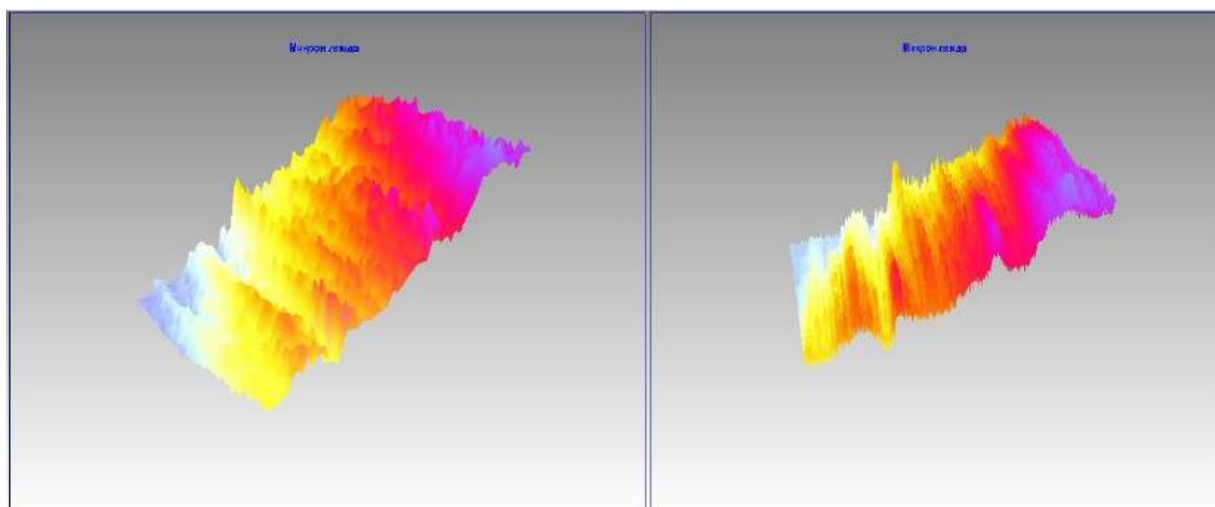
Results	Rz	Ra	H	R3z	Rq	Rku	Rp	Rv	Rt
Avg.results	1.216	0.2903	1.169	1.138	0.3622	2.931	0.9240	0.9547	1.878
Sample №1	1.399	0.3324	1.317	1.1376	0.4281	3.774	1.186	1.311	1.311
Sample №2	1.570	0.3284	1.275	1.685	0.4270	3.820	1.147	1.574	1.574
Sample №3	1.182	0.3082	1.257	1.134	0.3755	2.494	0.8121	0.8748	0.8748
Sample №4	1.072	0.2779	1.135	0.9429	0.3484	2.808	0.7263	0.8936	0.8936
Sample №5	1.170	0.3122	1.196	1.112	0.3662	2.199	0.7849	0.7893	0.7893
Sample №6	0.7500	0.1603	0.6139	0.6857	0.1900	2.581	0.5008	0.5168	0.5168
Sample №7	0.9847	0.2054	0.8757	0.9047	0.2525	2.677	0.6911	0.5941	0.5941
Sample №8	1.255	0.3745	1.492	0.9298	0.4667	2.642	1.086	0.9044	0.9044
Sample №9	1.422	0.2913	1.292	1.439	0.3643	2.763	1.044	0.7457	0.7457
Sample №10	1.359	0.3150	1.238	1.173	0.4032	3.556	1.260	1.343	1.343

Materiallar sirtining parametrlarining eksperimental tahlil natijalari diagrammasi 6- rasmda keltirildi.



6- rasm. Materiallar sirtining parametrlarining eksperimental tahlil natijalari diagrammasi

Aniqroq natijalarga erishish uchun bir xil material yuzasida bir nechta tajriba o'tkazdik, bundan tashqari, turli o'lchamdagi material yuzasining turli qismlariga e'tibor qaratdik. Quyida eksperimental natijalarni jadval va raqamlar bilan ko'rsatamiz.



7- rasm. Material yuzasining 3D vizual formatining 4x va 8x ko'rinishi

7-rasmda IYoDlari valsimon detallar materiallarining sirt g'adir-budiriligini turli ekspluatasion ta'sirlar bo'yich materialining 3D vizual formatining 4x va 8x ko'rinishi olingan va ularni optimal miqdorlari aniqlangan [5, 6].

Xulosa qilib aytganda, ichki yonuv dvigateli detallarini ekstsentrik rotatsion ishqalagich yordamida silliqlash jarayonini raqamli muhandislik vositalari orqali modellashtirish, ushbu texnologiyaning samaradorligini baholashda muhim ahamiyat kasb etadi. Tadqiqot natijalari shuni ko'rsatdiki, ishqalagichning geometrik parametrlari va elastik tuklarning fizik xossalarini optimallashtirish silliqlash jarayonining sirt sifati va ish unumdorligiga bevosita ta'sir ko'rsatadi. Kompyuter grafikasi asosidagi 3D modellashtirish esa real eksperimentlarga bo'lgan ehtiyojni kamaytirib, vaqt va resurs tejamkorligini ta'minlaydi. Mazkur usul IYoD detallarini qayta ishlashda samarali va innovatsion yechim sifatida tavsiya etiladi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

- [1] Мелисаров М. Практикум по конструкции тракторов и автомобилей. Учебное пособие. Ч. 2. -Тамбов: Тамб. гос. техн. ун-т, 2003. -128 стр.
- [2] Иванов В.П., Ярошевич В.П., Иванов В.К. и др. Ремонт автомобилей. Учебное пособие. -Минск: Высшая школа, 2009. - 383 стр.
- [3] Тимохин С. В., Родионов Ю. В. Современные технологии обкатки автотракторных двигателей. Монография. 2013. -104 стр.
- [4] Полюшкин Н. Г. Основы теории трения, износа и смазки. – 2013. -180 стр.
- [5] Т.С.Худойбердиев, К.З.Қосимов. Машина деталлари ресурсини оширишнинг илмий асослари". Монография. – Андижон, 2020. – 165 бет.
- [6] Нуриев К.К., Ўзароалшинувчанлик, метрология ва стандартлаштириш. Дарслик. - Тошкент: Фан, - 2005.-312 бет.

UKRAINA QUROLLI KUCHLARIDA ZAMONAVIY RADIOELEKTRON KURASH VOSITALARI

dotsent X.U. YAKUBOV

O'R MV Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti

Annotatsiya. Ukraina Qurolli Kuchlarida radioelektron kurash zamonaviy harbiy strategiyaning muhim elementi, ayniqsa yuqori texnologiyali dushman bilan urush sharoitida. Radioelektron kurash tizimlaridan foydalanish dushman aloqalarini, navigatsiya va razvedka tizimlarini samarali bostirish, axborot ustunligini ta'minlash va Ukraina qurolli kuchlarining jangovar samaradorligini oshirish imkonini beradi.

Kalit so'zlar: Radioelektron kurash, bostirish, mobil aloqa, jangovar harakatlar, masofa, radio razvedka, aniqlash, boshqarish, vositalar.

Аннотация. РЭБ в ВСУ является важным элементом современной военной стратегии, особенно в условиях войны с высокотехнологичным противником. Использование средств РЭБ позволяет эффективно подавлять вражеские средства связи, навигации и разведки, обеспечивая информационное превосходство и повышая боевую эффективность украинских вооружённых сил.

Ключевые слова: Радиоэлектронная борьба, подавления, мобильной связи, боевой действия, диапазон, радиоразведка, обнаружения, управления, средства.

Ukraina Qurolli Kuchlarining radioelektron kurash (REK) so'nggi yillarda, ayniqsa Rossiya bilan urush sharoitida muhim rol o'ynadi, bu erda REKdan foydalanish taktik operatsiyalarning ajralmas qismiga aylandi. Ukraina Qurolli Kuchlari dushman aloqalari va navigatsiyasini bostirish, o'z kuchlarini himoya qilish va razvedka o'tkazish kabi turli vazifalarni bajarish uchun zamonaviy radioelektron kurash tizimlarini faol ravishda rivojlantiradi va ishlatadi. Yuqori texnologiyali dushman bilan urush sharoitida Ukraina Qurolli Kuchlarining radioelektron kurash axborot urushining bir xil darajada muhim qismiga aylandi, bu erda radiochastotalardan foydalanish hal qiluvchi rol o'ynashi mumkin [1].

Ukraina Qurolli Kuchlari turli maqsadlarda ishlatiladigan mobil radioelektron kurash tizimlarining bir nechta turlaridan foydalanadi:

“Pelena” majmuasi

“Pelena” majmuasi - bu uyali aloqani bosim berish va radiochastota diapazonlarida shovqin yaratish uchun mo'ljallangan Ukraina radioelektron kurash tizimi. Bu dushman aloqa tizimlarining ta'siridan himoya qilish va jang maydonida elektron xavfsizlikni ta'minlash uchun faol foydalaniladigan eng mashhur Ukraina tizimlaridan biridir.

“Pelena” kompleksining asosiy xususiyatlari va imkoniyatlari:

Mobil aloqa tiqilib qolishi:

Mobil tarmoqlar aksariyat zamonaviy armiyalar uchun asosiy aloqa kanali bo'lib, “Pelena” uyali aloqa tarmoqlarini buzish uchun ishlatiladi, bu esa dushman kuchlariga ularni muvofiqlashtirish va nazorat qilishni qiyinlashtiradi.

Tizim mobil telefonlar, tayanch stansiyalar va mobil chastotalardan foydalangan holda boshqa aloqa qurilmalarining ishlashini samarali ravishda buzadi.

Keng tasir doirasida:

Kompleks keng chastota diapazonida shovqin yaratishi mumkin, bu esa ish radiusidagi aloqalarni bostirish imkonini beradi.

Bu nafaqat mobil qurilmalar bilan aloqani zararsizlantirish, balki turli darajadagi radio va aloqa vositalarining ishlashini buzishda ham yordam beradi.

Turli chastota diapazonlarini bosim berish:

“Pelena” turli avlod mobil tarmoqlariga (masalan, 2G, 3G, 4G) ta'sir o'tkazish qobiliyati bilan jihozlangan, bu eski va yangi aloqa texnologiyalarini bosim berish imkonini beradi.

Turli chastota diapazonlaridan foydalanish tizimga dushmanning aloqa infratuzilmasining xususiyatlarini hisobga olgan holda turli jangovar sharoitlarda ishlash imkonini beradi.

Mobillik va teskorlik:

“Pelena” mobil dizaynga ega, bu tizimni tezda jang maydoniga ko‘chirish va aloqa uchuni buzish uchun zarur bo‘lgan zarur nuqtalarda foydalanish imkonini beradi.

Bu harakatchanlik Ukraina qo‘shinlariga o‘zgaruvchan vaziyatlarga tezda javob berishga va dushmanga qarshi himoya qilish uchun radioelektron kurashdan samarali foydalanishga imkon beradi.

Turli urush teatrlarida foydalaning:

“Pelena” tizimi jangovar harakatlarda Ukraina hududidagi ham, boshqa to‘qnashuvlarda ham, dushman o‘z harakatlarini muvofiqlashtirish uchun mobil aloqadan foydalanishida samarali qo‘llaniladi.

Majmua dushman tomonidan bosib olingan hududda nafaqat harbiy, balki fuqarolik aloqalarini ham bosim berish uchun faol foydalanilmoqda.

Raqiblardan foydalanish:

Urush paytida, aloqa qo‘mondonlik va boshqaruvning muhim elementi bo‘lganida, ularni “Pelena” kabi tizimlar bilan bog‘lash dushman bo‘linmalarining tartibsizlanishiga olib kelishi, buyruqlarni uzatishni qiyinlashtirishi va qo‘mondonlikni chalg‘itishi mumkin.

“Pelena” tizimining afzalliklari:

Kam shovqin: tizim dushman aloqalariga xalaqit bersa-da, u o‘z aloqalariga ta‘sirini minimallashtirishga harakat qiladi, bu esa undan foydalanishning muhim elementidir.

Texnologik moslashuv: “Pelena” turli xil sharoit va tahdidlarga moslashishga qodir, bu unga jangovar vaziyatlarni o‘zgartirishda ustunlik beradi.

Oson va samarali foydalanish: harakatchanligi va turli xil aloqa turlarini bostirish qobiliyati tufayli “Pelena” zamonaviy jangovar teatrlarda foydalanish uchun universal tizimdir.

“Pelena” radioelektron kurash tizimi Ukraina mudofaa strategiyasining muhim elementi hisoblanadi. Mobil aloqaniga bosim berishishi va radiochastotalarning keng diapazonida shovqinlarni yaratish qobiliyati tufayli tizim Ukraina Qurolli Kuchlarining dushmanning yuqori texnologiyali aloqa vositalariga qarshi kurashish qobiliyatini sezilarli darajada oshiradi, qo‘mondonlik va boshqaruvni buzadi [2].



1-rasm. “Pelena” majmuasining ko‘rinish

“Pelena” kompleksi Rossiya-Ukraina urushida qo‘llanilishi bo‘yicha misollar

Severodonesk hududida radiolokatsiya tizimlarini bloklash

2022 yilda Severodonesk yaqinida “Pelena” kompleksi rus radarlari va radioaloqalarini samarali bloklab, Ukrain qo‘shinlarining harakatlarini yashirin tarzda amalga oshirishga imkoniyat bergan.

Janubiy frontda – Xerson va Zaporozhe

Ushbu hududlarda rus qo‘shinlarining radiolokatsiya va radio aloqa vositalarini buzish maqsadida “Pelena” tizimi faol qo‘llanilgan. Bu rus kuchlarining boshqaruvini cheklagan.

Rossiya dronlarini va radar tizimlarini nobud qilish

2022 yil mart oyi, Xarkov atrofida

Rossiya kuchlari Xarkov hududida ilk qo'lga kiritilgan tezkor razvedka ma'lumotlariga asosan jadal harakat qilayotgan paytda, ukrain dronlari faol foydalanilgan. "Pelena" kompleksi rus dronlarining radio signallarini buzish orqali ularning navigatsiyasini yo'qotishga va nazoratdan chiqishga olib kelgan. Bu Ukrain jangchilariga tez harakat qilish va rus kuchlarini chalg'itish imkonini bergan.

Mariupol shahri hujumlari davrida (2022 yil bahori)

Mariupolga bosqinchilik qilgan Ukrain kuchlari Rossiya tarafdan jo'natilgan razvedka dronlariga qarshi "Pelena" REB tizimidan foydalangan. Kompleks orqali dronlar radio aloqasi buzilib, ularning aniq joylashuvini aniqlash va zarba berish imkoniyati sezilarli darajada pasaygan.

2023 yilgi janglar, Donesk atrofida

Donesk viloyatidagi ko'p qatnovli janglarda "Pelena" tizimi rus armiyasining radarlari va boshqaruv signallariga qarshi tezkor radioelektron hujumlar amalga oshirgan.

Bu dushmanning artilleriya boshqaruvini buzish va zarbalarni kamaytirishga xizmat qilgan.

Aviatsiya uchun qo'llanilishi (2022-2023 yillar)

Ukrain harbiy aviatsiyasi uchun jangovar qo'llanilayotgan "Pelena" REB kompleksi dushman radarlarini aniqlash va bloklashda muhim rol o'ynagan. Bu uchuvchilarga yashirin harakat qilish va ziddiyatli hududlarda xavfsiz uchish imkoniyatini yaratgan.

"Pelena" orqali rus dronlari bilan boshqaruv va razvedka signallari buzib yuborilgan.

Bu, ayniqsa, kichik va taktik dronlarga qarshi kurashda muhim bo'lgan.

Harbiy bazalar va kommunikatsiya markazlarini himoya qilish

Ukrainaning muhim harbiy ob'ektlariga qarshi radioelektron hujumlardan himoya uchun "Pelena" tizimi ishlatilgan. Bu ob'ektlar hujum va razvedkadan barqaror himoyalangan.

Rossiya-Ukraina chegarasida operativ radioelektron kurash

Chegara hududida "Pelena" tizimi tezkorlik bilan dushman signallarini aniqlash va bloklash orqali harbiy harakatlarning muvaffaqiyatli bo'lishiga ko'maklashgan [3].

"Levada" tizimi

"Levada" - bu GPS va GLONASS kabi sun'iy yo'ldosh navigatsiya tizimlarini bostirish uchun mo'ljallangan Ukraina radioelektron kurash tizimi. Ushbu tizim Ukraina Qurolli Kuchlari mudofaa strategiyasining muhim elementi bo'lib, qurol-yarog', razvedka aktivlari va qo'shinlar harakatini nazorat qilish uchun sun'iy yo'ldosh navigatsiyasidan foydalanadigan yuqori texnologiyali dushman qurollariga qarshi kurashishga qaratilgan.

"Levada" tizimining asosiy xususiyatlari va imkoniyatlari:

"Levada" tizimi sun'iy yo'ldosh navigatsiya tizimlari, birinchi navbatda GPS (AQSh) va GLONASS (Rossiya) ishlashiga xalaqit berish uchun ishlab chiqilgan. Bular jang maydonida navigatsiya qilish, ayniqsa, aniq qurollar, uchuvchisiz uchish apparatlari (UUA), shuningdek, yerdagi transport vositalari va samolyotlarning navigatsiyasi uchun muhim tizimlardir.

"Levada" GPS va GLONASS signallarini tiqilib qolishi yoki taqlid qilishi, ularning ishlashiga xalaqit berishi mumkin. Bu aniq sun'iy yo'ldosh navigatsiyasiga tayanadigan asboblardan foydalanishni qiyinlashtiradi.

Effektlarning keng doirasi:

Tizim turli chastotalar va diapazonlardagi sun'iy yo'ldosh signallariga ta'sir ko'rsatishga qodir, bu unga sun'iy yo'ldosh navigatsiya tizimlarining har xil turlari, jumladan, aniq zarbalar va jangovar harakatlar uchun ishlatiladigan tizimlar bilan samarali ishlash imkonini beradi.

Bu ta'sir tiqilib qolish (signallarni to'liq blokirovka qilish) yoki noto'g'ri signallarni yaratish (dushman navigatsiya tizimlarini chalkashtirib yuborishi mumkin) bo'lishi mumkin.

UUA va aniq qurollar uchun qarshi bosim berish:

"Levada" tizimining asosiy maqsadlaridan biri navigatsiya va olovni yo'naltirish uchun GPS ishlatadigan UUALarning ishini bostirishdir. Bu dronlarni boshqarishni qiyinlashtirishi va

sun'iy yo'ldosh navigatsiya tizimlariga tayanadigan aniq qurollarning aniqligini kamaytirishi mumkin.

Bu ayniqsa dushman Ukraina pozitsiyalari va infratuzilmalariga zarba berish uchun uchuvchisiz uchish tizimlar va yuqori aniqlikdagi raketalardan faol foydalanayotgan sharoitda muhim ahamiyatga ega.

Yuqori aniqlikka ega qurollarga qarshi foydalanish:

Zamonaviy aniqlikka ega qurollar (masalan, qanotli raketalar va boshqariladigan bombalar) aniq yo'naltirish uchun GPSdan foydalanadi. "Levada" yordamida GPS signallarini to'sib qo'yish ushbu qurollarning samaradorligini sezilarli darajada pasaytiradi, ularni yo'ldan chetga surib qo'yishi yoki nishonga aniq zarba bera olmasligiga olib kelishi mumkin.

Mobillik va teskorlik:

"Levada" tizimi mobil yechim bo'lib, uni turli jangovar zonalarga tezda ko'chirish imkonini beradi. Bu Ukraina qo'shinlariga o'zgaruvchan sharoit va tahdidlarga javob berish uchun moslashuvchanlikni beradi.

Mobillik shuningdek, tizimni o'zgaruvchan taktik vaziyatlarga va dushman nishonlariga moslashishga imkon beradi, bu esa undan jang maydonida maksimal darajada foydalanish imkonini beradi.

Gibrid urushda samaradorligi:

Gibrid urush sharoitida nafaqat an'anaviy qurollar, balki kiberhujumlar, axborot texnologiyalari va radioelektron kurashlar ham qo'llaniladi, "Levada" tizimi dushman zarbalarining aniqligi va muvofiqlashtirilishini buzishda, Ukrainaning strategik tashabbusini qo'llab-quvvatlashda muhim rol o'ynaydi.

Levada tizimining afzalliklari:

Aniqlik va samaradorlik:

"Levada" tizimi sun'iy yo'ldosh navigatsiya tizimlarini bostirishda yuqori aniqlikni ta'minlaydi, bu uni navigatsiya uchun GPS va GLONASS ishlatadigan tizimlarga nisbatan ayniqsa samarali qiladi.

Boshqa radioelektron kurash tizimlari bilan integratsiya:

"Levada" boshqa radioelektron kurash tizimlari va artilleriya tizimlari bilan birgalikda qo'shnlarni uchuvchisiz uchish vositalari, aniq qurollar va razvedka tizimlari kabi dushman texnologiyalaridan har tomonlama himoya qilish uchun ishlatilishi mumkin.

Ko'p qirraligi:

Tizim jangovar sharoitlarda ham, tinchlik davrida ham ishlay oladi, razvedka yoki navigatsiya uchun sun'iy yo'ldosh tizimlaridan ruxsatsiz foydalanishdan himoya qiladi.

Mobillik va foydalanish tezligi:

Jang maydoni bo'ylab osongina olib o'tiladi gan tizim o'zgaruvchan taktik vaziyatlarga tezda moslasha oladi, dinamik jangovar sharoitlarda samaradorligini oshiradi.

"Levada" ni zamonaviy sharoitda qo'llash:

Ukrainadagi urush sharoitida, yuqori aniqlikdagi qurollar va UUAlar faol qo'llanilganda, "Levada" tizimi dushmanning navigatsiya tizimlarini buzishda hal qiluvchi rol o'ynaydi.

Sun'iy yo'ldosh navigatsiya tizimlari Ukraina qurolli kuchlariga aniq qurollar va dronlardan foydalangan holda aniq zarbalardan qochish, shuningdek, havo va raketa hujumlari samaradorligini kamaytirish imkonini beradi.

Bu, ayniqsa, Rossiya va boshqa dushmanlar o'zlarining harbiy aktivlarini boshqarish va jangovar harakatlarni amalga oshirish uchun GPS va GLONASS tizimlaridan foydalanishlari nuqtai nazaridan juda muhimdir.

"Levada" tizimi dushmanning sun'iy yo'ldosh navigatsiya texnologiyalaridan foydalanishga qarshi kurashning samarali vositasidir. GPS va GLONASS-ni blokirovka qilish qobiliyati aniq zarbalar, dronlar va raketalarning samaradorligini sezilarli darajada pasaytiradi, bu Ukraina Qurolli Kuchlariga zamonaviy janglarda muhim ustunlik beradi. Ushbu radioelektron kurash tizimi Ukrainaga dushmanning sun'iy yo'ldosh navigatsiya tizimlariga

yuqori texnologik qaramligi bilan bog‘liq tahdidlardan o‘zini himoya qilishga yordam beradi [3].



2-rasm. “Levada” tizimini jangovar qo‘llash

“Levada” kompleksi jangovar qo‘llanilishi bo‘yicha misollar

Xarkov va atrofida dronlarni bloklash

2022 yil bahorida Xarkov yaqinidagi hujumlar paytida “Levada” tizimi rus razvedka va hujumchi dronlarining radio kanallarini bloklab, ularning shu yerdagi razvedka va artilleriyani muvofiqlashtirish funksiyalarini muvaffaqiyatli buzgan.

Janubiy frontda – Xerson va Zaporozhe atrofida

Ushbu hududlarda Ukraina kuchlari “Levada”ni faol qo‘llab, rus UUA larining samaradorligini sezilarli darajada kamaytirgan. Bu frontdagi Ukraina pozitsiyalariga dronlar orqali bajarilayotgan razvedka va zarbalar kamayishiga sabab bo‘lgan.

Severodonesk va Lisichansk yaqinida

2022 yilda bu hududlarda Rossiya qo‘shinlari ko‘plab razvedka dronlaridan foydalangan. Ukraina tomonidan “Levada” tizimi orqali ushbu dronlarning radio signallari bloklangan, natijada ularning razvedka faoliyati sezilarli darajada pasaygan.

Mariupol atrofida dronlar bilan kurashish

Mariupoldagi ko‘pmarotabali janglar paytida rus dronlari faol qo‘llanilgan. “Levada” orqali ularning GPS va boshqaruv kanallari buzilgan, bu esa dushman dronlarining samaradorligini kamaytirgan.

Kommunikatsiya liniyalarini himoyalash

Rossiya tomonidan radiobog‘lanish vositalarini buzishga qaratilgan harakatlarning oldini olish uchun “Levada” Ukrain qo‘shinlari kommunikatsiya liniyalari yaqinida qo‘llangan. Bu holatlarda tizim dushmanning radio signallariga aralashish orqali ularning boshqaruv qobiliyatini pasaytirgan.

UUAlarni yo‘ldan chiqarish

Turli malaka darajasidagi janglarda, jumladan kichik taktik amaliyotlarda, “Levada” kichik dronlar bilan samarali kurashgan. Bu front bo‘yicha razvedka va xavfsizlikni oshirishga yordam bergan [6].

“Kolchuga” tizimi

“Kolchuga” - uzoq masofalardagi havo nishonlarini aniqlash va kuzatish uchun ishlatiladigan Ukraina radiolokasion razvedka (RLR) tizimi. Bu Ukraina Qurolli Kuchlari tizimida havo bo‘shlig‘i kengligini radar monitoringi, dushmanning radar va elektron jihozlaridan foydalanish sohasidagi kontrrazvedka uchun eng samarali vositalardan biridir.

Kolchuga tizimining asosiy xususiyatlari va imkoniyatlari:

Radiolokasion razvedka:

“Kolchuga” havo ob‘ektlarini - samolyotlar, vertolyotlar, uchuvchisiz uchish apparatlari (UUA) va boshqa uchish vositalarini aniqlash va kuzatish uchun mo‘ljallangan. Tizim faol radiolokasion bosim berishi va radioelektron kurash tizimining bir qismi bo‘lishi mumkin.

“Kolchuga” nafaqat nishonlarni aniqlaydi, balki ularning tezligi, balandligi va parvoz yo‘li kabi xususiyatlariga oid ma’lumotlarga asoslanib, ularni aniqlash va tasniflashda yordam beradi.

Uzoq masofalarda ishlashi:

“Kolchuga”ning asosiy afzalliklaridan biri bu uzoq masofalarda - 800 km gacha bo‘lgan havo nishonlarini aniqlash qobiliyatidir. Bu unga potentsial tahdid haqida qo‘mondonlikni tezda xabardor qilish imkonini beradi, bu esa qarshi choralar ko‘rish imkoniyatini beradi.

Ushbu diapazon tizimni keng hududlarni kuzatish uchun foydali hisoblanadi, bu ayniqsa jangovar vaziyatlarda muhimdir.

Ko‘p kanalli va aniqligi:

“Kolchuga” keng chastota diapazonida ishlaydi, bu bir vaqtning o‘zida bir nechta nishonlarni kuzatish va radio shovqinlarining ta’sirini kamaytirish imkonini beradi.

U nishon koordinatalarini aniqlashda yuqori aniqlikka ega, bu olov yo‘nalishini va havo hujimidan mudofaa va aviatsiya vositalaridan samarali foydalanish uchun juda muhimdir.

Yashirin nishonlarni aniqlash:

Bu tizim oddiy radarlar bilan aniqlash qiyin bo‘lishi mumkin bo‘lgan dron kabi kichik nishonlarni samarali aniqlay oladi.

“Kolchuga” nafaqat samolyot kabi katta ob’ektlarni, balki kichikroq nishonlarni ham kuzatish uchun ishlatiladi, bu uni turli xil razvedka vazifalarini hal qilish uchun universal qiladi.

Havo hujimidan mudofaasi tizimidagi roli:

Havo hujimidan mudofaa tizimlari bilan birgalikda “Kolchuga” havo bo‘shlig‘ini himoya qilish samaradorligini sezilarli darajada oshiradi. Bu dushman samolyotlarini, raketalarini yoki dronlarini o‘z vaqtida aniqlashga yordam beradi, ularni yo‘q qilish uchun havo hujimidan mudofaa tizimlari yoki aviatsiyadan foydalanish to‘g‘risida qaror qabul qilish uchun ma’lumot beradi.

“Kolchuga” boshqa radar va radioelektron kurash tizimlari bilan ham birlashtirilishi mumkin, bu havo tahdidlaridan ko‘p qatlamli himoya yaratadi.

Radioelektron kurash sharoitida ishlash:

“Kolchuga” ham kuchli radio bosim sharoitida ishlash qobiliyatiga ega. Bu shuni anglatadiki, tizim dushman radioelektron kurash tizimlaridan faol qarshilik ko‘rsatish sharoitida ishlashi mumkin, radio shovqinlari va elektron hujumlar strategiyaning muhim qismi bo‘lgan zamonaviy gibril urushlar sharoitida uni ajralmas holga keltiradi.

Mobillik:

“Kolchuga” mobil dizaynga ega, bu uni turli jangovar hududlarda tezda joylashtirish imkonini beradi. Bu tizimni moslashuvchan qiladi va o‘zgaruvchan sharoit va tahdidlarga moslasha oladi.

Harakatchanlik tizimga ham oldinga qirrada, ham xavfsizroq orqa zonalarda ishlashiga imkon beradi, bu esa havo bo‘shlig‘ining kechayu-kunduzi monitoringini ta’minlaydi.

“Kolchuga” tizimining afzalliklari:

Uzoq masofani aniqlash diapazoni: uzoq masofalardagi nishonlarni, shu jumladan dron kabi kichik va o‘rta o‘lchamli ob’ektlarni aniqlash qobiliyati uni zamonaviy urushlar kontekstida kuchli vositaga aylantiradi.

Radioelektron shovqinlarga qarshiligi: “Kolchuga” dushman tomonidan faol radio bosim berish sharoitida ishlashga qodir, bu radioelektron kurashdan foydalanish muhim tarkibiy qism bo‘lgan zamonaviy jangovar operatsiyalarda samaradorligini oshiradi.

Boshqa tizimlar bilan integratsiya:

Tizim boshqa radar tizimlari bilan, shuningdek, havo tahdidlariga javoban harakatlarni muvofiqlashtirishni yaxshilash uchun havo hujimidan mudofaa tizimlari bilan birlashtirilishi mumkin.

Bundan tashqari, u keyingi qayta ishlash va qaror qabul qilish uchun maqsadli ma'lumotlarni tezkor uzatish imkonini beruvchi olovni yo'naltirish nazorat qilish tizimlari bilan bog'lanishi mumkin.

Mobillik va teskorlik:

Tizimning harakatchanligi unga o'zgaruvchan taktik vaziyatlarga tez moslashish, shuningdek, o'z manzilini dushmanidan yashirish imkonini beradi.

Murakkablik va ko'p vazifalar:

Tizim nafaqat aniqlash, balki havodagi ob'ektlarni aniqlashni ham ta'minlaydi, bu uni havo razvedkasidan tortib jangovar boshqaruvgacha bo'lgan turli maqsadlar uchun foydali qiladi.

“Kolchuga” tizimini qo'llash:

Dronlarga qarshi kurash:

Uchuvchisiz uchish apparatlari razvedka va zarba berishning asosiy vositasiga aylanib borayotgan zamonaviy urush sharoitida “Kolchuga” tizimi uzoq masofalarda dronlarni samarali aniqlaydi, bu esa qarshi choralarni ko'rishga imkon beradi (masalan, tahdidni yo'q qilish uchun havo hujumidan mudofaa tizimlari yoki UUALarni yuborish).

Havo bo'shlig'ini nazorat:

“Kolchuga”ning muhim vazifasi - dushman aviatsiyasi tahdidlarini o'z vaqtida aniqlash va o'z havo operatsiyalarini himoya qilishni ta'minlash uchun havo bo'shlig'ini kuzatish.

Havo hujumidan mudofaa va aviatsiya tizimlarini qo'llab-quvvatlash:

Tizim havo hujumiga qarshi mudofaa tizimlarini ma'lumotlar bilan ta'minlash, shuningdek, havo zarbalarini sozlash, hujumlarning aniqligi va samaradorligini ta'minlash uchun ishlatiladi.

Radioelektron kurash sharoitida foydalanish:

Dushmanning faol radioelektron kurashi sharoitida “Kolchuga” nishonlarni aniqlashga va jangovar harakatlarni muvaffaqiyatli hal qiluvchi rol o'ynashi mumkin bo'lgan qarshi choralar uchun ma'lumotlarni uzatishga yordam beradi.

“Kolchuga” tizimi radiolokasion razvedka va havo bo'shlig'ini himoya qilishda muhim element hisoblanadi. Uning uzoq masofasi, REK muhitida ishlash qobiliyati va harakatchanligi uni Ukraina qurolli kuchlari uchun havo tahdidlarini o'z vaqtida aniqlash va kuzatishni ta'minlaydigan samarali vositaga aylantiradi. Bu tizim nafaqat havo hujumlaridan himoya qiladi, balki boshqa vositalar bilan integratsiyalashib, havo tahdidlariga qarshi ko'p qatlamli mudofaani yaratadi [4].



3-rasm. “Kolchuga” tizimi

“Kolchuga” kompleksi jangovar qo'llanilishi bo'yicha misollar

Donesk va Lugansk viloyati (2014–2015 yillar)

“Kolchuga” tizimi ushbu janglarda rus harbiy texnikasini, jumladan samolyotlar va vertolyotlarni aniqlash va ularning harakatini kuzatish uchun faol ishlatilgan;

Bu ma'lumotlar asosida Ukrain qo'shinlari dushman havo hujumlariga qarshi tayyorgarlik ko'rgan va o'z harakatlarini rejalashtirgan.

Mariupol hududi (2022 yil)

Ukraina tomonidan boshqarilgan “Kolchuga” tizimi rus tarafidan boshqarilayotgan radarlar va dronlarni aniqlashda muhim rol o‘ynagan.

Bu Ukraina artilleriyasi va REB tizimlariga dushman ob’ektlariga samarali zarba berish uchun tezkor razvedka ma’lumotlari taqdim etgan.

Xarkov yo‘nalishi (2022 yil bahori)

“Kolchuga” orqali rus havo texnikalari, xususan razvedka dronlari va samolyotlari aniqlangan va ularning harakatlari kuzatilgan.

Bu Ukrain qo‘shinlariga dushman harakatlarini oldindan bilish va tezkor javob berish imkonini bergan.

Severskiy Donesk va Lisichansk yaqini (2022–2023 yillar)

Janglarda “Kolchuga” tizimi rus radarlari va zenit raketalarining faoliyatini aniqlab, ularga qarshi REB va artilleriya hujumlari rejalashtirilgan.

Bu Ukraina kuchlarining himoyasini kuchaytirgan va dushmanning radiolokatsiya samaradorligini pasaytirgan.

2022 yilning birinchi yarmida Lugansk hududida

Ukraina qo‘shinlari “Kolchuga” tizimini dushmanning uchuvchi texnikalarini uzoqdan aniqlash va ularning harakatini kuzatish uchun faol ishlatgan. Bu razvedka ma’lumotlari Ukrain ZRK tizimlari uchun tezkor va aniq hujum rejalarini tayyorlash imkonini bergan.

2023 yildagi Donesk va Mariupol atrofidagi operatsiyalar

Ukrain qo‘shinlari «Kolchuga» tizimi orqali Rossiya radarlari va radio signallarini aniqlab, ularga qarshi REB va artilleriya hujumlarini rejalashtirgan. Bu frontda rus kuchlarining radioelektron kurash qobiliyatini kamaytirgan [6].

1-jadval

Bir qator mashhur antidron tizimlarining texnik va ekspluatatsiya xarakteristikalar

Tizimlarning nomlanishi	Islab chiqargan davlat	Texnologiya	Aniqlash diapazoni	Hujum usuli	Qo‘llanish sohasi	Mobillik	Qo‘shimcha imkoniyatlari
RFDEW	Buyuk Britaniya	Radio to‘lqinli energiya (RF jamming)	5-10 km	Radio signallarini buzish, elektronikaga zarar	Harbiy operatsiyalar, himoya bazalari, ommaviy tadbirlar	Mobil va statsionar	Integratsiyalangan razvedka va tahlil tizimi
Levada	Rossiya	Radioelekt ron kurash (REB)	3-7 km	Radio signallarni bloklash, kommutatsiya buzish	Harbiy jang maydonlari	Mobil	Bir nechta dronlarni bir vaqtda buzish
Kolchuga	Rossiya	Radioto‘lqinli signal aniqlovchi va kurash	50 km va undan yuqori	Signallarni aniqlash va buzish	Harbiy razvedka va REB	Mobil	Havodan hujum va razvedka dronlariga qarshi
Sky Sentinel	Ukraina	AI asosidagi radiolokatsiya	10 km	Dronlarni aniqlash va signal buzish	Xavfsizlik va razvedka	Mobil	AI tahlili, avtomatik kuzatuv
Peleena	Rossiya	Radioelekt ron kurash	2-5 km	Signallarni buzish	Harbiy operatsiyalar	Mobil	Zararli signallarni avtomatik aniqlash
Spider-AD	Pokiston	Radiojasad va RF jammer	3-7 km	Radio signallarini yo‘q qilish	Harbiy baza himoyasi	Mobil	Ko‘p kanalli buzish rejimi
Bhargavastra	Hindiston	Radioelekt ron kurash (REB)	5-8 km	Dronlarning signallarini buzish	Harbiy va chegara himoyasi	Mobil	Avtomatik aniqlash va tezkor yo‘q qilish

IHTAR	Turkiya	Radioelekt ron kurash	3-6 km	Radio signal buzish	Harbiy operatsiyalar	Mobil	Integratsiyalanga n xavfsizlik tizimi
KAPAN	Turkiya	Radioelekt ron kurash	2-5 km	Radio signallarni buzish	Harbiy va tinchlik zonasi himoyasi	Mobil	Kichik va o'rta dronlarga qarshi

Xulosa qilib aytganda, zamonaviy urushlarda radioelektron kurash (REK) juda muhim bo'lib, bugungi kundagi harbiy harakatlardagi eng asosiy yo'ndashuvlardan biriga aylangan. REK orqali raqibning boshqaruv tizimlarini buzish, aloqa va navigatsiyani rad qilish, havo hujumlariga qarshi samarali himoya qilish imkoniyatlari jarayonni aniq belgilaydi;

Ukraina va Rossiya o'rtasidagi urush, zamonaviy texnologiyalarni keng qo'llash bilan ajralib turadigan bir nechta urushlardan biridir. Ushbu urushda radioelektron kurash (REK) muhim ahamiyat kasb etmoqda, chunki u jangovar operatsiyalarda aloqani, boshqaruv tizimlarini va boshqa elektron qurilmalarni ta'sir qiladi. Barcha zamonaviy jangovar harakatlar singari, bu urushda ham REK dushmanning harbiy imkoniyatlarini cheklash va o'zining jangovar samaradorligini oshirishda asosiy vositaga aylangan;

Ukraina o'z navbatida, o'zining REK tizimlarini rivojlantirgan va Rossiyaning signalini rad qilish uchun turli xil tizimlar qo'llanilmoqda. Shuningdek, Ukrainada REK tizimlari yordamida sun'iy yo'ldoshdan foydalanishni himoya qilish va dushman tomonidan ishlatiladigan GPS tizimlarini bloklashga urinishlar amalga oshirilgan [5].

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

[1] Смирнов В.А., Гусев Ю.М. "Радиоэлектрон курашнинг асослари". Тошкент: ҳарбий нашр, 2019.

[2] Козлов А.В., Петров Д.И. "РЭК замонавий қуролли кучларда". Санкт-Петербург: илмий нашр, 2020.

[3] Переслегин В.П. "Радиоэлектрон кураш технологиялари замонавий урушларда". Москва: стратегик таҳлиллар институти, 2021.

[4] Соколов А. Боевое применение средств РЭБ – плюсы и минусы. Сайт [//www.arms-tass.su](http://www.arms-tass.su).

[5] Гордиенко В. К столетию радиоэлектронной борьбы. Сайт [//www.computer-museum.ru](http://www.computer-museum.ru).

[6] Ochiq internet sahifalari (Yandex, Rambler va h.k.).

AMIR TEMUR ARMIYASINI JANGOVAR TUZILISHI

I.I. SOTVOLDIYEV

O'R MV Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti

Annotatsiya: Amir Temur qo'shinining asosini ko'chmanchi qabilalar tashkil etib, ular otiqlar va kamonchilarni yetkazib bergan. O'troq xalq armiyaga piyodalarni va yordamchi xo'jaliklar uchun ishchilar va shaharlarni qamal qilish uchun jangchilarni, ya'ni katapultalarni ishlatuvchi, taranlarni uruvchi, yonib turgan kamon o'qlarni va neft aralashmasidan tayyorlangan yonuvchi granatalarni otuvchi askarlarni yetishtirib bergan.

Kalit so'zlar: Jangovar tartib front, armiyada yengil piyodalar ham bo'lib, (amiri lashkar) bosh kuchlari (qo'l) bilan, qal'alarining qalin devorlari oldida devor buzuvchi (manjanik) va tosh uloqtiruvchi (arroda) to'plar o'rnatilgan. To'plar (ra'd) harakatga keltirilgan. Oliy Bosh Qo'mondonning ad'yutanti (tavochi) yetkazgan maxsus buyruqqa (muchalkaga) binoan qo'shin yig'ilgan, avanpost (qaravul), uning ortidan avangard (xiravul), o'ng qanot (barang'or), chap qanot (jarang'or), markaz (qo'l), arergard (chag'dovul) harakatlangan.

Аннотация: Армия Амира Темура основывалась на кочевых племенах, которые обеспечивали кавалерию и лучников. Оседлое население готовило армию к участию в пехоте и вспомогательных работах: фермеров, рабочих для осады городов и поселений, солдат, использовавших катапульты, тараны, зажигательные стрелы и огненные гранаты на основе масляной смеси.

Ключевые слова: Боевой порядок фронта, в армии также присутствует легкая пехота, (главнокомандующий армией) с основными силами (рукой), перед толстыми стенами крепостей устанавливались стенобитные орудия (манжаник) и камнеметы (arroda). Снаряды запускались. По специальному приказу (мучалка), изданному адъютантом (tavochi) Верховного главнокомандующего, армия формировалась в следующем порядке: аванпост (стража), за ним авангард (хиравуль), правое крыло (барангор), левое крыло (жарангор), центр (ханд), арьергард (чагдовуль) двигались.

Annotation: Amir Temur's army was based on nomadic tribes, which supplied cavalry and archers. The settled people trained the army for infantry and auxiliary farms, workers for siege of cities and towns, soldiers who used catapults, hammers, burning arrows and flaming grenades made of oil mixture.

Keywords: Combat order front, there are also light infantry in the army, (commander army) with the main forces (arm), in front of the thick walls of the castles break the wall (manjanik) and stone throwing (arroda) cannons installed. The balls are fired. According to a special order (muchalka) issued by the adjutant (tavochi) of the Supreme Commander-in-Chief, the army was assembled, avanpost (guard), followed by avant-garde (hiravul), right wing (barangor), left wing (jarang'or), center (hand), arergard (chagdovul) moved.

Amir Temur armiyasidagi jangchilarga doimiy maoshlar to'langan. Maoshning hajmi xizmatni qanday olib borilishiga bog'liq bo'lgan. Oddiy askar 2 tadan 4 tagacha otning bahosiga teng bo'lgan maosh, o'nbegi – o'z o'nligining maoshiga teng miqdordagi maoshni olgan (shuning uchun u o'z jangchilarining yuqori maoshga erishishlaridan manfaatdor bo'lgan); yuzbegiga oltita o'nlikning maoshiga teng miqdordagi maosh to'langan va hokazo. Intizomiy jazolarning turlaridan biri maoshning o'ndan bir qismini ushlab qolish bo'lgan.

Armiyada yengil piyodalar ham bo'lib, ular safarda otlarda harakatlanganlar, jang olib borishda esa, kamondan nishonni bexato urish uchun arablarga o'xshab otlardan tushib piyoda holda jang qilganlar. Piyoda jangchi qilich, 30 ta o'qqa ega bo'lgan kamon bilan qurollangan. Yengil piyodalar baland pastliklarda harakatlanish va shaharlarni qamal qilish uchun qo'llanilgan. Bundan tashqari, Amir Temur tog'larda harakatlanish uchun maxsus otryadni (tog' piyodalarini) tashkil etgan.

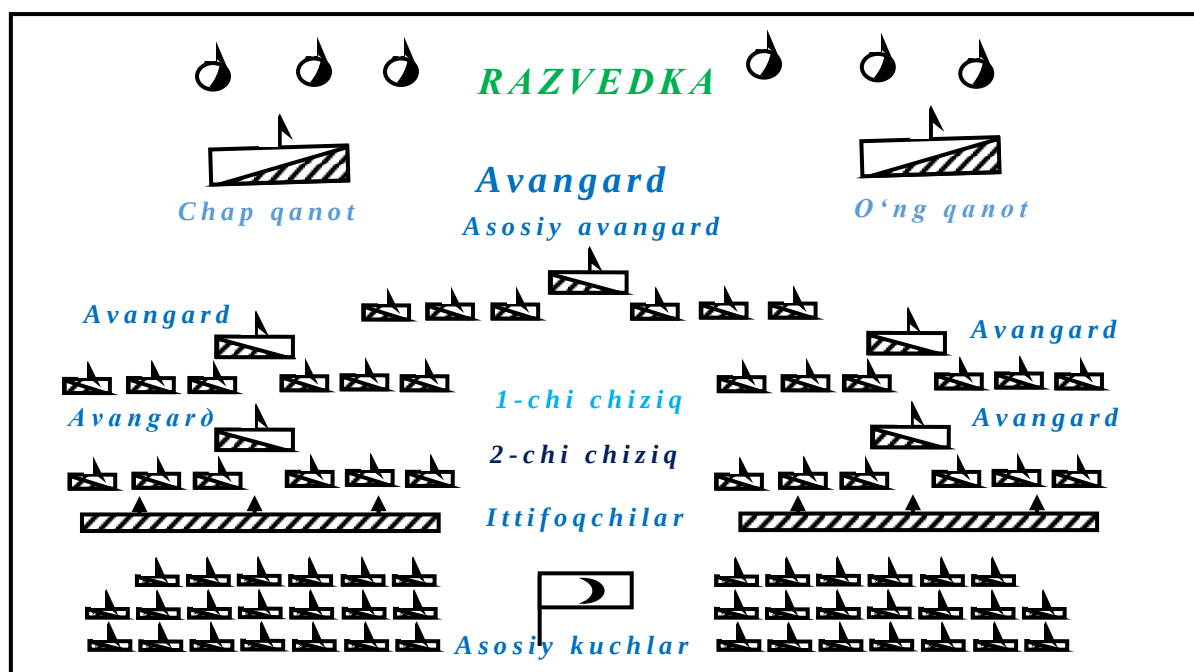
Qo'shin qat'iy tashkiliy tizimga va aniq saflanish tartibiga ega bo'lgan. Har bir jangchi o'z o'nligidagi joyini bilishi, har bir o'nlik yuzlikdagi joyini bilishi kerak bo'lgan va hokazo. Harbiy qismlar saflarda yaxshi harakatlana olgan va anjomlari, kiyim-boshlari va bayroqlarining rangi bilan bir-birlaridan ajralib turgan.

Ayrim otryadlar otlarining rangi bilan ham farq qilgan. Amir Temur davrida harbiy yurishdan oldin ko'riklar o'tkazish to'g'risidagi qonun og'ishmasdan bajarilgan.

Jang uchun katta va tekis maydon tanlangan, bunda suv va otlar uchun yem-xashakning yaqin bo'lishiga, quyoshning o'z jangchilarining ko'ziga tushmasligiga katta e'tibor berilgan. Jangovar tartib front, ayniqsa chuqurlik bo'ylab yoyilgan. Markazni kuchsizlantirishda dushmani qurshab olish vositasi hisoblangan qanotlar kuchaytirilgan. Hal qiluvchi zarbani berish uchun Amir Temur kuchli zaxira yaratgan.[1]

Yirik janglar davrida rang-barang jangovar bayroqlar bilan bezatilgan Bosh Qo'mondon chodiri (bargoh, saroparda) jangni boshqarish oson bo'lishi uchun balandlikda o'rnatilgan. Odatda, Bosh Qo'mondonning chodiri oldida harbiy orkestr uzluksiz nog'ora chalib, askarlarning jangovar ruhlarini ko'targan.

Jangni qo'riqlash xizmatini bajarayotgan yengil otliqlar yoki avanpostda turgan yengil qo'shinlar o'qlarni otib, drotiklarni uloqtirib boshlagan, keyin avangard jangga kirgan. Ularni qo'llab-quvvatlash kerak bo'lgan paytda jangga o'ng qanot avangardi (shaqovul), keyin chap qanot avangardi (chapovul) kirgan; agar yana madad kuchlari kerak bo'lib qolsa, jangga o'ng qanotning chap tomon yarmi va chap qanotning o'ng tomon yarmi kiritilgan; ularning kuchlari yetarli bo'lmasa, jangga ikkala qanotning qolgan qimslari kiritilgan va vaziyat to'g'risidagi axborot Amir Temurga yetkazilgan. Agar mana shu kuchlar ham yetarli bo'lmasa, qo'mondonning shaxsan o'zi (amiri lashkar) bosh kuchlari (qo'l) bilan, ya'ni zaxira bilan, to'qqizinchi hujum g'alaba keltirishiga komil-ishonch bilan jangga tashlanishi kerak edi. «To'qqizinchi hujum, degan edi Amir Temur, g'alaba keltiradi».

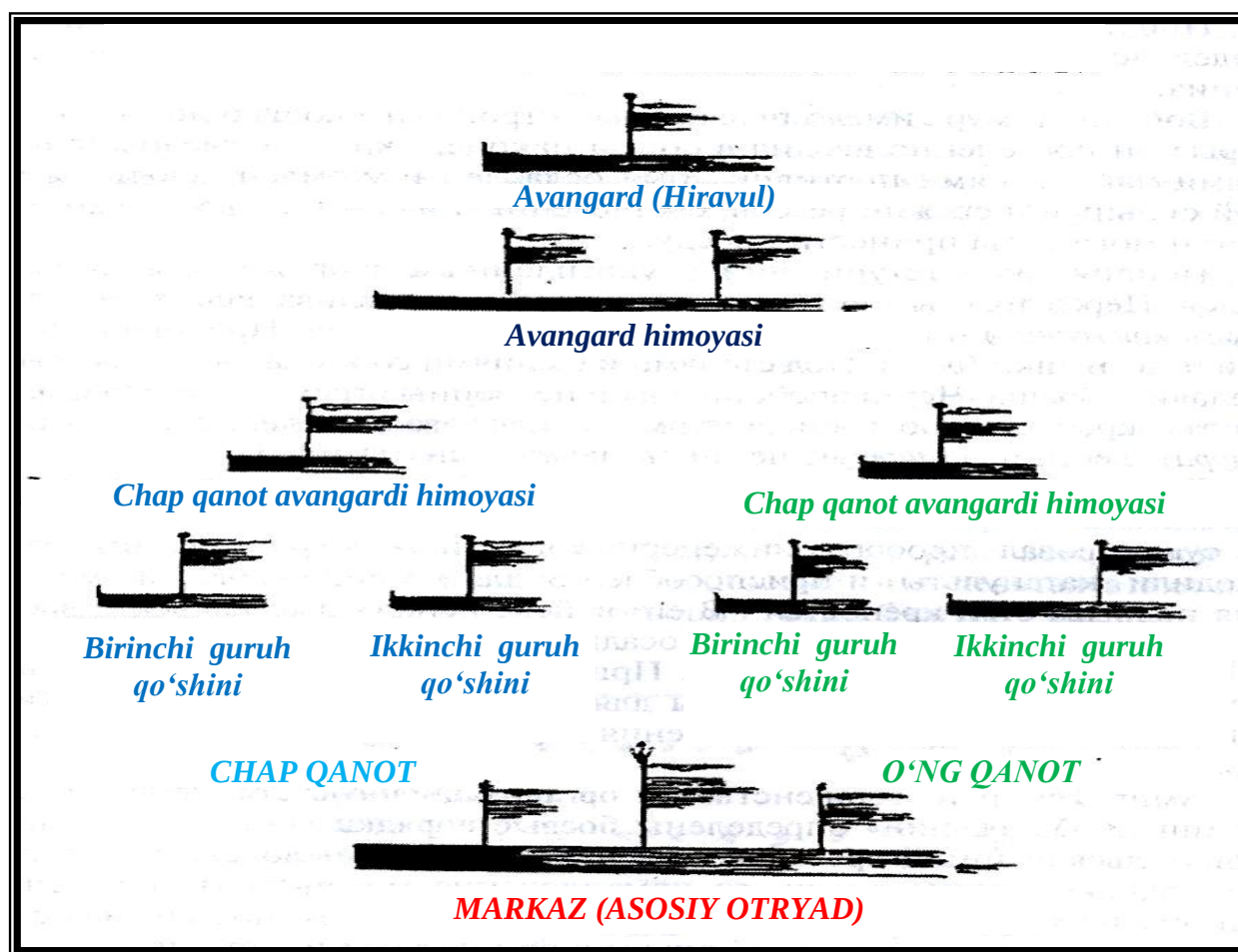


1-rasm. Amir Temur qo'shini jangovar tartibining tuzilish chizmasi

Amir Temur qo'shini to'g'ri safga va bir nechta jangovar chiziqqa ega bo'lib, ular birin-ketin jangga kiritilgan va oxirida ketma-ket hujumlar bilan dushman holsizlantirilib, kuchsizlantirilganidan keyin eng yaxshi jangchilardan tashkil topgan, doimo g'alabani ta'minlovchi qudratli zaxira jangga kiritilgan.

Chekinib, mustahkamlangan inshootlarda yashiringan g'anim qamal qilingan. Qal'alarning qalin devorlari oldida devor buzuvchi (*manjaniq*) va tosh uloqtiruvchi (*arroda*) to'plar o'rnatilgan. To'plar (ra'd) harakatga keltirilgan. Devor va minoralarning ostidan yerto'lalar kovlangan. Devorlarda bo'shliqlar hosil qilingan. Shu bo'shliqlardan jangchilar quyundek qal'a ichiga bostirib kirganlar. Shturm davrida himoya qalqonlari (to'ra), shotilar, halqalar, arqon va boshqalardan foydalanilgan.[3]

Amir Temur armiyasida kavaleriya hujumining tashkil etilishi, uning strategiya va taktikasi o'zining takomillashgan darajasiga yetdi. Amir Temur armiyasida muhandislik qismlari va bo'linmalarining birinchi namunalari bo'lib, ularga katapultalar, neftdan tayyorlangan yonuvchi moddani uloqtiradigan va qal'a devorlarini portlatuvchi moslamalar kirgan. Uning armiyasida o'sha vaqtning eng zamonaviy texnikalari – qamal qilish texnikasi, yonib turgan neft to'ldirilgan xurmachalarni uloqtiruvchi ballistalar qo'llanilgan. Amir Temur qo'shinida daryolardan kechib o'tishni ta'minlovchi mutaxassislar – pontonchilar ham bo'lgan. Fan va texnikaning yutuqlari, ayniqsa, Xitoy texnikasining yutuqlari keng foydalanilgan.

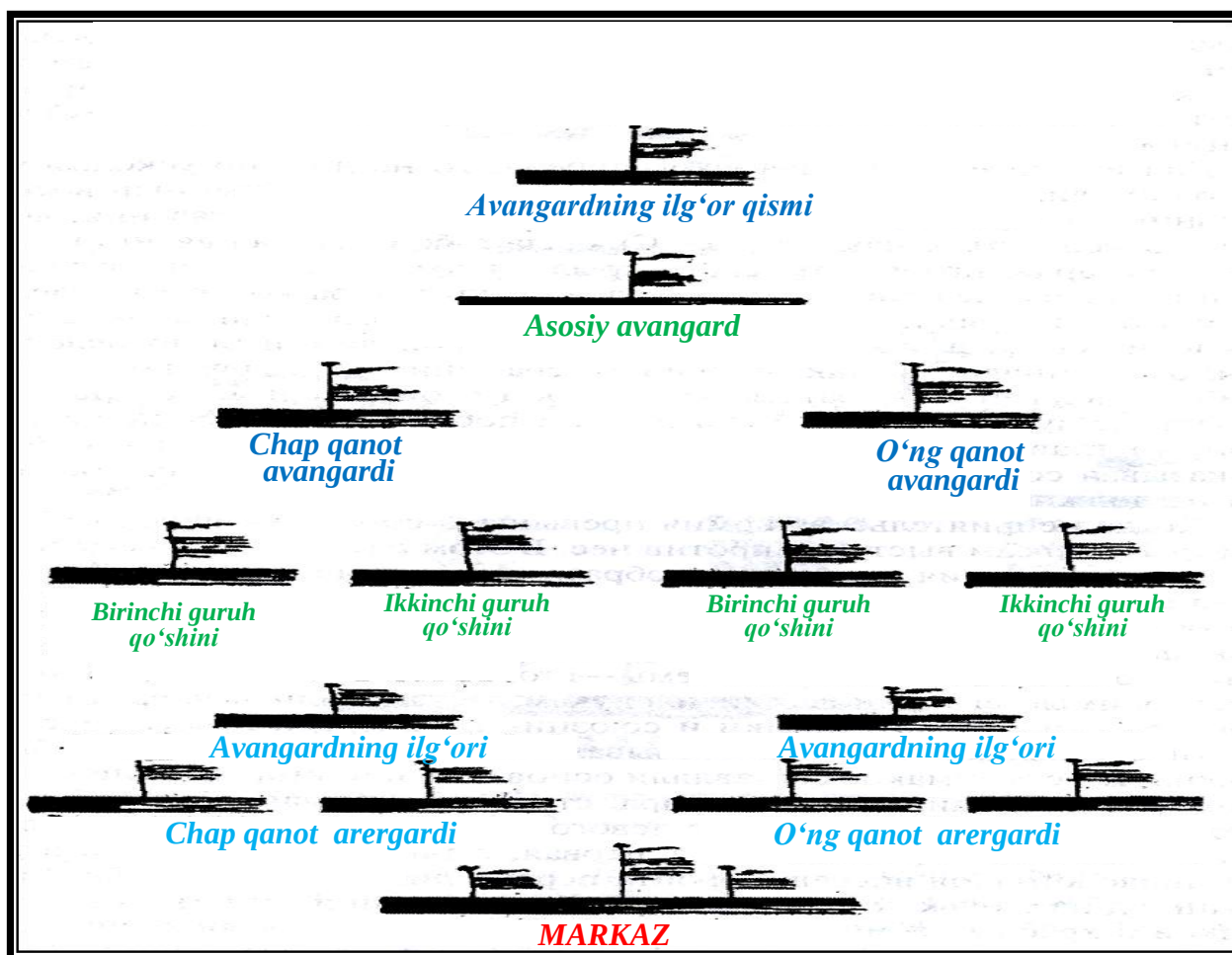


2-rasm. Qo'shinining saflanish tartibi

Sohibqironning qoidasiga ko'ra, yaxshi boshliq g'anim otryadining sonini bilgach, unga qarshi o'z otryadlarini qarshi qo'ya olishi, dushman harakatlarini kuzatishi, uning o'qchilari, nayzachilari, qilichbozlarining holati qanaqa ekanligini, ular tezkorlik bilan yoki sust hujum qilyaptimi, hammasi birgalikda hujumga o'tdimi yoki qismlarga bo'linibmi, bularning hammasini bilishi kerak, jang maydoniga hujum uchun kirish yo'llarini, kerak bo'lganda chekinish yo'llarini bilishi, dushmanning maqsadini anglab yetishi va uning jangovar tartibiga yorib kirishga harakat qilishi kerak. Bundan tashqari u pistirmaga tushib qolmaslik uchun ehtiyotkorlik bilan harakat

qilishi, jangning butun mohiyatini tushunishi, dushmanning niyatini anglashi va uning rejalarini buzib tashlash uchun hamma vositalarni ishga solishi kerak.[4]

«Sardor qirq ming chavandozlarni o'n to'rtta qismlarga quyidagi tartibda tuzishi kerak bo'lgan: u o'z jangovar chizig'ini tuzadi va uni markaz deb nomlaydi. Uch qism arergardni tashkil etadi (yoki o'ng qanot korpusi). Uchta qismdan biri ilg'or nomini oladi (mana shu arergardning ilg'ori). Chap qanotni tashkil etgan uch qismning biri uning uchun ilg'or bo'lib hisoblanadi. Xuddi shunday uchta boshqa qismlar o'ng qanot arergardining oldida joylashgan bo'lib, uning fronti bo'ladi, bu uchta otryadlardan biri chap qanot fronti uchun avangard bo'lib xizmat qiladi. Chap qanot ham xuddi shunday sondagi qo'shindan iborat bo'ladi va ular uning frontini tashkil etadi.

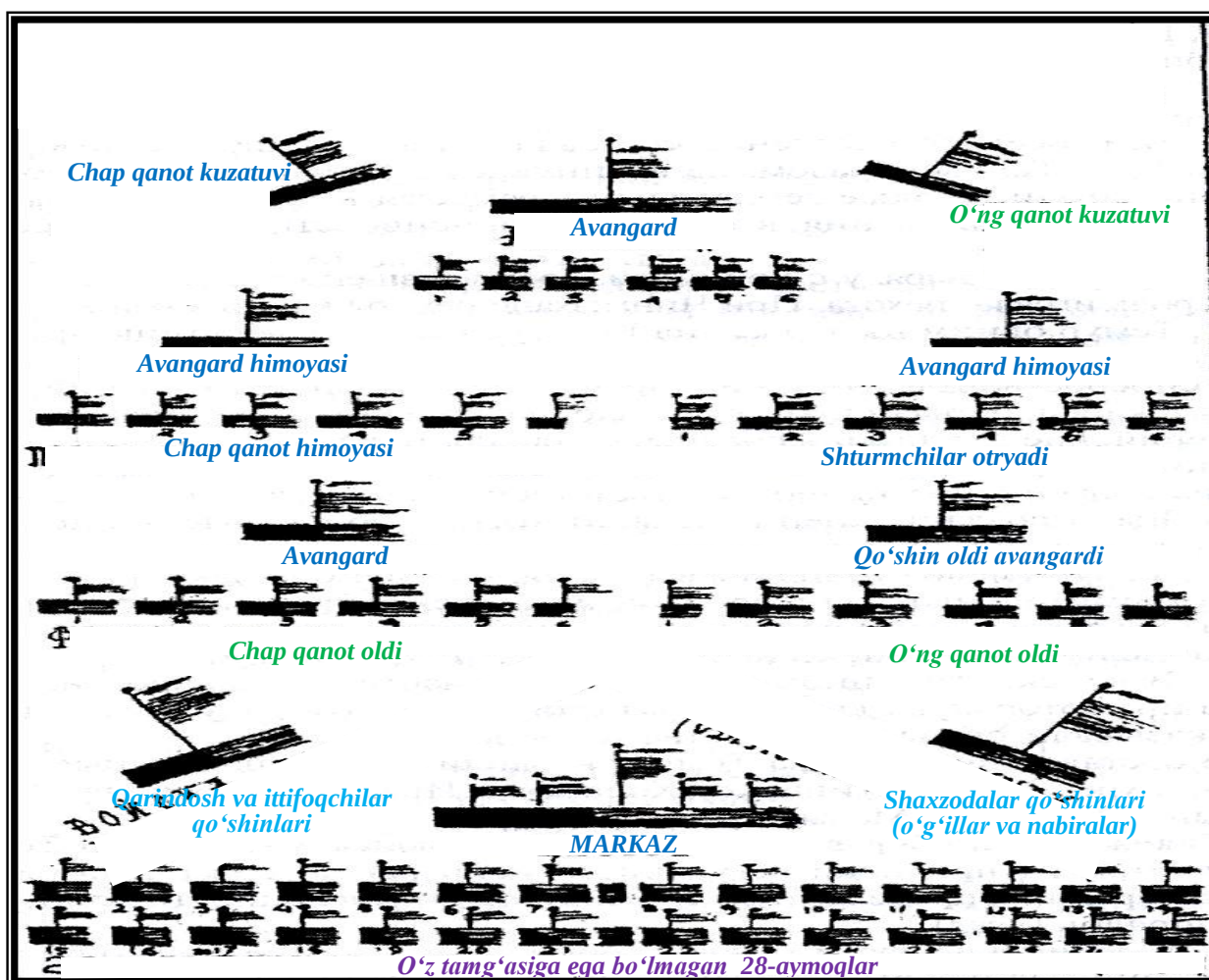


3-rasm. 40 ming chavandozdan iborat 14 ta bo'linmaning saflanish tartibi

Bitta qism, oldingiga o'xshab chap qanot avangardi bo'lib xizmat qiladi. Keyin u asosiy otryadini markaz qo'shinlari oldida saflagan. Avangardning safiga: kamanchilar, qilichlar bilan qurollangan jangchilar, nayzachilar, dushman avangardiga tartibsizliklarni keltirib chiqarish uchun baland ovozda baqirib jang qiladigan jasur va tajribali jangchilar kiritilishi kerak», deb yozilgan

«Tuzuklar»da – «Bosh qo'mondonning e'tiboridan dushmanning hech bir harakati chetda qolmasligi kerak, o'ziga bino qo'ygan harbiy boshliq buyruqsiz oldinga harakat qilishni boshlasa jazolanishi kerak», deb ta'kidlangan. Avval jangga avangard kirgan, keyin o'ng va chap qanot avangardlari, undan keyin o'ng va chap qanotda turgan otliq bo'linmalar kirgan, ularning ortidan o'ng qanotning ikkinchi otryadi va chap qanotning birinchi otryadi harakatlangan. Agar jang olib borayotgan jangovar chiziqni ikkinchi chiziq qismlari bilan to'ldirish yetarli bo'lmasa va o'n uchta hujum jangning oqibatini hal qilmasa, unda bosh qo'mondon ikkilanmasdan jangga saralangan jangchilardan tashkil topgan o'z zaxiralarini kiritishi kerak bo'lgan. Agar shunda ham g'alabaga erishilmasa, bosh qo'mondon o'zi dadillik bilan jangga kirishi va shaxsiy namuna ko'rsatib

jangchilarning ruhlarini ko'tarishi kerak edi. Bosh bayroq nazardan chetda qolmasligi kerak bo'lgan.[2]



4-rasm. O'z tamg'asiga ega 12 aymoqdan iborat 40 bo'linmaninigi saflanish tartibi

Agar g'animning armiyasi qirq ming kishidan oshsa, unga qarshi Amir Temurning o'zi qo'shinni boshlagan. Bu vaqtda uning qo'shini jangni olib borish uchun quyidagi tartibda bo'lingan: qirqta otryaddan tashkil topgan armiya ichidan o'n ikkita otryadni tanlagan va ularga ajralib turuvchi belgi (tamg'a) bergan; ular qirqta aymoqlarga bo'lingan. Ulardan eng saralangan o'n ikkitasi birinchi jangovar chiziqni, qolgan yigirma sakkiztasi esa – ikkinchi va uchinchi chiziqlarni tashkil etgan. O'g'illari va nabiralari qo'mondonligidagi qo'shinlar o'ng qanotning oldiga, qarindoshlari va ittifoqchilari boshchiligidagi qo'shinlar – chap qanotning oldiga saflangan. Bu qo'shinlar zaxirani tashkil etgan va qaerga yordam kerak bo'lsa, o'sha yerga yetib kelgan.

Oltita aymoq o'ng qanotning asosini yoki ikkinchi chizig'ini va bittasi – uning avangardini tashkil etgan, shuncha aymoqlar, xuddi shu tartibda chap qanotning asosini tashkil etgan; ikkinchi chiziqning ikkala qanotlari oldida birinchi, shu tartibda va shuncha sondagi aymoqlar birinchi chiziqning fronti ortida shuncha aymoqlardan iborat, tajribali qo'mondonlar va jasur jangchilardan iborat katta avangard qo'yilgan; bu avangardning oldida, o'zining shaxsiy avangardi hisoblangan yana bitta aymoq, dozor va raz'ezdlar sifatida ikkita yengil qo'shin otryadi joylashgan, ular armiyani to'satdan beriladigan zarbalardan himoya qilgan va dushmani kuzatgan.[4]

Yengil qo'shinlar va ilg'or avangard jangni boshlagan; bosh avangardning boshlig'i ularni kuchaytirgan va o'z qo'shinlarini jangga kiritgan, agar yordam kerak bo'lsa, birin-ketin jangga birinchi, keyin ikkinchi chiziqni kiritib hujumni kuchaytirgan. Agar bu yordam ham yetarli

bo'lmasa, unda o'ng va chap qanot zaxiralari, ya'ni Amir Temurning o'g'illari, nabiralari, qarindoshlari va ittifoqchilari boshliq qo'shin jangga kirgan.

Qo'shinni yig'ish va ta'minlash. Qo'shinni boshqarish. Amir Temur qo'shinida to'xtovsiz takomillashib borayotgan muntazam armiyaning ko'pgina xususiyatlari mujassamdir: qo'shinning aniq soni, jangovar tartibi (yosol) belgilangan.

Kavaleriya qismlari ko'p hollarda bir-birlaridan nafaqat kiyim-boshlari, bayroqlari va anjomlarining ranglari, balki otlarining rangi bilan ham farq qilgan. Bunday farq jang paytida qo'shinni boshqarishda katta rol o'ynagan. Dushmanga nisbatan ustunlik otliqlarning yuqori harakatchanligi va Amir Temur tomonidan ularni mohir manyovr qilinishi bilan ta'minlandi.

Turli usullar bilan dushmanning mudofaa tizimini yakson etish, g'animning yirik va yaxshi mustahkamlangan ob'ektlariga to'satdan hujum qilish, dushman tomonining hukmdorlari va taniqli harbiy boshliqlarini asirga olish, qurshab olingan shahar-qal'alarni uzoq vaqt qamal qilish, birma-bir qishloqlar, tumanlar, shaharlar va viloyatlarni zabt etish, dushmanni to'liq tor-mor etilgunigacha ta'qib etish, zabt etilgan hududlarni boshqarish uchun o'zining sodiq kishilarini tayinlashdek strategik maqsadlarni ketma-ket amalga oshirilishi Amir Temurga ko'plab g'alabalar olib keldi.[5]

Uning harbiy ishni rivojlantirishga qo'shgan katta hissasi butkul yangi ko'rinishdagi kavaleriya qismlarini (kunbul, kumbul) joriy etganidan iborat bo'lib, u nafaqat o'z qanotlarini himoya qilish uchun, balki dushman qanotlarini aylanib o'tish va front ortiga zarba berish uchun ham mo'ljallangan.

Otliq qo'shin armiyaning zarbdor qismini tashkil etib, yengil hamda og'ir otliqlarga bo'lingan. Yoylar, o'qdonlar, qilichlar bilan qurollangan yengil otliqlar razvedka bilan shug'ullangan, qo'riqlash xizmatini olib borgan va kerak bo'lgan hollarda dushmanning ilg'or otryadlariga qarshi jangga kirgan.

Saralangan jangchilar va zodagonlardan tuzilgan og'ir otliqlar dushmanning asosiy zarbdor kuchlariga qarshi jang olib borgan bo'lsa, chavandozlar nayza, dubulg'a, zirh, qilich, yoy, o'qlar solingan sadoq bilan qurollangan.

Harbiy yurishdan oldin Amir Temur odatda harbiy kengash (mashvarat) chaqirgan, unda harbiy boshliqlar, beklar va amirlar ishtirok etgan. Davlatning turli qismlaridan, Oliy Bosh Qo'mondonning ad'yutanti (tavochi) yetkazgan maxsus buyruqqa (muchalkaga) binoan qo'shin yig'ilgan. Jangchilarni yig'ishdan tashqari tavochilarning majuriyatlariga qo'shinni joylashtirilishi, uning harakatlanishi va jangovar tartibini nazorat qilish ham kirgan.

Amir Temur o'z qo'shinini jangga olib borishda uning hamma kerakli narsalar bilan ta'minlanishiga, lagerlarda joylashishiga alohida e'tibor bergan.

Sohibqironning buyrug'iga binoan viloyatlar hukmdorlari, tumanlar va shaharlar beklari, qal'alar boshliqlari (dorug'a) ro'yxat bo'yicha ko'rsatilgan muddatda o'z qo'shinlari, anjomlari, oziq-ovqatlari bilan oldindan ko'rsatilgan yerga (miod yeri) yetib kelgan.

Amir Temur To'xtamishga qarshi Dashti Qipchoqqa harbiy yurishni uyushtirishdan oldin (1390–1391) o'zining o'rinbosarlariga qo'shinni uzoq davrga yetadigan oziq-ovqat, qurol-yarog' va boshqa kerakli narsalar bilan ta'minlashga buyruq bergan. Har bir jangchi bitta yoyga, o'ttizta o'qqa, bitta kamondonga, bitta qalqon va bitta zaxira otga ega bo'lgan. Safar chog'ida har o'nta jangchiga bitta chodir, ikkita belkurak, kirka, o'roq, arra, bolta va yuzta igna berilgan.[2]

Bundan tashqari, har bir jangchi o'zi bilan arqon, teri va qozon olib yurgan. Oddiy jangchilar safar chog'ida o'n sakkiz kishiga bitta chodir olib yurgan. Ularning har biri yonida ikkita otni yetaklab yurgan, o'zi bilan yoy, zirh, qilich, o'qdon, qop, o'nta igna, bolta, arra va teridan tikilgan qop olib yurishi kerak bo'lgan. [6]

Jangchilar chodirlarda beshtadan bo'lib joylashgan. Ko'zda tutilgan ta'minot bo'yicha ularning har biri dubulg'a, zirh, qilich, yoy, o'qdon va ot bilan ta'minlangan. O'n begi alohida chodirga joylashgan. U zirh, qilich, yoy, kamondon bilan qurollangan. U o'zi bilan beshta qo'shimcha otni olib yurish huquqiga ega bo'lgan.

Yuz begiga ham alohida chodir berilgan. Uning qurol-yarog'larini qilich, yoy, zirh, o'qdon, gurzi, to'qmoq va kolchugalar (simdan tayyorlangan halqachalarni bir biriga o'tkazib to'qilgan ko'ylak) tashkil etgan. Yuz begiga qo'shimcha o'nta ot berilgan.

Ming begi chodirdan tashqari soyabonga ega bo'lib, qurol-yarog'lari nayza, qilich, o'q-yoy, dubulg'a, zirh (chax, oroyna), kolchugalardan iborat bo'lgan.

Piyodalar harbiy yurishlar paytida qilich, yoy va kerakli sondagi yoyni o'qlari bilan qurollanib harakatlangan.

Qo'shin bilan birgalikda bir joydan ikkinchi joyga qassoblar, oshpazlar, qovurilgan va qaynatilgan go'sht sotuvchilar, nonvoylar, arpa, meva sotuvchilar ko'chib yurgan. Jangchilarga ko'chma hammomlar xizmat ko'rsatgan. Yurishlarda nafaqat jangchilar, balki qo'shinga xizmat qiluvchi ko'p sonli ma'muriyat ham ishtirok etgan. Bu yerda temirchilar, qurolsozlar, duradgorlar, teriga ishlov beruvchilar, yer qazuvchilar, xo'jalik ishlarini bajaruvchilar va boshqalar bo'lgan. Amir Temur qo'shini safarlarida harakatlanayotgan jangovar qo'shin korpusi ortidan yirik qurolsiz omma harakat qilgan.

Qo'shinni yig'ish to'g'risidagi qaror chiqqanidan keyin, jangchilar o'z oilalari, anjomlari, oziq-ovqatlari bilan birgalikda belgilangan joyga yetib kelgan. Lagerning (o'rdagohning) markazida Oliy Bosh Qo'mondonning qarorgohi, shuningdek, turli-tuman qismlar va oddiy jangchilarning chodirlaridan tortib yirik harbiy boshliqning chodirigacha bo'lgan birlashmalarning chodirlari joylashgan, har bir kishi o'zining joylashgan o'rnini juda yaxshi bilgan. [7]

Lagerda Oliy Bosh Qo'mondonning rang-barang bayroqlar bilan bezatilgan chodiri (bargoh) o'rnatilgan. Ko'rsatilgan vaqtda (miod vaqti) lagerga yetib kelgan jangchilar, joriy etilgan tartibga ko'ra o'z joylarini egallagan va qo'shin ko'rigiga tayyorgarlik ko'rgan.

Kerakli sondagi jangchilar yig'ilganidan keyin, harbiy lagerda kamonchilar, arbaletchilar, tosh uloqtiruvchilar, nayzachilar, to'pchilar va boshqalardan tashkil topgan ulkan qo'shinning ko'rigi bo'lgan. Qo'shinda yonuvchi aralashma (naft) solingan xurmachalarni uloqtirish uchun maxsus askarlar bo'lib, ular o't otuvchi qurollarning to'xtovsiz ishlashlarini ta'minlaganlar.[1]

Oliy Bosh Qo'mondonning buyrug'iga ko'ra, jangchilar himoya sovuqlarida, to'liq qurol-yarog'lari bilan saflanganlar. Ko'rik o'tkaziladigan maydonda turli qismlarga tegishli bo'lgan yashil, qizil, sariq, binafsha, qora, ko'k bayroqlar hilpirab turgan. Harbiy orkestr sadosi ostida Amir Temur navbatma-navbat jangchilar sherengalari oldidan o'tgan. Jangchilar nayzalarini baland ko'tarib, bo'lajak jangga tayyor ekanliklarini namoyon etib baland ovozda na'ra (suron) tortganlar.

Jangchilarning jangovar ruhi va tayyorgarligini aniqlash uchun yurishlar va janglardan oldin harbiy ko'rikning o'tkazilishi Temuriylar davrida ham an'ana bo'lib qoldi. Ko'rikda nafaqat qo'shin birlashmalari, balki asosiy kuchlarning ortidan harakatlanadigan ta'minot aravalari ham ishtirok etgan.

Lagerning atrofi chuqur xandaqlar bilan o'ralgan va qo'riqlash zastavalari va postlari bilan puxta qo'riqlangan. Lagerda o'rnatilgan vaqtlarda qo'shin qo'riqlash xizmatini olib borgan. Qo'riqlash qismlari lagerdan 5–6 km oldinga chiqqan, undan postlar, postlardan soqchilar ajratilgan va oldinga yuborilgan.

Ta'kidlash kerakki, Amir Temur qo'shinni boshqarishga katta ahamiyat bergan.

Sohibqironning buyrug'i bo'yicha dongdor komandirlardan to'rttasi birinchi darajali qo'mondon – beklarbegi lavozimiga tayinlangan. Bitta harbiy boshliq bosh qo'mondon amir-ul-ulamo vazifasiga tayinlanib, u bevosita Oliy Bosh Qo'mondonga bo'ysungan.

Harbiy qismlarni boshqarish uchun yana o'n ikkita harbiy boshliqlar tayinlangan. Birinchi bek mingta chavandozlardan tashkil topgan birinchi guruhga, ikkinchi bek – ikki ming kavaleriyachilardan iborat ikkinchi guruhga qo'mondonlik qilgan, uchinchi bek uch minglik kavaleriyachilarga boshchilik qilgan. Xuddi shu tartibda o'n ikkinchi bek o'n ikki minglik otryadning tepasida turgan.

Quyi toifadagi harbiy boshliq, toifasi bo'yicha yuqori bo'lgan harbiy boshliqqa so'zsiz bo'ysungan.

Amir Temur qo'shinining turli qismlari va bo'linmalariga uch yuz o'n uchta beklar qo'mondonlik qilgan, ulardan yuztasi – o'nbegilar, yuztasi – yuzbegilar va yuztasi – mingbegilarni tashkil etgan. Yirik qo'shin birlashmalari Amir Temurning o'g'illari, nabiralari va Shayx Nuriddin, Xo'ja Sayfuddin, Shohmalik, Ollohdod, Jahonshohdek mashhur sarkardalar tomonidan boshqarilgan.

Rag'batlantirishda maqto'v, maoshga qo'shimchalar, sovg'alar, lavozimlar, unvonlar (botir, bahodir va boshqalar), qismlar uchun bayroqlardan keng foydalanildi.

Uddaburonliklari va jasoratlari bilan o'zlarini ko'rsatgan, saralangan jangchilar munosib taqdirlangan va o'nbegi darajasiga ko'tarilgan, keyingi jasoratlari uchun yuzbegi, undan keyin esa mingbegi lavozimini egallagan.

Jasur jangchilar va bahodirlar jangda ko'rsatgan jasoratlari uchun yuqori lavozimlarni egallagan va jamiyatning e'tiborli kishilari toifasiga kirgan. Ular gurzi, chodir, maxsus belbog', qilich va jangovar nayzalar bilan taqdirlangan.

G'animning otryadini qirib tashlagan mingbegi I-darajali amir unvoniga, dushmanning yirik otryadini mag'lub etgan I-darajali amir II-darajali amir unvoniga sazovor bo'lgan. Jang maydonida mardlik va jasorat namunalarini ko'rsatgan oddiy jangchining oylik maoshi oshirilgan. Jang maydonidan qochgan jangchilar o'ljani taqsimlash marosimiga qatnashish huquqidan mahrum etilgan, janglarda ko'p marta yarador bo'lgan jangchilarga g'amxo'rlik va katta ehtirom ko'rsatilgan.

Biror bir davlatni zabt etgan yoki dushman qo'shinini tor-mor etgan harbiy boshliq bahodir faxriy unvoniga sazovor bo'lib, unga burg'u va nog'ora berilgan. Biror bir g'anim shahzodasining yirik qo'shini ustidan qozongan g'alabasi uchun beklar ham xuddi shunday hurmat-e'tiborga sazovor bo'lgan.[8]

Dushman qo'shinini qochishga majbur etgan o'nbegi shahar garnizonining boshlig'i (dorug'a) etib tayinlangan, xuddi shunday qahramonligi uchun yuzbegi – viloyat hokimi, mingbegi – viloyat amiri (vali) lavozimiga ega bo'lgan.

U yoki bu davlatni zabt etgan amirga ushbu davlatning yeri imtiyozli asosda boshqarish uchun suyurg'ol (sovg'a) sifatida berilgan. Amir Temur va Temuriylar davrida suyurg'ol yerni boshqarishning ommabop usuli bo'lib, avloddan-avlodga o'tib kelgan.

Yuqorida ko'rsatib o'tilgan 12 amir nog'ora va jangovar bayroq olgan. Bosh Qo'mondon nog'ora va jangovar bayroqdan tashqari, burg'u va ikkita shtandartga (tumantug'ga, chortug'ga) ega bo'lgan.

Mingbegiga bayroq va karnay (ko'raga), yuzbegi va o'nbegiga nog'ora berilgan. Qo'shin qo'mondonining bayrog'i, nog'orasi va burg'usi bo'lgan. Kastiliya qirolligining elchisi – Klavixoning guvohlik berishicha, harbiy boshliq tinchlik davrida ko'k rangdagi, zardan tikilgan ko'ylak kiyib yurgan. Ular boshlariga telpak (burk) kiyib yurganlar. Bosh kiyimlarining ostidan uch qator kokillari ko'rinib turgan bo'lib, bu belgi Amir Temur armiyasining jangchilari ekanliklarini bildirib turgan.

Dushmanning harbiy kuchlari va uning mudofaa inshootlari to'g'risida, g'anim davlatining ichki ahvoli haqida aniq ma'lumotlarni olish uchun Amir Temur o'zining eng yaxshi razvedkachilarini (josuslarni) jo'natgan. Faqatgina kerakli ma'lumotlarni olgandan keyingina qo'shin harbiy yurishni boshlagan. U mahalliy aholi vakillaridan yo'lboshchilarni (kajarchi, kacharchi) tanlashga ham jiddiy e'tibor bergan.

Amir Temur armiyasida o'ljani taqsimlash davrida mabodo kimdir o'zboshimchalik qilsa, hatto u Sohibqironning yaqin kishisi bo'lsa ham, qattiq jazolangan. Uning butun mol-mulki musodara qilinib, o'zi esa qatl etilgan. Faqat ruxsat berilganidan keyingina yurishning har bir ishtirokchisi, uning toifasi va darajasiga qaramasdan, o'ljaning teng taqsimlangan qismini olish huquqiga ega bo'lgan.[9]

Xulosa:

Amir Temur tuzgan qo'shin o'zining tashkiliy-shtat tizimi bo'yicha Chingizxonning qo'shini tizimiga yaqin bo'lsada, quyidagi xususiyatlari bilan ajralib turgan:

1. Amir Temur armiyasi xalq lashkarlari hisoblansa ham, Chingizxon davrida bo'lgani kabi umumiy xarakterga ega bo'lmagan.

2. Chingizxon davrida qo'shinning asosini ko'chmanchilar tashkil etgan. Amir Temur davrida ko'chmanchilar otliqlar va kamonchilarni yetkazib bergan. Lekin shu bilan birga o'troq aholi ham qo'shinning katta qismini tashkil etgan. Shunday qilib, harbiy xizmatga chorvadorlar bilan birga, urushlarning tez-tez bo'lib turishi va ko'laminig oshganligi munosabati bilan dehqonlar, hunarmandlar va o'troq aholining boshqa toifalari ham chaqirilgan.

3. Amir Temur qo'shinida armiyaning asosini tashkil etgan otliqlar bilan birga piyodalar ham katta rol o'ynagan. Chingizxon davrida to'laqonli piyodalar bo'lmagan.

4. Amir Temur Sharqda birinchilardan bo'lib armiyasiga artilleriya qurolini (ra'd) kiritdi. Yangi turdagi o'q otar qurolning joriy etilishi artilleriya bo'linmalarini yaratishga imkon berdi va natijada to'pchilar (ra'dandozlar) soni bir necha ming kishiga yetdi. Artilleriya qurollari dushmanning tirik kuchlari va texnikasini tor-mor etish hamda qal'alar va tsitadellarni qamal qilish uchun mo'ljallangan. Ular qamal chizig'ining o'ta muhim uchastkalarida o'rnatilgan.

5. Tog'li joylarda mohirlik bilan harakatlanuvchi maxsus piyoda qo'shinlar tashkil etilgan.

6. Amir Temur jangovar tartibini mohirlik bilan tuzgan va ularni chaqqonlik bilan manyovr qilgan, dushman qanotlariga va front ortiga otliqlar bilan kutilmagan zarbalarni bergan, vaziyatdan kelib chiqib, o'z qo'shinini to'qqiz va yetti qismlarga (qo'lga) bo'lgan.

7. Armiyada ayollardan tashkil etilgan qismlar joriy etilgan bo'lib, ular jang paytida erkaklar bilan bir safda turgan va shon-shuhrat hamda jasorat namunalarini ko'rsatgan.

Amir Temur armiyasi safiga Movarounnahr, Dashti Qipchoq, Xuroson, Eron, Badaxshon, Mo'g'uliston, Mozandaron va Jetedan olib kelingan jangchilar kirgan

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

[1] Каримов И.А. Амир Темур – наша гордость. Доклад на международной научной конференции, посвященной 660-летию юбилею Амира Темура, 24 октября 1996 г. // Каримов И.А. Мыслит и работает по новому – требование времени. Т.5. – Ташкент: Узбекистон, 1997. – с. 175 – 185.

[2] Каримов И.А. Обител вечного величия. Речь на тсеремонии открытия памятника Амиру Темуру в г. Самарканде, 18 октября 1996 г. // Каримов И.А. Мыслит и работает по новому – требование времени. Т.5. – Ташкент: Узбекистон, 1997. – с. 165 – 168.

[3] Амир Темур в мировой истории. - Ташкент: Шарк, 2001. - 304 с.

[4] Каримов И.А. Пока народ жив, имя Амира Темура вечно. Речь на тсеремонии открытия Государственного музея истории Темуридов, 18 октября 1996 г. // Каримов И.А. Мыслит и работает по новому – требование времени. Т.5. – Ташкент: Узбекистон, 1997. – с. 160 - 164.

[5] Xudayarov. A.Sh. Darslik. Harbiy tarixi. O'R AKT va AHI, Harbiy nashriyot, 2022. - 552 b.

[6] Muhammad Ali. Darslik. "Amir Temur solnomasi" Toshkent-2008. A. Navoiy nomidagi O'zbekiston Milliy kutubxonasi nashriyoti.

[7] Hamdam Sodiqov. Darslik. "Amir Temur hayotidagi g'aroyibotlar" Toshkent-2007. - 320 b.

[8] Marsel Brion. "Men kim, sohibqiron – Jahongir Temur" Toshkent-2018.

[9] Yunus O'g'uz. "Amir Temur" tarixiy roman. Yangi asr avlodi nashriyoti. Toshkent – 2014. 588 b

BUGUNGI TRANSFORMATSION HARBIY TO‘QNASHUVLARDA MIKROKONTROLLERLARNING QO‘LLANILISHI

A.A. ABIDOV, B.N. UMARALIYEV, Sh.R. SAPAYEV

O‘R MV Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti

Annotatsiya: Hozirgi shiddat bilan rivojlanayotgan zamonamiz texnika va texnologiyalar asri deb bejizga aytilmaydi – ushbu rivojlanishning markazida mikroprotssessorlar va mikrokontrollerlar turadi.

Mikroprotssessorlar haqida o‘quvchilarimizning aksariyati boshlang‘ich ma‘lumotlarga ega. Keling, biz mikrokontrollerlar bilan yaqinroq tanishaylik. Mikrokontroller dastlab bitta kristalli mikro-kompyuter deb nomlangan. Ular hozirda insoniyat faoliyatining deyarli barcha sohalarida keng qo‘llaniladi – sanoat avtomatlashtirish tizimlaridan tortib to maishiy texnikagacha, atom elektr stansiyasini boshqarishdan tortib bolalar o‘yinchoqlarigacha, maxfiy harbiy tizimlardan tortib radioqurilmalardagi kanallarni o‘zgartirishgacha.

Kalit so‘zlar: mikrokontroller, protssessor, periferik, avtomatlashtirish, xotira, dron, datchik, sensor, kompyuter, texnologiya, modul va magnit.

Аннотация: Нашу стремительно развивающуюся эпоху недаром называют веком технологий и инженерии — в основе этого развития лежат микропроцессоры и микроконтроллеры.

Большинство наших студентов имеют базовые знания о микропроцессорах. Давайте подробнее рассмотрим микроконтроллеры. Первоначально микроконтроллер назывался однокристалльным микрокомпьютером. В настоящее время они широко используются практически во всех областях деятельности человека — от систем промышленной автоматизации до бытовой техники, от управления атомными электростанциями до детских игрушек, от секретных военных систем до переключения каналов в радиоустройствах.

Ключевые слова: микроконтроллер, процессор, периферийное устройство, автоматизация, память, дрон, датчик, компьютер, технология, модуль и магнит.

Abstract: Our rapidly developing era is not for nothing called the age of technology and engineering - at the heart of this development are microprocessors and microcontrollers.

Most of our readers have basic information about microprocessors. Let's get to know microcontrollers better. A microcontroller was originally called a single-crystal microcomputer. They are now widely used in almost all areas of human activity - from industrial automation systems to household appliances, from nuclear power plant control to children's toys, from secret military systems to changing channels in radio devices.

Keywords: microcontroller, processor, peripheral, automation, memory, drone, sensor, sensor, computer, technology, module and magnet.

Texnika va texnologiyalar asrida zamon juda tez rivojlanmoqda. Bu rivojlanishning markazida mikrokontroller turibdi.

Ushbu mikrokontroller (eski nomi - bitta kristalli mikro-kompyuter) hozirda barcha sohalarda keng foydalanilmoqda. Ushbu mikrokontrollerlar sanoat avtomatlashtirish tizimlaridan tortib to maishiy texnikagacha, atom elektr stansiyasini boshqarishdan tortib bolalar o‘yinchoqlarigacha, maxfiy harbiy tizimlardan tortib, radio qurilmalaridagi kanallarni o‘zgartirishgacha barcha sohalarga kirib keldi.

Mikrokontroller elektronkada eng ko‘p qo‘llaniladigan qurilmadir. Mikrokontrollerlar yuqori unumli protssessor, operativ va faqat o‘qish uchun mo‘ljallangan xotira hamda periferik qurilmalar to‘plamini yagona mikrosxema korpusiga birlashtirib, minimal xarajatlar bilan turli ob‘yektlar va jarayonlarni boshqarish tizimlarining keng doirasini amalga oshirish imkonini beradi. Mikrokontrollerlar ma‘lumotlarini kiritish/chiqarish uchun tizimli tashkil etish, buyruqlar to‘plami,

apparat va dasturiy vositalar ma'lumotlarni qayta ishlash muammolarini hal qilish uchun emas, balki qurilmalar, bloklar va avtomatlashtirish tizimlarida boshqarish va tartibga solish muammolarini hal qilish uchun mos keladi [1].



1- rasm. AVR, ARM, 8051 va PIC mikrokontrollerlari

1971-yilga kelib birinchi mikroprotsessorlar yaratildi – unda doimiy va tezkor xotira integratsiya qilinib, tashqi qurilmalarni ulash uchun kirish/chiqish portlari paydo bo'ldi. O'shandan beri mikrokontrollerlar va mikroprotsessorlarning rivojlanishi parallel ravishda davom etdi. Boshqarish tizimlarida kompyuterni avtomatlashtirish davri boshlandi.

Amerikaning elektronika mahsulotlarini ishlab chiqaruvchi Intel kompaniyasining asoschisi Gordon Mur mikroprotsessor texnologiyasining rivojlanish tendentsiyasini belgilovchi qonunni (Mur qonuni) ishlab chiqdi. Ushbu qonunga ko'ra, integral mikrosxemadagi tranzistorlar soni har ikki yilda ikki baravar ko'payadi, natijada hisoblash quvvati keskin oshadi va xarajatlar kamayadi.

Texnologik taraqqiyot va nisbatan past ishlab chiqarish xarajatlari mikrokontrollerlarning xilma-xilligini oshishiga olib keldi. Shuning uchun ular oddiy sxemalarda, masalan, multilovchi Led chiroqlarda, va murakkab boshqaruv tizimlarida, jumladan sanoatda, harbiy sohada, robototexnika va aqlli uy jihozlari keng qo'llanilib kelmoqda.

Hozirgi kunda eng ilg'or mikrokontrollerlar sifatida AVR, ARM va PIC (1 va 2 rasmlar) tan olingan. Ushbu mikrokontrollerlarga mashhur Arduino va Raspberry Pi platformalari asosida dastur yozish mumkin.[2].



2- rasm. Mikrokontrollerlar asosida qurilgan platalar

Mikrokontrollerlarni harbiy sohada qo'llanishi

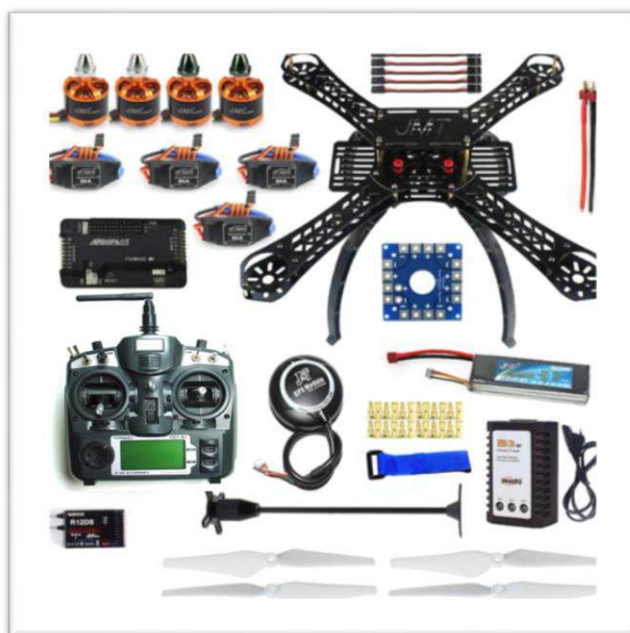
1. Uchuvchisiz uchish apparatlarida.

Bugungi kunda dronlar barcha sohalarda tobora kengroq qo'llanilmoqda. Harbiy, logistika, yetkazib berish, kinematografiya, baland tog'da suratga olish, poyga va boshqa ko'plab sohalarda o'z munosib o'rnini egalladi. Keling, uchuvchi dronning "miyasi" hisoblanmish mikrokontroller boshqaruvchisini ko'rib chiqamiz.

Uchuvchisiz uchish apparatlarda boshqaruvchi mikrokontroller – dronni boshqarish uchun mo'ljallangan qurilma (3- rasm). Bu boshqaruvchi mikrokontroller undagi o'rnatilgan tashqi qurilmalarni (motorlar, kamera, masofani o'lchash sensorlari va b.) maxsus yozilgan dasturiy ta'minot yordamida avtonom ravishda yoki yerdagi boshqaruv pulti yordamida masofadan turib boshqaradi. Masalan, sensorlardan olingan ma'lumotlarga asoslanib, boshqaruvchi motorlarning aylanish tezligini tartibga solgan holda parvozni nazorat qiladi [3].



3- rasm. Uchuvchisiz uchish apparati va uning ichidagi mikrosxema



4- rasm. Uchuvchisiz uchish apparatini ichki qismlarini yoyilgan holdagi ko'rinishi

Mergan o'q-otar qurolining optik moslamasi.

Hozirda rivojlangan mamlakatlar armiyalarida merganlarning o'q-otar quroli uchun optik mikrokontroller qo'llanilgan elektron optik moslamalar paydo bo'ldi. Ushbu qurilmalarda juda ko'plab qo'shimcha imkoniyatlar qo'shilgan. Masalan, ob-havo, GPS, masofani aniqlash kabi

optsiyalar integratsiya qilingan holda, boshqa qurilmalari (kontur yoritgichlari, kunduzi va kechasi, kuchli tuman sharoitidagi ishlash moslamalari) bilan mergan o'q-otar qurolining juhozlanishi boyitilgan.

Bunday qurilmalar endi nafaqat ATN korporatsiyasi kabi taniqli bozor yetakchilari tomonidan balki, Xitoyning iRay kompaniyasi tomonidan ham ishlab chiqarila boshladi. Ammo bunday qurilmalarning narxi yuqori bo'lganligi sababli, uni sotib olishga hammaning ham qurbi yetmaydi [4].

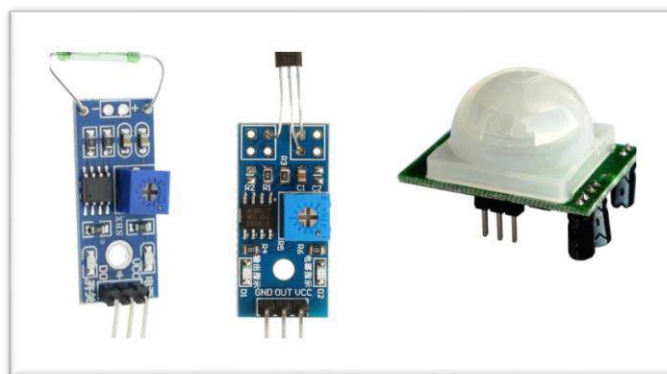


5- rasm. Ko'p funktsiyali elektron ko'rish moslamasi

Qo'riqlash tizimlarida foydalaniladigan datchik va sensorlar.

Oldingi zamonlarda biror-bir joyni qo'riqlash zarur bo'lsa, o'sha joyga qorovul qo'yilardi. Qo'riqlashning texnik vositalari paydo bo'lgach, bunga deyarli ehtiyoj qolmadi. Turli obyektlarni, ayniqsa Davlat chegaralarini qo'riqlash tizimlarida mikrokontrollerlarning qo'llanilishi esa qo'riqlashning texnik vositalari va tizimlarining imkoniyatlarini karrasiga oshirib yubordi. Hozirgi kunda "Aqlli uy" kontseptsiyasi ham aynan mana shunday tizimlarga asoslangan.

Ixtiyoriy hududga o'rnatilgan signalizatsiya 24/7 rejimida hududning tashqi chegaralarini yoki binolardan chiqish/kirish joylarini nurlar yoki sensorlar yordamida kuzatishni ta'minlaydi. Nur uzilib qolganda yoki kabel zarbaga ta'sir qilganda, operatorga himoyalangan obyektga ruxsatsiz kirish haqida signal kelib tushadi. Ushbu vazifalarni bajarish uchun juda ko'p datchik va sensorlardan foydalaniladi (6- rasm).



6- rasm. Chapdan – Gerkon, Hall va harakat datchik(sensor)lari

Sensor qurilmasi juda oddiy, u inert gaz yoki vakumli kolbadagi ikkita ochiq yoki yopiq kontaktlardan iborat. Magnit yaqinlashganda kontaktlar o'z holatini o'zgartiradi va modul chiqishida past kuchlanish darajasi paydo bo'ladi [5]. Ishda magnit yaqinlashganda, kontaktlar yopilganda, odatda ochiq gerkon ko'rsatilgan, modulning o'zi quvvat mavjudligini va sensorning ishlashini anglatadi.

Oddiy Hall datchiklari [6], bu qattiq holatda bo'lgan qurilmalar bo'lib, ularga qo'llaniladigan magnit maydonga mutanosib elektr signallarini hosil qiladi. Keyinchalik, ushbu elektr signallari kerakli chiqishni ishlab chiqarish uchun foydalanuvchining maxsus elektron sxemasi tomonidan qayta ishlanadi. Bugungi kunda ushbu magnit sensorlar magnit maydonlarining keng doirasiga javob berishga qodir. Bunday magnit sensorlardan biri Hall sensori bo'lib, uning chiqishi (kuchlanish) magnit maydonning zichligiga bog'liq.

Keling, aqlli uy xavfsizligi bilan bog'liq boshqa sensorni ko'rib chiqaylik. Bu HC-SR501 harakat sensori moduli bo'lib, u PIR sensorining o'zi (Pyroelektrik (passiv) infraqizil sensor) va boshqaruv sxemasidan iborat. Bunday sensorlar ko'pincha xavfsizlik tizimlarida va kundalik hayotda xonadagi harakatni aniqlash uchun ishlatiladi. Modulda ikkita o'zgaruvchan rezistor va rejimni sozlash uchun o'tish moslamasi mavjud. U odatda passiv holatda bo'ladi. Chunki harakatni aniqlash uchun jismlarning o'zlari chiqaradigan energiyadan boshqa hech qanday qo'shimcha energiya ishlatilmaydi. Modulning boshqaruv mikrosxemasi ikkala elementning signallaridagi o'zgarishlarni qayd qiladi va ularning o'zgarishi xarakteridan kelib chiqib, infraqizil signallarni (tirik organizmlar) chiqaradigan ob'ektlarning harakatini aniqlaydi.

Xulosa sifatida shuni aytish mumkinki, mikrokontrollerlar insoniyat faoliyatining barcha sohalarida qo'llanilib, ular inson hayotining ajralmas bir qismiga aylanib bormoqda desak mubolag'a bo'lmaydi. Hozirgi zamonni mikrokontroller qurilmalarisiz tasavvur qilish qiyin.

Mikrokontrollerni dasturlash orqali ko'plab amaliy apparat muammolarini hal qilish mumkin. Biz mikrokontrollerni (MK) bitta mikrosxemada joylashgan kompyuter deb hisoblashimiz ham mumkin. Uning asosiy jozibali fazilatlarini – o'lchamining kichikligi, ishlash tezligining yuqoriligi, ishonchlilligi va turli xil vazifalarni bajarishga moslashish qobiliyati.

Mikrokontroller unga qo'yilgan vazifalarni ketma-ket bajarilishini ta'minlaydigan tizimdir hamda u fan va texnikada inqilobiy o'zgarishlarga katta hissa qo'shmoqda.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

- [1] <https://eduherald.ru/ru/article/view?id=21077>
- [2] https://supereyes.ru/articles/arduino-i-robototekhnika/primeneniemikrokontrollerov/?srltid=AfmBOoqsLU18MMLRYO7TaYz-sW8apfkSjKi_9Mefw2zAQ1murC6tVDMk
- [3] <https://habr.com/ru/companies/leader-id/articles/491770/>
- [4] <https://dzen.ru/a/YuORLACqfXz1Jkzq>
- [5] А.С. Применение оптоволоконных и термочувствительных элементов в системах охранной и пожарной сигнализации / А.С. Козлов, Р.Я. Лабковская, В.Л. Ткалич, О.И. Пирожникова // Известия высших учебных заведений. Приборостроение. — 2018. — №4. — С. 356-359. [Электронный ресурс]. — Режим доступа: <https://cyberleninka.ru/article/n/primeneniyeoptovolonnyh-i-termochuvstvityelnyh-elementov-v-sistemah-ohrannoy-ipozharnoy-signalizatsii> (дата обращения: 20.12.19)
- [6] Gartener: Seven cloud-computing security risks. InfoWorld.2008-07-02. <http://www.infoworld.com/d/security-central/gartener-seven-cloud-computing-security-risks-853>.
- [7] Data Remanence, https://en.wikipedia.org/wiki/Data_remanence.
- [8] Rijndael.Advanced Encryption Standard (AES). FIPS. November 23, 2001. <http://csrc.nist.gov/publications/fips/fips197/fips197.pdf>
- [9] Бакытбек Е.Б. Датчики для измерения слабых магнитных полей // Наука и образование сегодня. — 2016. — №4(5). — С. 30-31. [Электронный ресурс]
- [10] [://habr.com/ru/articles/137987/](https://habr.com/ru/articles/137987/).

БАНК ВА ТЎЛОВ ТИЗИМЛАРИДА БАНК КАРТАЛАРИ БИЛАН БОҒЛИҚ ФИРИБГАРЛИК ХОЛАТЛАРИНИ ОЛДИНИ ОЛИШДА АНТИФРОД ТИЗИМЛАРИНИ ҚЎЛЛАНИЛИШИ

О.О. ТАЛИПОВ

Ўзбекистон Республикаси Марказий банки “Ахборотлаштириш Бош маркази” ДУК

Аннотация. Банк ва тўлов тизимларида замонавий ахборот коммуникация технологияларини қўллаган ҳолда мижозларга банк ва тўлов хизматларни кенг қўламда тақдим этиб келмоқда. Шу билан бирга, мижозларга масофадан банк ва тўлов хизматларини кўрсатишда фирибгарлар томонидан фуқароларнинг ишончига кирган ҳолда, банк карталари билан боғлиқ шубҳали фрод операцияларни амалга ошириш ҳолатлари кундан кунга ошиб бормоқда. Бу ўз навбатида фирибгарлик ҳолатларини олдини олиш масаласини долзарб муаммога айлантирмоқда. Молиявий муассасалар ва тўлов тизимлари фойдаланувчиларнинг маълумотларини ҳимоя қилиш ва маблағларини хавфсизлигини таъминлаш учун замонавий антифрод тизимларидан фойдаланиш зарурияти ортиб бормоқда.

Калит сўзлар: Фирибгарлик, фрод операциялар, кибержсиноят, антифрод, транзакцион ва сессион антифрод.

Аннотация. Банковские и платежные системы предоставляют клиентам широкий спектр банковских и платежных услуг с использованием современных информационно-коммуникационных технологий. При этом при предоставлении клиентам услуг дистанционного банковского обслуживания и платежных услуг с каждым днем увеличивается число случаев злоупотребления доверием граждан и совершения подозрительных мошеннических операций с банковскими картами. Это, в свою очередь, делает вопрос предотвращения мошенничества актуальным. Финансовые организации и платежные системы все чаще сталкиваются с необходимостью использования современных систем противодействия мошенничеству для защиты данных пользователей и обеспечения безопасности их средств.

Ключевые слова: Мошенничество, фрод операции, киберпреступность, антифрод (противодействие мошенничеству), транзакционное и сеансовое противодействие мошенничеству.

Рақамли технологияларини ривожланиши давлат органлари ва идораларининг ахборот тизимлари ва ресурсларини замон талабларига мувофиқ замонавий ахборот коммуникация технологияларини қўллаш зарурлигини кўрсатмоқда.

Бунинг асосий мақсадлардан бири бўлиб, давлат органлари ва идораларининг ахборот тизимлари ва ресурслари ҳамда муҳим ахборот инфраттузилма объектларининг ахборот хавфсизлиги ва киберхавфсизлиги таъминлашдан иборат.

Халқаро тажриба шундан далолат бермоқдаки, банк карталари билан боғлиқ фирибгарлик ҳолатларини олдини олиш ва аниқлашда сунъий интеллект (AI) ҳамда машинали ўрганиш (ML) технологияларидан самарали фойдаланиш тенденцияси жаҳонда кенг тарқалмоқда. Ушбу соҳада олиб борилган илмий тадқиқотлардан бири - Hafez ва ҳаммуаллифларининг (2025) “A systematic review of AI-enhanced techniques in credit card fraud detection” номли илмий мақоласидир. Унда 2019–2024 йиллар давомида турли давлатларда тижорат банклари ва молия институтлари томонидан жорий қилинган антифрод ечимлари таҳлил қилинган.

Мазкур тадқиқотда муаллифлар сунъий интеллект асосидаги бир қатор усуллар - Random Forest, Gradient Boosting, Deep Neural Networks (чуқур нейрон тармоқлар), Convolutional Neural Networks (конволюцион тармоқлар), Autoencoders ва XGBoost каби алгоритмларни таққослаб таҳлил қилишган. Улардан айримлари маълумотларни қайта

ишлаш ва аномал транзакцияларни аниқлашда жуда юқори аниқлик кўрсатган. Мақолада, хусусан, реал вақтда фаолият юритувчи антифрод тизимлари - фаол кузатув ва тезкор блоклаш имкониятларига эга платформаларнинг самарадорлиги алоҳида таъкидланган.

Тадқиқот натижаларига кўра, банкларда қўлланилаётган анъанавий қоидаларга асосланган антифрод механизмларининг самарадорлиги чекланган бўлиб, улар тез ўзгарувчи ва мураккаб бўлган фирибгарлик схемаларини аниқлашда етарли эмас. Шу сабабли, машинали ўрганишга асосланган адаптив антифрод ечимлари ҳозирги кунда долзарб аҳамият касб этмоқда.

Бундай ёндашувлар, Ўзбекистон банк тизимида ҳам антифрод тизимларини такомиллаштириш ва замонавий технологик асосда шакллантириш зарурлигини кўрсатади. Жумладан, реал вақтда транзакцияларни таҳлил қилувчи, шубҳали фаолиятларни динамик идентификация қилувчи, фойдаланувчи ҳаракатларини таҳлил қилувчи (session behaviour) ва курилма маълумотларини қиёслайдиган антифрод тизимлар фаолиятини сунъий интеллект воситасида янада самарали йўлга қўйиш имкони яратилади.

Охирги йилларда транзакциялар ва фойдаланувчилар ўртасидаги кўп қиррали алоқаларни ҳисобга оладиган янги моделлар ишлаб чиқилмоқда. Бунда банк мижозлари, терминаллар, ҳисобварақлар, курилмалар ва бошқа элементлар орасидаги алоқалар маълумотлар графига орқали ифодаланади. Мазкур ёндашув маълумотлар тузилишидаги алоқаларни чуқур таҳлил қилиш имконини бериб, фирибгарлик схемаларини эрта босқичда аниқлашда самарали ҳисобланади.

Шу билан бирга, мижозларга масофадан банк ва тўлов хизматларини кўрсатишда фирибгарлар томонидан фуқароларнинг ишончига кирган ҳолда, банк карталари билан боғлиқ шубҳали фрод операцияларни амалга ошириш ҳолатлари кундан кунга ошиб бормоқда. Бу ўз навбатида фирибгарлик ҳолатларини олдини олиш масаласини долзарб муаммога айлантирмоқда.

Ижтимоий тармоқларнинг жадал ривожланиши натижасида фуқаролар ўзларининг рақамли кўринишларини яратган. Бунда, фуқаролар ўзларига тегишли бўлган маълумотларни тўлиқ яратиб бормоқдалар. Жумладан, фуқаронинг тўлиқ исми, фамилияси, туғилган йили, таълим муассасалари, иш жойи, шахсий расмлар ва бошқа маълумотлари киритилган.

Фирибгарлар ижтимоий тармоқлардан фуқароларнинг шахсий маълумотларидан фойдаланган ҳолда уларни ўрганиб чиқиб, уларга телефон

ёки интернет орқали алоқага чиқиб, фуқароларнинг мобил курилмаларига зарар келтирувчи иловаларни ўрнатиш, сохта ҳужжатларни тақдим этган ҳолда уларнинг банк карта маълумотларини қўлган киритиб, уларнинг пул маблағларини ўғирлаш ҳолатлари ортиб бормоқда.

Бунда жабрланувчи шахслар фирибгарларнинг турли кўринишдаги алдовларига ишонган ҳолда ўзларига тегишли бўлган маълумотларни тақдим этади ҳамда мобил курилмаларини масофадан бошқариш имкониятини берувчи дастурий воситаларни ўрнатиб берадилар.

Шу каби ҳолатларнинг юзага келишининг асосий сабабларидан бири бу фуқароларнинг ишонувчанлиги ҳамда ҳуқуқий ва молиявий саводхонлигининг камлигидан юзага келмоқда.

Ўзбекистон Республикаси Ички ишлар вазирлигининг ҳуқуқбузарликларни олдини олиш ва уларнинг профилактикаси бўйича 2024 йилда амалга оширилган ишлар ҳолати тўғрисидаги ахборотида кўра, киберхавфсизлик йўналишида 58 800 та жиноятлар содир этилган бўлиб, уларнинг 97,7 фоизи (57 480 та) фуқароларнинг банк карталаридаги пул маблағларини қўлга киритиш билан боғлиқдир. Шунингдек, электрон тўлов тизимлари орқали содир этилган жиноятларнинг 28,3 фоизи (16 269 таси) сохта ҳаволалар юбориш орқали тасдиқловчи кодни қўлга киритиб, карта бошқарувини эгаллаш йўли билан, 8,7 фоизи (5 123 таси) онлайн савдо платформаларида турли алдовлар билан товарлар учун тўловни олдиндан амалга оширишга эришиш орқали, 5,5 фоизи (3 191 таси) телефон қўнғироқлари

орқали банк карта бошқарувини тасдиқловчи кодни қўлга киритиш йўли билан содир этилган.

Мамлакатимизда сўнгги беш йилликда кибержиноятлар 68 баравар, биргина ўтган йилда эса 2023 йилдагига нисбатан 9,1 баравар ошган. Ушбу даврда кибермакондаги ҳуқуқбузарликлар юзасидан жисмоний ва юридик шахслардан келиб тушаётган мурожаатлар сони 34 баравар кўпайган.

Мазкур жиноятлар натижасида фуқароларнинг 1 трлн 909 млрд сўмдан ортиқ маблағи талон-тарож қилинган.

Кибержиноятлар асосан қуйидаги усулларда содир этилмоқда:

- 60 фоизи зарарли ҳаволалар ва дастурлар юбориш орқали банк картаси ёки мобил қурилма бошқарувини қўлга киритиш йўли билан;
- 16 фоизи турли алдовлар билан банк картаси ҳамда мобил иловалардаги аккаунтлар бошқарувини тасдиқловчи SMS кодни қўлга киритиш йўли билан;
- 4 фоизи шахс номига онлайн кредит расмийлаштириш орқали;
- 11 фоизи онлайн савдо платформаларидаги фирибгарликлар орқали;
- 9 фоизи турли усулдаги фирибгарлик схемалари орқали фуқароларнинг пул маблағларини жалб қилиш тарзида содир этилмоқда.

Ҳозирда банк карталаридан фойдаланиш билан боғлиқ фирибгарлик жиноятини содир этиш ҳолати ва усулига қараб, Ўзбекистон Республикаси Жиноят кодексининг 168-моддаси 2-қисми “в” бандига асосан компьютер техникаси воситаларидан фойдаланиб содир этилганда ушбу норма билан квалификация қилинади.

Банк карталаридан фойдаланиш билан боғлиқ фирибгарлик жинояти фош этилиши жуда қийин бўлган жиноятлардан бири бўлиб, пухта режалаштирилганлиги, ўта мураккаблиги ҳамда трансчегаравий хусусиятга эгаллиги билан бошқа турдаги жиноятлардан фарқ қилади.

Ушбу фирибгарлик ҳолати ҳалқаро тажрибага асосан, фрод (fraud – инглизча сўз бўлиб, “фирибгарлик”) дегани. Шунингдек, ҳалқаро тажриба кўра, банк ва молия соҳасида юзага келадиган фирибгарлик ҳолатларини олдини олишда антифрод тизимларидан кенг фойдаланилади. Жумладан, ҳозирда ривожланган давлатларда AML антифрод (яъни транзакцион) тизимларидан кенг фойдаланилади.

Интернет тармоғидаги фирибгарлик ҳолатлари бўйича Нигерия, АҚШ, Хиндистон, Хитой, Буюк Британия, Россия, Бразилия, Жанубий Африка, Рунимия ҳамда Канада давлатларида қайд этилган.

1-жадвал

Интернет-фирибгарлик: энг кўп кузатилган ҳолат 10 давлат таҳлили

Рейтинг	Давлатлар	Тарқалган фирибгарликлар	Тахминий йиллик зарарлар (млн АҚШ доллари)
1	Нигерия	Олдиндан тўлов қилиш (аванс) ҳамда романтик фирибгарлик	\$200
2	АҚШ	Фишинг ва лотерея билан боғлиқ фирибгарлик	\$180
3	Хиндистон	Техник қўллаб-қувватлаш ҳамда лотерея билан боғлиқ фирибгарлик	\$160
4	Хитой	Қалбаки маҳсулотлар ва инвестиция киритиш билан боғлиқ фирибгарлик	\$140
5	Буюк Британия	Фишинг ва ишга жойлашиш бўйича фирибгарлик	\$120
6	Россия	Банк карталари билан боғлиқ фирибгарлик ҳамда хакерлик	\$100
7	Бразилия	Банк троянлари ва фишинг	\$80
8	Жанубий Африка	Инвестиция киритиш ҳамда кредит бериш билан боғлиқ фирибгарлик	\$70
9	Рунимия	Аукцион ва банк карталари билан боғлиқ фирибгарлик	\$60
10	Канада	Лотерея ҳамда шахсга доир маълумотларни ўғирлаш	\$50

Дунё тажрибасида, чуқур ўрганувчи нейрон тармоқлар (Deep Learning) ва диққат механизмларидан (Attention Mechanisms) фойдаланган ҳолда банк карталари билан боғлиқ шубҳали операцияларни аниқлаш соҳасида жиддий ютуқларга эришилмоқда. Хусусан, транзакциялар кетма-кетлигини таҳлил қилишга мўлжалланган моделлар маълумотлар орасидаги узоқ муддатли боғланишларни аниқлаб, фрод ҳолатларни вақтида аниқлаш имконини беради. Бу каби ёндашувлар маълумотларни қайта ишлаш самарадорлигини сезиларли даражада ошириб, нотўғри фаолиятларни аниқлашда юқори аниқликка эга экани билан ажралиб туради.

Турли усуллар ва сунъий интеллект моделларини бирлаштирувчи махсус интеграцияланган тизимлар (ансамбл усуллари) антифрод соҳасида юқори натижаларни кўрсатмоқда. Бундай тизимлар диққат механизмлари орқали фаолиятнинг энг муҳим жиҳатларини автоматик равишда ажратиб олиш имконини беради ва шубҳали транзакцияларни аниқлашда юқори аниқликка эришади. Шунингдек, бундай моделларни маълумотлар оқимида мослаштириш ва реал вақтда таҳлил қилиш имконияти уларни банк ва тўлов тизимлари учун жуда самарали ва долзарб ечимга айлантирмоқда.

Ўзбекистон Республикаси Президентининг 2023 йил 30 ноябрдаги ПҚ-381-сонли “Рақамли маҳсулотлар (хизматлар) истеъмолчилари ҳуқуқларини ҳимоя қилиш ва рақамли технологиялар воситасида содир этиладиган ҳуқуқбузарликларга қарши курашишни кучайтириш чоралари тўғрисида”ги қарори билан тасдиқланган “Йўл харитаси”нинг 4-бандига кўра, банклар, тўлов тизими операторлари ва тўлов ташкилотларида антифрод тизимларини жорий этиш белгиланган. Унга кўра, тўлов тизими операторларида транзакцион антифрод тизимини ҳамда банклар ва тўлов ташкилотларида сессион антифрод тизимларидан фойдаланиш учун Марказий банкда марказлашган антифрод тизимини жорий этилиши қайд этилган.

Транзакцион антифрод тизими – банк ва тўлов тизимларида пул маблағларига чекловларни ўрнатиш, катта миқдордаги пул маблағларини ҳамда шубҳали (фрод) амалиётларда иштирок этган мижозларни аниқлаш ва тўловларни ўтказилишини чеклашни таъминлайди.

Сессион антифрод тизими – фойдаланувчининг ҳаракатлари, рақамли бармоқ излари, интернет тармоғига уланиши, браузер соғламалари, фойдаланувчи аккунтига бошқа қурилмадан кириш, эмуляторлар ҳамда қўлда ёзилган скриптларни аниқлаш ва бошқа кўплаб техник маълумотларини умумлаштиради.

Телеком антифрод тизими – банк ва тўлов ташкилотлари мобил иловаларида ўрнатилгач, телефон қурилмасининг ўзига хос идентификация кодларини автоматик аниқлаш орқали фойдаланувчига СМС-хабар тарзида юборилган бир марталик тасдиқлаш коди (ОТР) фақатгина унинг телефон қурилмасида амал қилишини таъминлайди.

Марказлашган антифрод тизими – барча банк ва тўлов тизимлари ҳамда тўлов тизими операторларининг антифрод тизимлари маълумотларини йиғади, таҳлил қилади, сунний интеллект функцияларига эга бўлиб, фирибгарлик ҳолатлари бўйича таълилий маълумотларни эгасизлантирган ҳолда банк ва тўлов тизими иштирокчиларига тақдим этади.

Банк карталари билан боғлиқ шубҳали фрод операцияларини аниқлаш ҳамда уларни олдини олиш мақсадида Ўзбекистон Республикаси Марказий банкида Марказлашган антифрод тизими тест-синов тарзида жорий қилинди. Мазкур тизимга ҳозирги кунда 34 та банк ва 5 та тўлов ташкилоти уланган.

Банк ва тўлов тизимларида антифрод тизимларини ҳамда Марказий банкда Марказлашган антифрод тизимини жорий этилиши натижасида 2024 йил давомида 472 та банк карталари билан боғлиқ фирибгарлик ҳолатида 9,5 млрд сўм миқдоридаги пул маблағлари блокранишига эришилган.

Банк ва тўлов тизимларида юзага келадиган фирибгарлик ҳолатларини олдини олишда қуйидаги ишларни амалга ошириш мақсадга мувофиқ. Яъни:

1. Барча банклар, тўлов ташкилотларида сессион ҳамда телеком антифрод тизимларини жорий этиш ҳамда Марказий банкнинг Марказлашган антифрод тизимига интеграция қилиш.

2. Ҳуқуқни муҳофаза қилувчи органлар фуқаролар томонидан банк карталари билан боғлиқ фирибгарлик ҳолатлари бўйича келиб тушадиган мурожаатлар бўйича Марказий банк билан маълумот алмашинувини йўлга қўйиш.

3. Фуқароларнинг ҳуқуқий, молиявий саводхонлигини ҳамда уларнинг кибермаданиятини ошириш юзасидан ижтимоий тармоқларда, оммавий-ахборот воситалари тарғибот ишларини кенг қўламда тизимли равишда амалга ошириш.

Хулоса

Банк карталари билан боғлиқ фирибгарлик ҳолатларини олдини олишда антифрод тизимлари муҳим аҳамиятга эга. Замонавий технологияларнинг ривожланиши билан бу тизимлар кун сайин мукамаллашиб, янги фирибгарлик усуллариға қарши самарали курашиш имкониятларини яратади. Бироқ, муваффақиятли натижага эришиш учун технологик ечимлар билан бирга фойдаланувчилар ҳуқуқий, молиявий ва кибермаданиятини ошириш ҳамда тегишли идоралар ва банклараро ҳамкорлик такомиллаштириш зарур.

Келажақда сунъий интеллект ва машина ўрганиши технологияларининг янада кенг қўлланилиши ва банклараро маълумотлар алмашинуви тизимининг ривожланиши антифрод тизимларининг самарадорлигини сезиларли даражада оширади.

Фойдаланилган адабиётлар рўйхати:

[1] Hafez, I. Y., Hafez, A. Y., Saleh, A., Abd El-Mageed, A. A., & Abohany, A. A. (2025). A systematic review of AI-enhanced techniques in credit card fraud detection. *Journal of Big Data*, 12, Article 6. <https://journalofbigdata.springeropen.com/articles/10.1186/s40537-024-01048-8>

[2] Sha, Q., Tang, T., Du, X., Liu, J., Wang, Y., & Sheng, Y. (2025). Detecting Credit Card Fraud via Heterogeneous Graph Neural Networks with Graph Attention. *arXiv preprint*. <https://arxiv.org/pdf/2504.08183>

[3] Ўзбекистон Республикаси Ички ишлар вазирлиги. Ички ишлар вазирлиги фаолиятига оид ҳисоботлар. Ҳукумат портали. Қўлланилди: 12.07.2025. Манба: <https://gov.uz/uz/iiv/pages/ichki-ishlar-vazirligi-faoliyatiga-oid-hisobotlar>

[4] Ўзбекистон Республикаси Ички ишлар вазирлиги. (2024, 22 январь). 2023 йил якунлари ва 2024 йилдаги устувор вазифаларга бағишланган йиғилиш. Ҳукумат портали. Қўлланилди: 12.07.2025. Манба: <https://gov.uz/uz/iiv/news/view/57775>

[5] Fineproxy.org таҳририяти. (2023). Интернет-фирибгарлик: энг кўп кузатилган ҳолат 10 давлат таҳлили. Интернет наشري. Қўлланилди: 12.07.2025. Манба: <https://fineproxy.org/ru/the-top-10-internet-scamming-countries-a-deep-dive-into-the-world-of-online-fraud>

[6] Benchaji, I., Douzi, S., El Ouahidi, B., & Jaafari, J. (2021). Enhanced credit card fraud detection based on attention mechanism and LSTM deep model. *Journal of Big Data*, 8, Article 151. <https://journalofbigdata.springeropen.com/articles/10.1186/s40537-021-00541-8>

[7] Hosseini Chagahi, M., Delfan, N., Dashtaki, S. M., Moshiri, B., & Piran, M. J. (2024). An Innovative Attention-based Ensemble System for Credit Card Fraud Detection. *ResearchGate*. https://www.researchgate.net/publication/384929834_An_Innovative_Attention-based_Ensemble_System_for_Credit_Card_Fraud_Detection

[8] Ўзбекистон Республикаси. (2024). Ўзбекистон Республикасининг Жиноят кодекси (янги таҳрир). Lex.uz – Норматив-ҳуқуқий ҳужжатлар миллий базаси. Қабул қилинган сана: 14.03.2024. Қўлланилди: 12.07.2025. Манба: <https://lex.uz/docs/6681111>

[9] Ўзбекистон Республикаси Олий Мажлиси Сенати. (2025, 26 июнь). Сенатнинг саккизинчи ялпи мажлиси. Банк карталари билан боғлиқ жиноятлар муҳокамаси [Видеомажлис]. YouTube. Қўлланилди: 12.07.2025. Манба: https://www.youtube.com/watch?v=iWWecuWqs_E

SUN'IIY INTELLEKT TEXNOLOGIYALARINING IJTIMOIIY SOHALARNI RIVOJLANTIRISHDA TUTGAN O'RNI

D.N. XOLMURODOV

O'R Strategik tahlil va istiqbolni belgilash oliy maktabi

Annotatsiya. So'nggi yillarda sun'iy intellekt (SI) texnologiyalari jamiyat hayotiga jadallik bilan kirib kelmoqda. Ayniqsa ijtimoiy sektorning eng ko'p fuqarolarini band qilgan tibbiyot, ta'lim, bandlik va boshqa shu kabilarda SI texnologiyalarining samarali xorijiy na'munalari haqidagi ma'lumotlarni internet tarmoqlarida uchratishimiz mumkin. Mazkur maqolada O'zbekistonda ijtimoiy sohalarni rivojlantirish jarayonida sun'iy intellekt texnologiyalarining roli va ahamiyati tahlil qilinadi. Unda SI texnologiyalarining sog'liqni saqlash, ta'lim, ijtimoiy himoya va davlat boshqaruvi sohasidagi qo'llanilish imkoniyatlari, afzalliklari hamda mavjud muammolar ko'rib chiqilgan. Muallif O'zbekistonning "Raqamli O'zbekiston – 2030" va "2030-yilgacha sun'iy intellekt texnologiyalarini rivojlantirish strategiyasi" kabi hujjatlar asosida belgilangan maqsadlarini sharhlab, SI integratsiyasi uchun mavjud infratuzilma, inson kapitali va huquqiy bazaning holatini baholaydi. Shuningdek, maqolada SI texnologiyalarini joriy qilishdagi tahdidlar, jumladan, infratuzilma yetishmovchiligi, axloqiy va huquqiy muammolar, algoritmik tarfakashlik va ish o'rinlari qisqarishi kabi xavf-xatarlar ham yoritilgan. Shu bilan birga muallif tomonidan O'zbekistonda SI ni samarali joriy etish bo'yicha qator strategik tavsiyalar ham berib o'tilgan.

Kalit so'zlar: sun'iy intellekt (SI), ijtimoiy soha, sog'liqni saqlash, ta'lim tizimi, ijtimoiy himoya, davlat boshqaruvi, raqamli transformatsiya, axloqiy masalalar, algoritmik tarfakashlik, raqamli infratuzilma, ma'lumotlar ekotizimi, inson kapitali, xalqaro hamkorlik, elektron hukumat, pilot loyihalar, innovatsiya, huquqiy asoslar.

Аннотация. В последние годы технологии искусственного интеллекта (ИИ) стремительно входят в жизнь общества. В частности, в сети Интернет мы можем найти информацию об эффективных зарубежных образцах технологий ИИ в медицине, образовании, занятости и других областях, которые обеспечивают наибольшую занятость граждан социального сектора. В данной статье анализируется роль и значение технологий искусственного интеллекта в процессе развития социальных сфер в Узбекистане. В нем рассматриваются возможности, преимущества и существующие проблемы применения технологий ИИ в здравоохранении, образовании, социальной защите и государственном управлении. Автором проекта "Цифровой Узбекистан – 2030" и "Стратегия развития технологий искусственного интеллекта до 2030 года", оценивает состояние существующей инфраструктуры, человеческого капитала и правовой базы для интеграции ИИ. В статье также рассматриваются угрозы внедрения технологий искусственного интеллекта, включая нехватку инфраструктуры, этические и правовые проблемы, алгоритмическую предвзятость и сокращение рабочих мест, также освещены риски. Вместе с тем, автором также представлен ряд стратегических рекомендаций по эффективному внедрению ИИ в Узбекистане.

Ключевые слова: искусственный интеллект (ИИ), социальная сфера, здравоохранение, система образования, социальная защита, государственное управление, цифровая трансформация, этические вопросы, алгоритмическая предвзятость, цифровая инфраструктура, экосистема данных, человеческий капитал, международное сотрудничество, электронное правительство, пилотные проекты, инновации, правовые основы.

Abstract. In recent years, artificial intelligence (AI) technologies have been rapidly entering the life of society. We can find information on the Internet about effective foreign examples of AI technologies, especially in medicine, education, employment, etc., which employ the largest number of citizens in the social sector. This article analyzes the role and importance of artificial

intelligence technologies in the development of social spheres in Uzbekistan. It examines the possibilities, advantages, and existing problems of using AI technologies in the fields of healthcare, education, social protection, and public administration. By the author of Uzbekistan's "Digital Uzbekistan – 2030" and "Strategy for the Development of Artificial Intelligence Technologies until 2030" and assesses the state of the existing infrastructure, human capital, and legal framework for the integration of AI. The article also addresses threats to the implementation of AI technologies, including infrastructure shortages, ethical and legal issues, algorithmic bias, and job losses. These risks are also highlighted. Additionally, the author provides a number of strategic recommendations for the effective implementation of AI in Uzbekistan.

Keywords: artificial intelligence (AI), social sphere, healthcare, education system, social protection, public administration, digital transformation, ethical issues, algorithmic bias, digital infrastructure, data ecosystem, human capital, international cooperation, e-government, pilot projects, innovation, legal framework.

Bugungi kunda sun'iy intellekt (SI) ijtimoiy soha, jumladan, jamiyat hayotining barcha jabhalariga kirib borayotgan kuchli o'zgartiruvchi kuchga aylanmoqda. Jahon tajribasi shuni ko'rsatadiki, SI texnologiyalari sog'liqni saqlash, ta'lim, ijtimoiy himoya va davlat boshqaruvi kabi sohalarda jarayonlarni optimallashtirish, samaradorlikni oshirish va xizmatlar sifatini yaxshilash uchun katta salohiyatga ega. Raqamli transformatsiyaga faol intilayotgan O'zbekiston ham ilg'or texnologiyalarni, shu jumladan, SI ni rivojlantirish va joriy etishga ustuvor ahamiyat bermoqda. "Raqamli O'zbekiston – 2030" va "2030 yilgacha sun'iy intellekt texnologiyalarini rivojlantirish strategiyasi" kabi strategik hujjatlar iqtisodiyot va ijtimoiy sohaning turli tarmoqlariga SI ni integratsiya qilish bo'yicha aniq maqsad va vazifalarni belgilaydi.

O'zbekiston ijtimoiy sohasilarining umumiy tavsifi. O'zbekistonning ijtimoiy sohasi bir qator asosiy yo'nalishlarni o'z ichiga oladi, ularning har biri aholi farovonligini ta'minlashda muhim rol o'ynaydi.

O'zbekiston sog'liqni saqlash tizimi bir qator muammolarga duch kelmoqda, jumladan, malakali tibbiy xodimlarning yetishmasligi, ayniqsa, olis hududlarda, ixtisoslashgan tibbiy yordamga cheklanganligi va ayrim kasalliklarning tarqalganligi oshib bormoqda [1]. Hukumat sog'liqni saqlash tizimini isloh qilish bo'yicha faol sa'y-harakatlarni amalga oshirmoqda. Bu sa'y-harakatlar tibbiy xizmatlar sifatini va ulardan foydalanish imkoniyatini oshirishga, davolashning yangi standartlarini joriy etishga, tibbiy muassasalarning moddiy-texnik bazasini mustahkamlashga va birlamchi tibbiy-sanitariya yordamini rivojlantirishga qaratilgan [2]. Erishilgan iqtisodiy o'sishga qaramay, sog'liqni saqlash sohasida muammolar saqlanib qolmoqda, bu esa tibbiy yordam samaradorligi va sifatini oshirish maqsadida SI ni qo'llash uchun potentsial sohalarni yaratadi.

O'zbekiston ta'lim tizimi aholining savodxonlik darajasini oshirishga va iqtisodiyotning turli tarmoqlari uchun malakali kadrlar tayyorlashga yo'naltirilgan. Asosiy ustuvorliklar raqamli savodxonlikni va axborot texnologiyalari sohasidagi ko'nikmalarni rivojlantirishdan iborat.

Ushbu sohadagi muhim loyihalardan biri yoshlarga dasturlash asoslari va IT mutaxassisliklari bo'yicha bepul ta'lim berishga qaratilgan "Bir million o'zbek dasturchisi" dasturidir [3]. Raqamli ko'nikmalarni rivojlantirishga e'tibor qaratilishi ta'lim jarayonida va ushbu sohada mutaxassislar tayyorlashda SI texnologiyalarini kelgusida joriy etish va ulardan foydalanish uchun qulay zamin yaratadi.

O'zbekiston ijtimoiy himoya tizimi kambag'allik darajasini kamaytirishga va aholining zaif qatlamlarini qo'llab-quvvatlashga qaratilgan turli dasturlarni o'z ichiga oladi. Hukumat ijtimoiy qo'llab-quvvatlash masalalariga alohida e'tibor bermoqda, yordam dasturlari qamrovini kengaytirmoqda va ularni taqdim etish mexanizmlarini takomillashtirmoqda. Shu bilan birga, mavjud ijtimoiy himoya tizimi ma'lum darajada tarqoqlik va cheklangan qamrov darajasi bilan ajralib turadi, bu esa, shu jumladan, SI dan foydalangan holda yanada samarali va manzilli yondashuvlarni izlash zarurligini ko'rsatadi [4].

O'zbekiston davlat boshqaruvi sohasida davlat xizmatlarini raqamlashtirishda, xususan, Interaktiv davlat xizmatlari yagona portali (my.gov.uz) orqali sezilarli yutuqlarga erishdi. Hukumat raqamli texnologiyalarni joriy etish orqali shaffoflikni oshirishga, byurokratiyani kamaytirishga va fuqarolar bilan o'zaro aloqalarni yaxshilashga intilmoqda. Mavjud raqamli infratuzilma va elektron hukumatni rivojlantirish natijasida davlat boshqaruvining samaradorligini oshirish va ko'rsatilayotgan xizmatlar sifatini yaxshilash maqsadida SI ni yanada integratsiya qilish uchun mustahkam asoslarni yaratmoqda.

O'zbekistonda SI rivojlanishining hozirgi holati. O'zbekiston sun'iy intellektni rivojlantirish sohasida o'sib borayotgan faollikni namoyish etmoqda, bu bir qator strategik hujjatlarning qabul qilinishi va aniq tashabbuslarning amalga oshirilishida o'z aksini topgan.

"2030-yilgacha sun'iy intellekt texnologiyalarini rivojlantirish strategiyasi" ushbu sohada mamlakatning asosiy maqsadlari va ustuvorliklarini belgilaydi, jumladan, 2030-yilga kelib SI asosidagi dasturiy mahsulotlar va xizmatlar bozorining hajmini 1,5 milliard AQSh dollariga yetkazish, SI ni davlat xizmatlariga integratsiya qilish, tadqiqot infratuzilmasini rivojlantirish va hukumatning SI ga tayyorlik indeksi bo'yicha TOP-50 mamlakat qatoriga kirish rejalashtirilgan. Ushbu maqsadli ko'rsatkichlar O'zbekistonning mintaqada SI sohasida yetakchilardan biriga aylanishga jiddiy intilayotganidan dalolat beradi.

O'zbekistonda SI ni qo'llash bilan bog'liq bir qator aniq loyihalar amalga oshirilmoqda, jumladan, Interaktiv davlat xizmatlari yagona portali va Soliq qo'mitasi uchun SI-assistentlarini ishlab chiqish, PalmPay tizimini joriy etish, shuningdek, LexAI yuridik platformasini yaratish kabilar shular jumlasidandir. Ushbu sohadagi sa'y-harakatlarni muvofiqlashtirish va startaplarni qo'llab-quvvatlashga qaratilgan Sun'iy intellekt va raqamli iqtisodiyotni rivojlantirish Markazining tashkil etilishi ham muhim qadam bo'ldi [5]. Shu bilan birga, "Bir million o'zbek dasturchisi" dasturi SI ni yanada rivojlantirish uchun zarur bo'lgan asosiy ko'nikmalarni shakllantirishda muhim rol o'ynaydi. Bundan tashqari, mamlakatda zamonaviy ma'lumotlarni qayta ishlash markazlarini yaratish va SI bilan ishlash uchun zarur bo'lgan hisoblash infratuzilmasini rivojlantirish bo'yicha ishlar ham olib borilmoqda [6].

O'zbekiston SI sohasida xalqaro hamkorlikni faol rivojlantirmoqda, Jahon banki va YUNESKO kabi tashkilotlar bilan o'zaro aloqada bo'lib, Birlashgan Arab Amirliklari bilan hamkorlik aloqalarini o'rnatmoqda. Meta kompaniyasi bilan SI til modellarini o'zbek tiliga moslashtirish bo'yicha hamkorlikni alohida ta'kidlash lozim [7]. Xalqaro loyihalarda ishtirok etish va tajriba almashish ham O'zbekistonda SI ni muvaffaqiyatli rivojlantirish uchun muhim omillardir.

O'zbekistonning ijtimoiy sohasida SI ning qo'llanilishi. Sun'iy intellekt texnologiyalari O'zbekistonning ijtimoiy sohasidagi dolzarb vazifalarni hal qilish va xizmatlar sifatini yaxshilash uchun keng imkoniyatlar ochib beradi:

Sog'liqni saqlash sohasida SI diagnostika jarayonlarini avtomatlashtirish (masalan, ko'krak bezi saratonini aniqlash sohasida), tibbiy tasvirlarni tahlil qilish va shifokorlarning qaror qabul qilishini qo'llab-quvvatlash uchun ishlatilishi mumkin. Diagnostika protseduralarini avtomatlashtirish tibbiy xodimlarning ish yukini kamaytirishga va ayniqsa, ixtisoslashgan sohalarda diagnostika aniqligini oshirishga imkon beradi. SI, shuningdek, telemeditsina va bemorlarning holatini masofadan monitoring qilishni rivojlantirishga yordam berishi mumkin, bu ayniqsa, olis hududlardagilarni tibbiy yordam bilan ta'minlash uchun muhimdir. SI yordamida katta hajmdagi epidemiologik ma'lumotlarni tahlil qilish kasalliklar tarqalishini bashorat qilish va ularning oldini olish bo'yicha samarali choralar ishlab chiqishga yordam beradi. Bundan tashqari, SI tibbiy muassasalarda ma'muriy jarayonlarni, jumladan, bemorlarning yozuvlarini boshqarish va resurslarni taqsimlashni optimallashtirish imkoniyatiga ham ega.

Ta'lim sohasida SI har bir talabaning individual ehtiyojlari va o'qish tezligiga moslashib, o'qitish materiallarini moslashtirib, ta'limga individual yondashuvlarni kiritishi mumkin [8].

SI asosidagi intellektual o'qitish tizimlari talabalar bilan individual qayta aloqa o'rnatishga va ularga yakka tartibda yordam berishga qodir [9]. SI topshiriqlarni tekshirish jarayonini avtomatlashtirishi, o'qituvchilarning vaqtini muhimroq ishlarga yo'naltirishi mumkin. Nutqni

matnga aylantirish va tarjima qilish uchun SI vositalari imkoniyati cheklangan talabalar va o'quvchilar uchun ta'lim olish imkoniyatini sezilarli darajada oshiradi [10]. SI bilan fan, texnologiya, muhandislik va matematika sohalarini o'z ichiga birlashtirilgan ta'lim tizimlariga ixtisoslashgan yo'nalishlarning "Al-Xorazmiy universiteti" (O'zbekiston Milliy universitetining tarixiy nomi) da ochilishi ushbu sohada kelajakdagi mutaxassislarni tayyorlashda muhim qadam hisoblanadi [11].

Ijtimoiy himoya sohasida SI turli xil ma'lumot manbalarini tahlil qilish orqali aholining zaif guruhlarini yanada aniqroq aniqlash va manzilli qo'llab-quvvatlash uchun ishlatilishi mumkin.

SI eligibility (inglizchadan - "moslik", "talabga javob berish", "huquqiylik" degan ma'nolarni anglatadi. Bu atama ko'pincha biror narsa uchun ariza berish yoki qatnashish huquqiga ega bo'lish holatini bildiradi. Ya'ni, kimdir yoki nimadir ma'lum shartlar, talablar yoki mezonlarga mos kelsa, u "eligible" (mos, loyiq) hisoblanadi) ni tekshirish, to'lovlarni tayinlash va benefisiar (bu biror mablag', huquq yoki xizmatdan foyda ko'ruvchi shaxs yoki tashkilot) lar bilan o'zaro aloqalarni optimallashtirishi mumkin [12]. SI texnologiyalari ijtimoiy qo'llab-quvvatlash dasturlari doirasida firibgarlik harakatlarini aniqlash va oldini olish uchun samarali qo'llanilish imkoniyatlari mavjud bo'lib, SI asosidagi chat-botlar va virtual assistentlar benefisiarlarga shaxsiy ma'lumot va maslahatlar bera oladi.

Davlat boshqaruvi sohasida SI elektron hukumat faoliyati samaradorligini sezilarli darajada oshirishi, fuqarolarning davlat organlari bilan o'zaro aloqalarini yaxshilashi va byurokrtiyani kamaytirishi mumkin. SI vositalari fuqarolarning murojaatlarini qayta ishlash, maslahatlar berish va kommunikatsiyani yaxshilash qobiliyatlariga ega. LexAI kabi SI asosidagi Legal Tech platformalari yuridik masalalar va hujjatlarni tayyorlashda yordam bera oladi. SI davlat muassasalarida kundalik ma'muriy vazifalarni avtomatlashtirishi, ma'lumotlarni boshqarishni yaxshilashi va resurslarni taqsimlashni optimallashtirishi mumkin. Ayniqsa, bojxona sohasida SI transit xavflarini tahlil qilish, firibgarlikni aniqlash va protseduralar samaradorligini oshirish uchun ishlatilishi mumkin.

SI texnologiyalarining imkoniyatlari va afzalliklari. O'zbekistonning ijtimoiy sohalariga SI ni joriy etish bir qator muhim imkoniyatlar va afzalliklarni ochib bera oladi.

SI turli ijtimoiy sohalarida kundalik vazifalarni avtomatlashtirish, jarayonlarni optimallashtirish va umumiy boshqaruvni yaxshilash orqali samaradorlik va unumdorlikni oshirishga qodir. Bu resurslardan yanada oqilona foydalanish va ularni murakkabroq va ustuvor vazifalarni hal qilishga yo'naltirish imkonini beradi.

SI ni qo'llash sog'liqni saqlash, ta'lim va davlat boshqaruvida ko'rsatilayotgan xizmatlar sifatini va undagi aniqlikni oshirishi mumkin. Masalan, sog'liqni saqlash sohasida SI kasalliklarni yanada aniqroq tashxislashga yordam berishi mumkin, bu esa o'z vaqtida va samarali davolanishga olib keladi.

SI texnologiyalari ijtimoiy xizmatlarning geografik to'siqlarni bartaraf etish, ta'limdagi turli ehtiyojlarni hisobga olish va aholining zaif qatlamlari uchun ta'minotni yaxshilash orqali ularning ommabopligi va inklyuzivligini oshirishga yordam bera oladi. Bu O'zbekistonning xilma-xil tabiiy landshafti va olis aholi punktlarining mavjudligini inobatga olsak bu muhimdir.

SI asosidagi tahlil rejalarni ishlab chiqish, resurslarni taqsimlash va xizmatlar sifatini yaxshilash sohasida asosli qarorlar qabul qilish uchun qimmatli ma'lumotlarni taqdim etadi.

Bu O'zbekiston hukumatiga aholi ehtiyojlariga yanada samaraliroq qondirish va yanada oqilona strategik qarorlar qabul qilish imkonini beradi.

O'zbekistonda SI ekotizimini rivojlantirish yangi ish o'rinlarini yaratish, eksportni ko'paytirish va xorijiy investitsiyalarni jalb qilish orqali iqtisodiy o'sish uchun katta salohiyatga ega hisoblanadi. O'zbekistonning 2030-yilga kelib SI bozorining hajmini 1,5 milliard AQSh dollariga yetkazish bo'yicha ambitsioz maqsadi (bu oddiy maqsadlarga qaraganda murakkabroq, ko'proq mehnat, bilim va resurs talab qiladigan, ammo katta muvaffaqiyat olib keladigan maqsad hisoblanadi) SI rivojlanishi bilan bog'liq sezilarli iqtisodiy umidlarni ta'kidlaydi [13].

SI texnologiyalari bilan bog'liq muammolar va tahdidlar. Katta salohiyatga qaramay, O'zbekistonning ijtimoiy sohasiga SI ni joriy etish bir qator muammolar va xavflar bilan bog'liq bo'lib, ularni hisobga olish va samarali usul va vositalar orqali bartaraf etish lozim. Jumladan:

internet aloqasining sifat va miqdor jihatdan yetarli darajada emasligi va ma'lumotlarni qayta ishlash markazlarining rivojlanmaganligi kabi infratuzilmadagi cheklovlar SI texnologiyalarini keng joriy etish uchun jiddiy to'siqlardan biri bo'lib qolmoqda;

ma'lumotlar sifati va ulardan foydalanish imkoniyati SI modellarini o'qitish uchun juda muhimdir. Ma'lumotlarning tarqoqligi, ularning xavfsizligi va yetarli darajada sifatli emasligi bilan bog'liq muammolar SI dan samarali foydalanishni qiyinlashtirishi mumkin;

SI sohasida malakali mutaxassislarning yetishmasligi yana bir jiddiy muammodir. SI ni muvaffaqiyatli rivojlantirish va joriy etish uchun ta'lim dasturlariga va kadrlar tayyorlashga investitsiyalar kiritish zarur [14];

algoritmik tarafkashlik, ma'lumotlar maxfiyligini buzish va SI dan mas'uliyatli foydalanish masalalari kabi axloqiy mulohazalar alohida e'tibor talab qiladi va tegishli tartibga solish mexanizmlarini ishlab chiqishni talab qiladi. Bu kabi axloqiy muammolarni tan olish va axloqiy standartlarni ishlab chiqish SI ni mas'uliyatli tarzda joriy etish yo'lidagi muhim qadamdir [15];

SI bilan bog'liq faoliyatni huquqiy va normativ tartibga solishdagi mavjud bo'shliqlar uning ijtimoiy sohada rivojlanishi va qo'llanilishini cheklashi mumkin. Buning uchun aniq va moslashuvchan huquqiy asoslarni ishlab chiqish zarur;

SI ni joriy etish natijasida yuzaga keladigan avtomatlashtirish iqtisodiyotning ayrim tarmoqlarida ish o'rinlarining qisqarishiga olib kelishi mumkin. Ushbu jarayonning salbiy oqibatlarini yumshatish uchun ishchi kuchini qayta tayyorlash va malakasini oshirish strategiyalarini ishlab chiqish zarur. Yangi ish o'rinlarini yaratishga intilishga qaramay, mavjud ish o'rinlarining potentsial qisqarishi haqida xabarlar ham mavjud [16]. Bu esa ishchi kuchini rivojlantirish sohasida

chora-tadbirlar ko'rish zarurligini ta'kidlaydi;

Bundan tashqari aholi ustidan nazoratni kuchaytirish va kuzatuvni kuchaytirish uchun

SI texnologiyalaridan foydalanish imkoniyati bilan bog'liq avtoritarizmning kuchayish xavfi ham mavjud [17].

SI texnologiyalari sohasida xalqaro hamkorlik va ilg'or jahon tajribalari. O'zbekiston

SI va raqamli transformatsiya sohasida xalqaro hamkorlikni faol rivojlantirmoqda. Xususan, Jahon banki, YUNESKO va Meta kabi tashkilotlar bilan hamkorlik tajriba almashishga, investitsiyalarni jalb qilishga va ilg'or amaliyotlarni joriy etishga yordam beradi.

Hozirgi kundagi tendensiyalarga ko'ra, jahon tajribasi SI ning turli ijtimoiy sohalarda muvaffaqiyatli qo'llanilishini ko'rsatmoqda. Sog'liqni saqlash sohasida SI kasalliklarni tashxislash, telemeditsina va ma'muriy jarayonlarni optimallashtirish uchun ishlatiladi. Ta'lim sohasida

SI individual ta'lim, intellektual o'qitish tizimlari va avtomatlashtirilgan baholash uchun qo'llaniladi [18]. Ijtimoiy himoya sohasida SI yordamning manzilliligini yaxshilash, xizmat ko'rsatishni optimallashtirish va firibgarlikni aniqlash ham uchun ishlatiladi [19]. Davlat boshqaruvi sohasida

SI elektron xizmatlar samaradorligini oshirishga, fuqarolar bilan o'zaro aloqalarni yaxshilashga va ma'muriy jarayonlarni optimallashtirishga yordam beradi.

Markaziy Osiyo va boshqa rivojlanayotgan mamlakatlarning SI ni rivojlantirish strategiyalarini tahlil qilish mintaqaviy tendensiyalarni, ilg'or amaliyotlarni va hamkorlik uchun potentsial sohalarni aniqlashga imkon beradi. O'zbekiston yondashuvini qo'shni mamlakatlar tajribasi bilan taqqoslash mamlakatda SI ni yanada rivojlantirish uchun qimmatli yo'nalishlarni taqdim etishi mumkin.

O'zbekistondagi ijtimoiy sohalarda SI texnologiyalarini joriy qilish bo'yicha tavsiyalar. O'zbekistonning ijtimoiy sohasida sun'iy intellekt texnologiyalarini yanada rivojlantirish va samarali joriy etish uchun bir qator strategik chora-tadbirlarni amalga oshirish zarur:

birinchidan, internet aloqasini sifat va qamrov jihatidan kengaytirish va modernizatsiya qilish, ma'lumotlarni qayta ishlash markazlari va yuqori unumdorlikdagi hisoblash quvvatlariga investitsiyalar kiritish orqali raqamli infratuzilmani mustahkamlash lozim;

ikkinchidan, "Katta ma'lumotlar" bazalarini yaratishni ham o'z ichiga olgan holda, ma'lumotlar sifati, ulardan foydalanish imkoniyati, o'zaro ishlash qobiliyati va xavfsizligini oshirish strategiyalarini ishlab chiqish orqali ma'lumotlar ekotizimini takomillashtirish zarur;

uchinchidan, barcha SI sohasidagi ta'lim dasturlarini kengaytirish va takomillashtirish,

"Bir million o'zbek dasturchisi" kabi tashabbuslarni qo'llab-quvvatlash va Al-Xorazmiy universiteti kabi ixtisoslashgan o'quv yurtlarini rivojlantirishni o'z ichiga olgan holda inson kapitalini rivojlantirishga katta investitsiyalar kiritish kerak;

to'rtinchidan, tarafkashlik, maxfiylik, shaffoflik va hisobdorlik masalalarini hisobga olgan holda, axloqiy standartlarni integratsiya qilish bo'yicha olib borilayotgan sa'y-harakatlarga asoslanib, SI ni rivojlantirish va qo'llash uchun har tomonlama axloqiy asosni ishlab chiqish va joriy etish lozim;

beshinchidan, SI uchun aniq va moslashuvchan huquqiy va normativ bazani yaratish zarur, bu SI ni tartibga solish bo'yicha olib borilayotgan jarayonni hisobga olgan holda, innovatsiyalarni rag'batlantiradi va shu bilan birga xavflarni kamaytiradi;

oltinchidan, innovatsiyalarni rag'batlantirish va SI ni joriy etish uchun davlat muassasalari, texnologik kompaniyalar, ilmiy-tadqiqot institutlari va fuqarolik jamiyati tashkilotlari o'rtasida hamkorlikni yo'lga qo'yish va mavjudlarini rag'batlantirish lozim;

yettinchidan, global tajribadan foydalanish, moliyalashtirish imkoniyatlariga erishish va ilg'or amaliyotlarni almashish uchun xalqaro hamkorlikda faol ishtirok etishni davom ettirish zarur;

sakkizinchidan, SI ni rivojlantirish va joriy etish hukumatning qarashlariga muvofiq, inson ehtiyojlariga va uning imkoniyatlarini kengaytirishga yo'naltirilishi kerak;

to'qqizinchidan, SI yechimlarining samaradorligini sinab ko'rish uchun asosiy ijtimoiy sohalarda pilot loyihalar (bu kichik miqyosda sinov tariqasida amalga oshiriladigan loyiha bo'lib, uning asosiy maqsadi - asosiy (katta) loyihani to'liq joriy qilishdan oldin tajriba o'tkazish, natijalarni tekshirish va muammolarni aniqlash) ni amalga oshirish va muvaffaqiyatli ilovalarni milliy miqyosda kengaytirish strategiyalarini ishlab chiqish lozim;

o'ninchidan, SI natijasida yuzaga keladigan avtomatlashtirishning potentsial salbiy oqibatlarini yumshatish uchun ishchi kuchini qayta tayyorlash va malakasini oshirish strategiyalarini ishlab chiqish, shuningdek, ijtimoiy himoya tizimlarini yaratish zarur.

Xulosa sifatida shuni aytish mumkinki, sun'iy intellekt O'zbekistonning ijtimoiy salohiyatini o'zgartirish va milliy taraqqiyot maqsadlariga erishishga yordam berish uchun ulkan salohiyatga ega. SI strategik, axloqiy va hamkorlikka asoslangan yondashuvlar negizida O'zbekistonga ushbu texnologiyalarning afzalliklarini to'liq ro'yobga chiqarishga, shu bilan birga potentsial xavflarni minimallashtirishga imkon beradi. Taqdim etilgan tavsiyalarni izchil bajarish O'zbekistonning sun'iy intellekt imkoniyatlaridan foydalangan holda farovon va inklyuziv jamiyatni yaratish yo'lidagi taraqqiyotiga yanada yordam beradi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

[1] Harnessing AI for development: Uzbekistan's progress towards becoming a regional IT hub. (Elektron resurs) <https://oxfordinsights.com/insights/harnessing-ai-for-development-uzbekistans-progress-towards-becoming-a-regional-it-hub/> (Murojaat etilgan sana: 06.05.2025 y.);

[2] Helping Uzbekistan Undertake a Historic Social and Economic Transformation - World Bank. (Elektron resurs) <https://www.worldbank.org/en/results/2024/07/16/helping-uzbekistan-undertake-a-historic-social-and-economic-transformation> (Murojaat etilgan sana: 05.05.2025 y.);

[3] Doç. Dr. Oğuzhan Erdoğan, Uzbekistan's national artificial intelligence strategy (PDF). https://www.researchgate.net/publication/388146491_UZBEKISTAN'S_NATIONAL_ARTIFICIAL_INTELLIGENCE_STRATEGY (Murojaat etilgan sana: 07.05.2025 y.);

- [4] Uzbekistan - ILO | Social Protection Platform. (Elektron resurs) <https://www.social-protection.org/gimi/ShowCountryProfile.action?iso=UZ> (Murojaat etilgan sana: 05.05.2025 y.);
- [5] Uzbekistan sets AI development strategy, aiming for \$1.5bn market by 2030. (Elektron resurs) <https://daryo.uz/en/2024/10/18/uzbekistan-sets-ai-development-strategy-aiming-for-15bn-market-by-2030> (Murojaat etilgan sana: 05.05.2025 y.);
- [6] Omar Ashurbaev, The future of artificial intelligence in Uzbekistan. (Elektron resurs) <https://webofjournals.com/index.php/1/article/download/2104/2082/4105> (Murojaat etilgan sana: 07.05.2025 y.);
- [7] Uzbekistan and Meta: AI cooperation at a new stage – Pivot. (Elektron resurs) <https://pivot.uz/uzbekistan-and-meta-ai-cooperation-at-a-new-stage/> (Murojaat etilgan sana: 06.05.2025 y.);
- [8] Artificial intelligence in geographical education of Kazakhstan and Uzbekistan: Revolution of knowledge and approaches | International Journal of Innovative Research and Scientific Studies. (Elektron resurs) <https://www.ijirss.com/index.php/ijirss/article/view/5546> (Murojaat etilgan sana: 07.05.2025 y.);
- [9] What are some real-world examples of AI being used in education today? (Elektron resurs) <https://www.quora.com/What-are-some-real-world-examples-of-AI-being-used-in-education-today> (Murojaat etilgan sana: 06.05.2025 y.);
- [10] The Ultimate Guide to AI in Education: Benefits, Challenges, & Real-World Uses. (Elektron resurs) <https://www.powerschool.com/blog/ai-in-education/> (Murojaat etilgan sana: 05.05.2025 y.);
- [11] Uzbekistan unveils Al-Khwarizmi University for AI and STEM. (Elektron resurs) <https://www.muslimnetwork.tv/uzbekistan-unveils-al-khwarizmi-university-for-ai-and-stem-education/> (Murojaat etilgan sana: 05.05.2025 y.);
- [12] AI-Driven Social Protection: Enhancing Access and Delivery - CSM Technologies. (Elektron resurs) <https://www.csm.tech/blog-details/ai-driven-social-protection-enhancing-access-and-delivery> (Murojaat etilgan sana: 07.05.2025 y.);
- [13] Uzbekistan sets AI development strategy, aiming for \$1.5bn market by 2030. (Elektron resurs) <https://daryo.uz/en/2024/10/18/uzbekistan-sets-ai-development-strategy-aiming-for-15bn-market-by-2030> (Murojaat etilgan sana: 07.05.2025 y.);
- [14] Omar Ashurbaev, The future of artificial intelligence in Uzbekistan. (Elektron resurs) <https://webofjournals.com/index.php/1/article/download/2104/2082/4105> (Murojaat etilgan sana: 07.05.2025 y.);
- [15] Uzbekistan to integrate ethical standards in AI, PM announces. (Elektron resurs) <https://daryo.uz/en/2025/02/02/uzbekistan-to-integrate-ethical-standards-in-ai-pm-announces> (Murojaat etilgan sana: 06.05.2025 y.);
- [16] Shaping the Future of AI and ICT: IT Park Uzbekistan – ITPARK. (Elektron resurs) <https://it-park.uz/en/itpark/news/shaping-the-future-of-ai-and-ict-it-park-uzbekistan-strengthens-international-partnerships> (Murojaat etilgan sana: 06.05.2025 y.);
- [17] Uzbekistan's Military Modernisation: AI, UAVs, and Robotic Systems – SpecialEurasia. (Elektron resurs) <https://www.specialeurasia.com/2025/02/27/uzbekistan-military-upgrade/> (Murojaat etilgan sana: 05.05.2025 y.);
- [18] Uzbekistan - International Science Council. https://council.science/wp-content/uploads/2025/02/AI-Paper-Case-Study-Uzbekistan_V1.pdf (Murojaat etilgan sana: 06.05.2025 y.);
- [19] AI-Driven Social Protection: Enhancing Access and Delivery - CSM Technologies. (Elektron resurs) <https://www.csm.tech/blog-details/ai-driven-social-protection-enhancing-access-and-delivery> (Murojaat etilgan sana: 07.05.2025 y.).

BULUTLI TIZIMLARDA MULTI-TENANT VA CROSS-DOMAIN SHARING XAVFSIZLIK TAHLILI

A.A. KARIMOV

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Annotatsiya. Ushbu maqolada Bulutli hisoblash tizimlarida Multi-Tenant va Cross-Domain Sharing arxitekturasi tuzilishi afzaliklari va kamchiliklari keltirib o'tilgan. Bundan tashqari Multi-Tenant va Cross-Domain Sharing bo'yicha xavfsizlik muammolari o'rganib chiqilib batafsil keltirib o'tildi. Aniqlangan xavfsizlik muammolariga yechim sifatida tavsiyalar ishlab chiqildi.

Kalit so'zlar: Multi-Tenant, scalability, Isolated Schema, API, SSO, AWS, Google Drive, Identity & Access Management, Zero Trust Security.

Аннотация. В данной статье рассматриваются преимущества и недостатки многопользовательской и кросс-доменной архитектуры совместного использования в системах облачных вычислений. Кроме того, были подробно изучены и обсуждены вопросы безопасности, связанные с многопользовательским и кросс-доменным доступом. Были разработаны рекомендации по решению выявленных проблем безопасности.

Ключевые слова: Multi-Tenant, scalability, Isolated Schema, API, SSO, AWS, Google Drive, Identity & Access Management, Zero Trust Security.

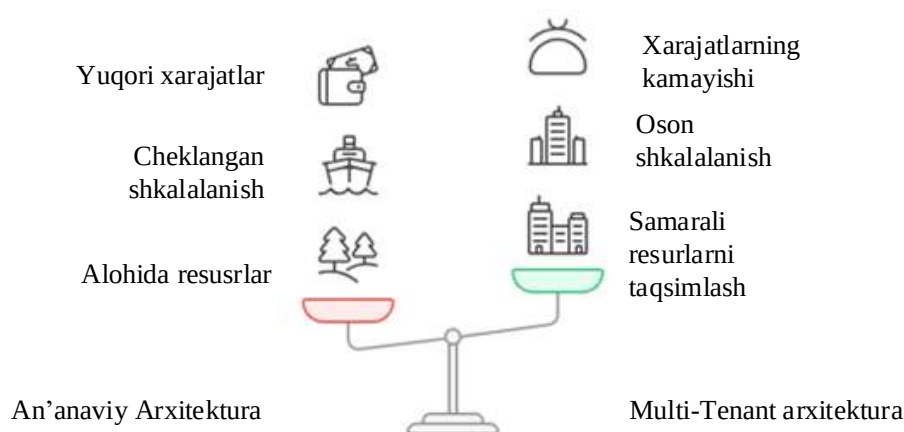
Bulutli hisoblashda multi-tenant multi-tenant (ko'p ijarachi) va cross-domain sharing (domenlararo almashish) tushunchalari muhim hisoblanadi, chunki ular Bulutli infratuzilmasining samaradorligini va xavfsizligini ta'minlashda asosiy rol o'ynaydi.

1. Multi-Tenant Arxitektura (Ko'p ijarali arxitektura)

Multi-tenant arxitektura deganda bitta dastur yoki tizimni bir nechta mustaqil foydalanuvchilar (tenantlar) umumiy foydalanishi tushuniladi. Bunda har bir tenant (mijoz yoki tashkilot) o'zining ma'lumotlari va konfiguratsiyalarini mustaqil boshqaradi, lekin umumiy infratuzilmadan foydalanadi.

Multi-Tenantning afzalliklari:

- Resurslarni samarali taqsimlash – Bir xil hardware va software resurslar ko'p mijozlar tomonidan ishlatiladi.
- Shkalalanish (scalability) – Kengaytirish osonroq, chunki yangi mijozlar uchun alohida infratuzilma tayyorlash shart emas.
- Xarajatlarning kamayishi – Har bir tenant uchun alohida server yoki dasturiy ta'minot ishlatish talab etilmaydi.
- Markazlashgan yangilanishlar – Dasturiy ta'minot yangilanishlari barcha tenantlarga bir vaqtning o'zida ta'sir qiladi.



1-rasm. Multi-Tenantning afzalliklari

Multi-Tenant Turlari:

1. Shared Database, Shared Schema – Hamma tenantlar bitta ma'lumotlar bazasidan foydalanadi.

2. Shared Database, Isolated Schema – Har bir tenant uchun alohida ma'lumotlar bazasi sxemasi mavjud.

3. Separate Database – Har bir tenant uchun alohida ma'lumotlar bazasi ajratilgan.

Misol uchun: Salesforce – CRM tizimi multi-tenant arxitekturaga ega, Google Workspace – Bir nechta tashkilotlar Gmail, Drive va boshqa xizmatlardan umumiy infratuzilma asosida foydalanadi.

2. Cross-Domain Sharing (Domenlararo ma'lumot almashinuvi)

Cross-domain sharing deganda bir domen (tashkilot yoki tizim)dagi ma'lumotlarni yoki xizmatlarni boshqa domenlar bilan xavfsiz tarzda almashish jarayoni tushuniladi.

Cross-Domain Sharingda quyidagi muhim jihatlar mavjud:

- Xavfsizlik – Ma'lumotlar boshqa domenlarga o'tish jarayonida shifrlanishi va maxfiyligi ta'minlanishi kerak.

- Avtorizatsiya va autentifikatsiya – Foydalanuvchilarning kimligini aniqlash va huquqlarini tekshirish muhim.

- Standart protokollar – OAuth, SAML, OpenID Connect kabi texnologiyalar ishlatiladi.

Cross-Domain Sharingga misollar:

- Single Sign-On (SSO) – Bir martalik kirish imkoniyati (masalan, Google yoki Microsoft hisoblari orqali bir nechta xizmatlarga kirish).

- API orqali integratsiyalar – Masalan, Stripe va Shopify integratsiyasi.

- Federated Identity Management – Tashkilotlararo identifikatsiya almashinuvi.

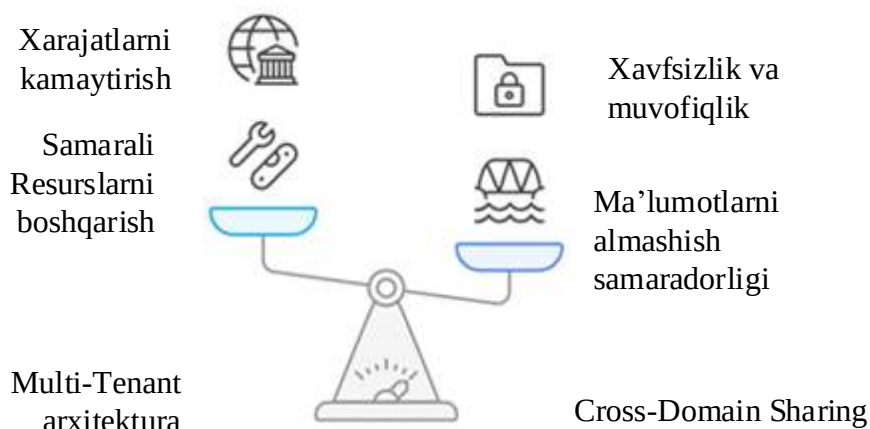


2-rasm. Cross-Domain Sharingga misollar

3. Multi-Tenant va Cross-Domain Sharing o'rtasidagi bog'liqlik.

Multi-tenant tizimlarda cross-domain sharing juda muhim, chunki bir xil bulut tizimi bir nechta tashkilot tomonidan ishlatilsa ham, ularning ma'lumotlari izolyatsiya qilinishi va ba'zan xavfsiz tarzda almashilishi talab qilinadi.

Masalan: Google Driveda fayllarni boshqa tashkilotlar bilan bo'lishish yoki AWS multi-tenant infratuzilmasida turli mijozlar uchun xavfsiz ma'lumot almashinuvi amalga oshiriladi.



3-rasm. Samarali resurslarni boshqarish va ma'lumotlarni almashish o'rtasidagi muvozanat

4. Multi-Tenant va Cross-Domain Sharing bo'yicha xavfsizlik muammolari va yechimlari.

Cloud computingda Multi-Tenant va Cross-Domain Sharing texnologiyalarining xavfsizlik muammolari dolzarb hisoblanadi. Ushbu muammolarni hal qilish uchun bir nechta xavfsizlik mexanizmlari va texnologiyalar qo'llaniladi.

Multi-Tenant xavfsizlik muammolari va ularning yechimlari.

Muommolar:

1. Ma'lumotlarning tenantlar orasida aralashishi

- Bir nechta mijoz bitta cloud platformada ishlaydi, va noto'g'ri konfiguratsiya sababli ma'lumotlar bir-biri bilan aralashib ketishi mumkin.

2. Tenantlar o'rtasida huquqsiz kirish (Unauthorized Access)

- Bir tenant boshqa tenantning ma'lumotlariga ruxsatsiz kira olmasligi kerak.

3. Identity & Access Management (IAM) muammolari

- Har bir tenant uchun foydalanuvchilarning autentifikatsiya va avtorizatsiya jarayonlarini to'g'ri boshqarish muhim.

4. Shifrlash (Encryption) masalalari

- Agar ma'lumotlar yetarlicha himoyalansa, ular boshqa tenantlar tomonidan o'qilishi yoki o'g'irlanishi mumkin.

Yechimlar:

1. Data Isolation (Ma'lumotlarni izolyatsiya qilish)

- Logical Isolation: Har bir tenant uchun alohida database schema yoki virtual instance ajratish lozim.

- Physical Isolation: Yirik mijozlar uchun alohida server yoki ma'lumotlar bazasi taqdim etish lozim.

2. Role-Based Access Control (RBAC) va Attribute-Based Access Control (ABAC)

- Tenantlar o'rtasidagi ma'lumot almashinuvini qat'iy nazorat qilish.

- IAM (Identity and Access Management) tizimlaridan foydalanish (AWS IAM, zure AD, Google IAM).

3. Tenant ID Mapping va Logging

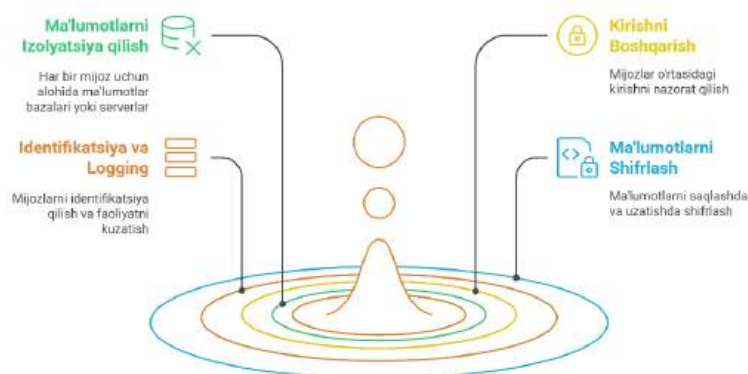
- Har bir tenantga noyob identifikator berish va barcha harakatlarni logga olish kerak.

- SIEM (Security Information and Event Management) tizimlari orqali monitoring qilib borilishi kerak.

4. Data Encryption (Ma'lumotlarni shifrlash)

- At-Rest Encryption: Ma'lumotlarni saqlashda shifrlash (AES-256)ni amalga oshirish.

- In-Transit Encryption: TLS/SSL orqali ma'lumotlarni uzatishda shifrlashni amalga oshirish.



4-rasm. Multi-Tenant xavfsizlik muommolariga yechimlar arxitekturası

Cross-Domain Sharing xavfsizlik muommolari va ularning yechimlari
Muammolar:

1. Ma'lumotlarni boshqa domenlarga uzatishda xavfsizlik xavflari
- Xavfsiz autentifikatsiya va avtorizatsiya amalga oshirilmasa, ma'lumotlar noto'g'ri odam qo'lga tushishi mumkin.

2. Man-In-The-Middle (MITM) hujumlari

- Domenlararo uzatilayotgan ma'lumotlar o'g'irlanishi yoki buzilishi mumkin.

3. Identity Federation muammolari

- Turli domenlar orasida autentifikatsiya va avtorizatsiyani to'g'ri boshqarish qiyin.

Yechimlar:

1. Strong Authentication & Authorization

- OAuth 2.0, SAML, OpenID Connect kabi protokollarni ishlatish.

- API-larni himoya qilish uchun JWT (JSON Web Token) yoki API Gateway ishlatish.

2. Zero Trust Security Model (Nol ishonch modeli)

- Har bir so'rovni tasdiqlash va foydalanuvchini doimiy verifikatsiya qilish.

- Least Privilege Access – foydalanuvchiga faqat kerakli huquqlarni berish.

3. Data Loss Prevention (DLP)

- Ma'lumotlar noto'g'ri domenlarga uzatilmasligini ta'minlash uchun DLP tizimlari qo'llash.

- Google DLP, Microsoft Purview DLP kabi texnologiyalardan foydalanish.

4. Mutual TLS (mTLS) va End-to-End Encryption

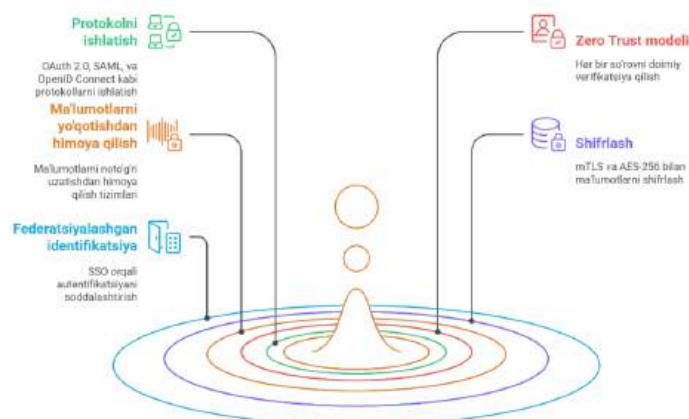
- mTLS orqali ikkala tomon ham autentifikatsiyadan o'tadi.

- AES-256 va TLS 1.3 bilan ma'lumotlarni shifrlash.

5. Federated Identity Management (FIM)

- SSO (Single Sign-On) orqali domenlararo autentifikatsiyani soddalashtirish.

- Microsoft Entra ID, Okta, Google Identity kabi tizimlardan foydalanish.



4-rasm. Cross-Domain Sharing xavfsizlik muommolariga yechimlar arxitekturası

Xulosa

Mazkur maqolda davomida quyidagila natijalarga erishildi:

- Multi-tenant arxitekturasi va turlari o'rganilib chiqildi.
- Cross-domain sharingning muhim jixatlari o'rganib chiqildi.
- Multi-Tenant va Cross-Domain Sharing o'rtasidagi bog'liqlik tahlili amalga oshirildi.
- Multi-Tenant xavfsizlik muommolari tahlili amalga oshirildi
- Multi-Tenant xavfsizlik muommolariga qarshi yechimlar ishlab chiqildi.
- Cross-Domain Sharing xavfsizlik muommolari tahlili amalga oshirildi.
- Cross-Domain Sharing xavfsizlik muommolariga qarshi yechimlar ishlab chiqildi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

[1] Nuno Bettencourt, "Recommending Access Policies in Cross-domain Internet" 7th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management At: Lisbon, Portugal 2015. Volume: 3

[2] Stefan Wiesner, Fenareti Lampathakib, Evmorfia Bilirib, Klaus-Dieter Thoben, "Requirements for cross-domain Knowledge Sharing in collaborative Product-Service System design" 2016.

[3] Omessead BenMbarak, Anis Naanaa, Sadok ElAsmi "New secure access control model for cloud computing based on Chaotic systems" 2023 International Wireless Communications and Mobile Computing (IWCMC) ©2023 IEEE

[4] Z.Liu, Luo, L.Xu, "A fine-Grained Attribute-Based Authentication For Sensitive Data Stored in Cloud Computing" International Journal of Grid and Utility Computing 7(4), pp. 237-244, 2016.

[5] Kai Fan, Qiang Pan, Junxiong Wang, Tingting Liu "Cross-Domain Based Data Sharing Scheme in Cooperative Edge Computing" 2018 IEEE International Conference on Edge Computing (EDGE).

[6] Manchao Zhang, Hong Zhu, Kai Jiang "Secure Cross-Domain Data Sharing Technology Based on Blockchain".

[7] Karimov, A., Olimov, I., Berdiyev, K., Tojiakbarova, U., & Tursunov, O. (2021, November). Cloud Computing Security Challenges and Solutions. In 2021 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-6). IEEE.

DEVELOPMENT OF A MULTI-PARAMETER GROUNDWATER MONITORING DEVICE USING LEVEL, TEMPERATURE, AND pH SENSORS

G.N. MEMONOVA

Tashkent university of Information technologies

Abstract. Groundwater is essential for agriculture and ecosystem balance, particularly in water-scarce regions. This study introduces a low-power, compact groundwater monitoring device integrating three key sensors: PL315 (water level), PT100 (temperature), and a pH sensor. The system employs LoRa-based wireless communication for real-time, long-range data transmission. Sensor data is visualized through a centralized platform, allowing continuous tracking of groundwater parameters. Field tests in agricultural areas confirmed the system's accuracy, low energy consumption, and reliable performance over time. The device provides a scalable, cost-effective solution for rural water monitoring, helping to detect salinity, pollution, and enabling more sustainable irrigation planning. It supports informed decision-making in groundwater resource management.

Keywords: groundwater monitoring, water level sensor (PL315), temperature sensor (PT100), pH sensor (pH-4502C), real-time system, IoT, LoRa communication, Energy-efficient wireless transmission.

Global climate change, population growth, and rising agricultural demands have significantly increased the reliance on groundwater. In semi-arid and water-scarce regions, phreatic water serves not only as a drinking water source but also plays a critical role in irrigation, industry, and livestock sectors [1]. However, these vital resources are often exploited without proper regulation, leading to negative outcomes such as salinization, ecological degradation, and water supply shortages [2]. In such contexts, continuous monitoring of water level and quality parameters is essential for early warning systems and the formulation of sustainable management strategies. Digital technologies-particularly sensor-based devices and Internet of Things (IoT) systems-offer new opportunities for addressing these challenges [3]. Therefore, the development of modern, reliable, and cost-effective monitoring tools is a pressing scientific and technological necessity.

This study presents the development of a multi-parameter groundwater monitoring device capable of real-time measurement of water level, temperature, and pH. The device operates on a LoRa communication module and incorporates the PL315 water level sensor, PT100 temperature sensor, and pH-4502C pH sensor. It is programmed using the Arduino platform, and the data collected is transmitted to a centralized monitoring interface. The proposed solution was evaluated through real-world testing and compared with findings from related literature. The outcomes of this research could contribute significantly to efficient water resource management, optimization of irrigation systems, and enhancement of environmental safety.

In many rural areas, groundwater monitoring still relies on traditional, manual measurement methods. These techniques are time-consuming, resource-intensive, and offer limited spatial and temporal coverage. Most existing systems do not provide real-time data or are heavily dependent on physical infrastructure [4]. Moreover, devices designed to monitor individual parameters often require significant space and are difficult to integrate into a unified system. For example, using separate devices for level, temperature, and pH measurements reduces system efficiency. Additionally, communication technologies like GSM or Wi-Fi are power-intensive and unsuitable for long-range transmission in remote areas [5]. There is thus a clear need for a compact, multi-parameter, low-power, and long-range automated monitoring solution.

Recent literature highlights several developments in low-power sensor networks and IoT-based systems for water quality monitoring. For example, Kumar proposed a modular and low-cost monitoring system using Arduino to measure TDS, pH, and temperature [6]. Additionally, LoRa-based architecture has been shown to enable energy-efficient, long-range data transmission [7]. A

multi-parameter monitoring solution by Panigrahi was successfully tested in real-world conditions, confirming its applicability [8]. Other studies have implemented real-time monitoring using LPWAN-based microcontroller systems to reduce power consumption and enable wireless data collection [9]. However, many of these solutions focus on only one or two parameters and often face limitations in stability, accuracy, or scalability.

The main objective of this research is to design and test an automated multi-parameter groundwater monitoring device that integrates sensors for measuring water level, temperature, and pH. The device incorporates LoRa-based long-range communication, an Arduino-programmed control system, and a centralized data visualization platform. This configuration enables continuous real-time monitoring of subsurface water conditions. The research also evaluates sensor stability, power efficiency, and measurement accuracy. Based on the results, practical recommendations will be proposed for deployment in agriculture, reclamation projects, and environmental monitoring applications.

The system integrates three primary sensors: PL315 (water level), PT100 (temperature), and pH-4502C (pH), which are managed via an Arduino microcontroller and connected to a central gateway through a LoRa communication module. The device operates autonomously using a solar panel and rechargeable battery as its energy source. Initially, the system is configured and tested in laboratory settings, followed by field trials in agricultural environments. The sensor data are filtered and averaged through custom algorithms before being stored and analyzed. The monitoring platform is web-connected, offering real-time visualizations and alerts to end-users. This architecture supports the development of a robust, energy-efficient, and scalable groundwater monitoring solution [10].

Materials and Methods

The developed groundwater monitoring device integrates a set of low-power and cost-effective components designed to measure key physical and chemical parameters of phreatic water in real time. The core structure of the system consists of three primary sensors: a water level sensor (PL315), a temperature sensor (PT100 Waterproof), and a pH sensor (pH-4502C), which are selected based on their compatibility with Arduino-based microcontrollers and their proven stability under field conditions.

Each sensor is connected to an Arduino UNO microcontroller, which serves as the control unit for data acquisition and preprocessing. The water level sensor (PL315) utilizes ultrasonic or pressure-based measurement principles to detect variations in groundwater depth with high resolution, while the PT100 temperature sensor provides accurate temperature readings with minimal drift over time [11]. The pH sensor pH-4502C operates via an electrochemical interface and is capable of continuously monitoring the hydrogen ion concentration in water, offering insight into water acidity or alkalinity.

To enable long-range wireless data transmission, the system is equipped with a LoRa (Long Range) module operating at 868 MHz, which ensures energy-efficient communication over several kilometers without the need for existing communication infrastructure. The LoRa module is directly interfaced with the Arduino board via UART protocol, facilitating efficient packetized transmission of sensor data [12].

The entire device is powered by an autonomous energy unit composed of a 6V 5W solar panel and a rechargeable Li-ion battery pack, allowing for extended outdoor operation in remote areas without stable electricity access. The hardware components are housed within a weather-resistant IP65 enclosure to protect the electronics from environmental hazards such as dust, rain, and direct sunlight.

A simplified schematic of the component layout is illustrated in Figure 1, while Table 1 lists the technical specifications of the sensors and microcontroller used. This modular architecture ensures scalability, allowing additional sensors to be integrated as needed, and supports reliable operation for long-term groundwater quality monitoring.

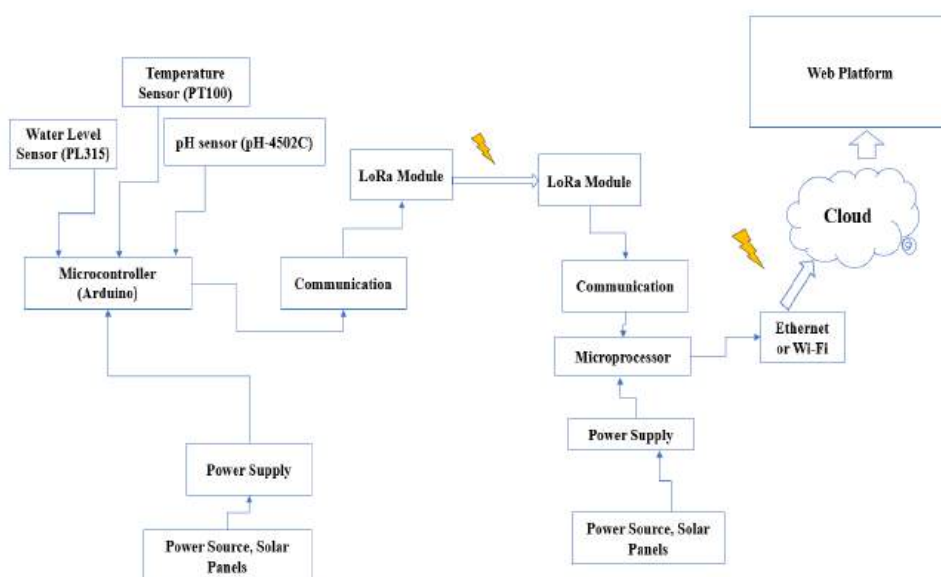


Figure 1. Block diagram of the groundwater monitoring device structure

Table 1.

Technical specifications of the main sensors and hardware components

Component	Specifications
Water Level Sensor (PL315)	Analog output, range 0 - 4.5V, resolution ± 2 cm, waterproof enclosure
Temperature Sensor (PT100 Waterproof)	High-accuracy RTD sensor, range -50°C to 250°C , accuracy $\pm 0.5^{\circ}\text{C}$, SPI interface via MAX31865
pH Sensor (pH-4502C)	Range 0-14 pH, accuracy ± 0.3 pH, analog output, BNC connector
Microcontroller (Arduino UNO)	ATmega328P, 10-bit ADC, operating voltage 5V, flash memory 32 KB
Communication Module (LoRa SX1278)	Frequency 868 MHz, UART interface, range up to 10 -15 km, low power consumption
Power Supply (Solar + Battery)	6V 5W solar panel, rechargeable Li-ion battery pack, 4.5Ah capacity

For the effective operation of a multi-parameter groundwater monitoring system, all its components - sensors, microcontroller, communication module, and power source - must be reliably connected electrically.

The Arduino Uno microcontroller was selected as the main control module of the monitoring device. This module reads analog and digital signals from the sensors, processes them accordingly, and transmits the data to an external monitoring platform via LoRa. The three sensors used in the device are connected via different interfaces: the PL315 water level sensor is connected via an analog input port, the PT100 temperature sensor is connected via SPI using the MAX31865 interface, and the pH-4502C sensor provides an analog output signal connected to the A0 port.

The data coming from the sensors is first converted into measurable voltage. Arduino converts this voltage into digital format via the ADC (Analog to Digital Converter). The digital values are converted into the required units using software: water level in cm, temperature in $^{\circ}\text{C}$, and pH in index format [11,12]. Sensor data is measured every 10 minutes, and an average value is calculated. This interval reduces the device's power consumption and increases signal stability [13].

In the electrical design, all sensors and the microcontroller are connected to a single power supply - through a 5V voltage stabilizer. The LoRa module (Ra-02 SX1278) is connected to the

Arduino microcontroller via UART and serves as the data transmitter. In the software, after each measurement session, the average values are packaged in JSON format and transmitted via LoRa.

To reduce signal interference and noise within the system, shielded cables and filter capacitors are used for all analog signals. To prevent measurement inaccuracies caused by external electromagnetic interference, low-pass RC filters are placed before the output ports of each sensor [14].

This integrated solution ensures synchronized operation of all components and provides reliable real-time data on groundwater parameters. The device also features a modular design that can be easily relocated and reconfigured in field conditions.

The effectiveness of a groundwater monitoring system depends not only on the accuracy of the sensors but also on the ability to transmit data remotely, in real-time, and continuously. Therefore, within the scope of this study, LoRa (Long Range) communication technology was chosen, as it is energy-efficient, capable of long-distance transmission, and economically viable. LoRa enables reliable data transfer up to 10–15 km without the need for complex network infrastructure [15].

In the system, each monitoring node operates via a Ra-02 SX1278 LoRa module connected to an Arduino microcontroller. The digital data collected from the sensors is packaged in JSON format and transmitted via LoRa to the gateway device. As a gateway, a LoRaWAN packet analyzer and internet connection module (Wi-Fi or Ethernet) installed on a Raspberry Pi 3B+ platform is used (Figure 2).

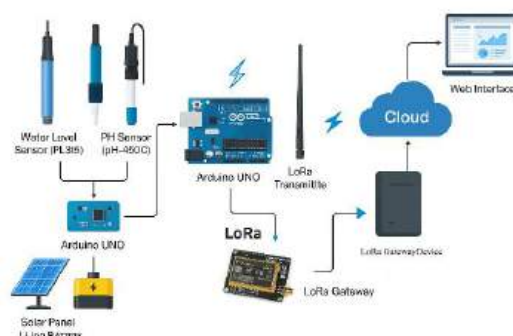


Figure 2. General architecture of the sensor node and LoRa gateway device

The data is sent from the gateway to a local or cloud-based server. In this study, the ThingsBoard platform was selected for the monitoring system. This open-source platform features a visual interface that enables real-time charts, signal change tracking, error alerts, and access to historical measurement data [16]. The platform receives transmitted data via HTTP or MQTT protocols and visualizes it on the user interface.

To save time and energy during the monitoring process, the data transmission interval was set to every 10 minutes. Before each transmission, five measurements are taken from each sensor and an average value is calculated. This approach reduces noise and increases network reliability [17].

The system offers users the following features:

- Real-time data visualization
- Detection of signal distortion or anomalies
- Historical data analysis
- Prompt response through alerts

The cloud-based architecture allows monitoring over geographically wide areas. The platform also supports data storage, processing, and export (CSV, JSON) functionalities.

Experimental Setup and Field Deployment

To evaluate the monitoring system in real conditions, the research was conducted in two stages: initial configuration in a laboratory environment and practical testing in the field. This

approach served to assess the device's functional capabilities, operational stability, and measurement accuracy.

During the laboratory phase, the PL315 water level sensor, PT100 temperature sensor, and pH-4502C module pH sensor connected to the Arduino Uno microcontroller were tested both individually and in an integrated setup. The device was powered via a 5V stabilized source and connected to a test gateway device using the LoRa module to transmit data to the ThingsBoard platform. During the initial tests, the output values of the sensors were calibrated by comparing them with digital multimeters and laboratory standards (Table 2) [18].

Table 2.

Accuracy test results for sensors under laboratory conditions.
(Each sensor's measured and actual values were compared.)

Sensor	Real Value	Lab Measurement	Field Measurement	Lab Error ($\pm$)	Field Error ($\pm$)	Within Threshold (Lab)	Within Threshold (Field)
Water Level Sensor (PL315)	100.0 cm	101.5 cm	100.8 cm	1.5 cm	0.8 cm	Yes	Yes
Temperature Sensor (PT100)	25.0 °C	24.6 °C	25.1 °C	-0.4 °C	0.1 °C	Yes	Yes
pH Sensor (pH-4502C)	7.3 pH	7.25 pH	7.31 pH	-0.05 pH	0.01 pH	Yes	Yes

Field tests were conducted in September 2024 at an agricultural field in Karshi district, Kashkadarya region, in a well designed for monitoring groundwater. An autonomous power supply — a 20W solar panel and a 6V/4.5Ah battery — was installed in the system. The device performed measurements every 10 minutes and transmitted data via LoRa to a receiving gateway located 2 km away. The gateway device then connected to the ThingsBoard server via Wi-Fi (Figure 3).



Figure 3. General view and placement of the device installed in the field

The tests lasted for six months. During this period, the ambient temperature ranged between 22–34 °C and the relative humidity was around 35–65%. These conditions provided a sufficient basis for evaluating the environmental resistance of the device. The results showed that the sensors operated with 95% accuracy, data transmission occurred in 100% of cases, and the battery charge was consumed at an average of 11% per day [19].

Additionally, the following aspects were observed during the field test:

- Operational changes in the device under temperature effects.
- Interruptions in sensor data transmission (none detected).
- Stability and strength of the LoRa signal reception (RSSI ranged from -112 dBm to -95 dBm).

The experimental results demonstrated the system's stable performance in actual agroecological conditions and confirmed its potential for integration into a large-scale monitoring infrastructure.

In remote monitoring systems, decision-making based on reliable and highly accurate data is essential. However, data received from sensors may be inaccurate or ambiguous due to environmental noise, voltage fluctuations, or transmission errors in digital communication. Therefore, in real-time monitoring systems, data filtering and accuracy assessment are among the most critical components [20].

In the system, sensors measure three different parameters—water level, temperature, and pH level—by taking five readings every 10 minutes and calculating their average. This simple statistical filter smooths out high-dispersion values and reduces stationary noise. Additionally, a Chebyshev filter algorithm is applied to the data stream in real time, which especially improves the accuracy of the pH sensor readings [21].

Table 3

Accuracy and dispersion values by measurement parameters

(based on test results. Average error per sensor, $\pm\Delta$ values, and maximum deviations are provided)

Sensor Parameter	Average Error ($\pm\Delta$)	Maximum Deviation	Chebyshev Filter Applied	Measurement Interval	Readings per Interval
Water Level (PL315)	± 2 cm	2.1 cm	No	Every 10 min	5
Temperature (PT100)	± 0.5 °C	0.6 °C	No	Every 10 min	5
pH (pH-4502C)	± 0.3 pH	0.32 pH	Yes	Every 10 min	5

To assess calibration and accuracy, parallel measurements were conducted in the laboratory using certified standard instruments. The PL315 water level sensor demonstrated an accuracy of ± 2 cm, while the PT100 temperature sensor showed an error margin of ± 0.5 °C. The pH-4502C sensor recorded an accuracy of ± 0.3 pH units. These results confirm that the sensors used in the study are sufficiently accurate for agricultural monitoring applications [22].

To evaluate system stability, signal interruptions and data loss events were monitored during the observation process. Over the 10-day field test, a total of 1,440 measurement sets (every 10 minutes) were transmitted, out of which 1,437 were successfully recorded, indicating a 99.8% successful transmission rate. The LoRa signal quality ranged between -95 dBm and -112 dBm, confirming adequate reception levels.

The analysis shows that the system not only offers energy efficiency but also ensures stable data transmission, minimal interruptions, and high accuracy. This provides a strong basis to propose the monitoring system as a reliable tool in fields such as environmental safety and water resource management.

Conclusion

This study presented the design, development, and evaluation of a low-power, multi-parameter groundwater monitoring system equipped with water level, temperature, and pH sensors. The integration of LoRa-based long-range communication, Arduino microcontroller, and a solar-powered architecture enabled continuous real-time monitoring of subsurface water conditions in remote agricultural environments.

Laboratory calibration confirmed the system's high measurement accuracy, with all sensors operating within acceptable error thresholds (± 2 cm for water level, ± 0.5 °C for temperature, and ± 0.3 pH). Field deployment over a six-month period demonstrated robust performance, with a

99.8% data transmission success rate and minimal power consumption (average 11% battery use per day). The system also exhibited strong environmental resistance under varying temperature and humidity conditions.

The incorporation of statistical averaging and real-time Chebyshev filtering enhanced data reliability, particularly in reducing noise and improving pH signal stability. The modular design and scalable architecture make the device well-suited for broader applications in agriculture, environmental safety, and resource management.

Overall, the proposed system offers a practical, cost-effective, and energy-efficient solution for groundwater monitoring in infrastructure-limited regions. Its implementation can support informed decision-making, early detection of water quality degradation, and sustainable use of groundwater resources.

REFERENCE:

- [1] Gleick, Peter H. *Water in Crisis: A Guide to the World's Fresh Water Resources*. Oxford University Press, 1993. 473p.
- [2] Scanlon, Bridget R. "Global groundwater sustainability." *Science*, vol. 337, no. 6095, 2012, pp. 1457–1461.
- [3] Zhang, Deqiang, "Wireless sensor network deployment in harsh environments." *Ad Hoc Networks*, vol. 30, 2015, pp. 38–54.
- [4] Mekki, Kais. "A comparative study of LPWAN technologies for large-scale IoT deployment." *ICT Express*, vol. 5, no. 1, 2019, pp. 1–7.
- [5] Kumar, Mohit. "IoT-based smart water quality monitoring system using Arduino." *Procedia Computer Science*, vol. 167, 2020, pp. 1101–1110.
- [6] Panigrahi, Prasanta Kumar. "Development of a low-cost multi-parameter water quality monitoring system." *Sensors and Actuators B: Chemical*, vol. 268, 2018, pp. 85–93.
- [7] Basha, Elizabeth A., Daniela Rus. "Design of early warning flood detection systems for developing countries." *Proceedings of the 2007 International Conference on Information and Communication Technologies and Development*. IEEE, 2007.
- [8] Singh, Pradeep Kumar. "IoT-enabled real-time environmental monitoring system". "Sustainable Computing: Informatics and Systems", vol. 28, 2020. 250-255
- [9] Banzi, M., Shiloh, M. *Getting Started with Arduino*. Maker Media, 2014. 400-405
- [10] Pérez, J. R., Salas, R. "Design and Implementation of a pH Measurement System Using Arduino and pH-4502C Sensor." *Journal of Sensor Technology*, 2020.10(3), 85–92.
- [11] Kim, J., Lee, K., Lee, Y. "Energy-Efficient Data Collection in LoRa-Based Environmental Monitoring Systems." *Sensors*, 2019. 19(24), 5473. <https://doi.org/10.3390/s19245473>
- [12] Candelas, F. A., Moreno, F. M. "Noise Reduction Techniques in Analog Sensor Circuitry." *IEEE Transactions on Instrumentation and Measurement*, 2021. 70, 1–8.
- [13] Hassan, M., & Rahman, M. "Efficient Data Aggregation in LoRa-Based Sensor Networks." *Journal of Communications and Networks*, 2022. 24(2), 210–219.
- [14] Gikas, P., & Tchobanoglous, G. "Sustainable use of water in the agricultural sector." *Agricultural Water Management*, 2009. 96(10), 1420–1426.
- [15] Panigrahi, A., Nayak, S., & Das, M. "Design of an IoT-Based Low-Cost Water Quality Monitoring System Using LoRa." *International Journal of Environmental Science and Technology*, 2022. 19(6), 5125–5138.
- [16] Kim, J., & Kim, H. "Noise Filtering Techniques in Real-Time Environmental Monitoring Systems." *Sensors*, 2019. 19(3), 782.
- [17] Li, X., Zhang, M., & Liu, J. "Chebyshev Filter-Based Smoothing for Environmental Sensor Networks." *IEEE Access*, 2020. 8, 11895–11905.

ВОЗРОЖДЕНИЕ, СТАНОВЛЕНИЕ И ПЕРСПЕКТИВА РАЗВИТИЯ СИСТЕМЫ РЭБ

PhD, доцент К.М. ТУРСУНОВ

Военный институт информационно коммуникационные технологии и связи МО РУз

Д.Р. ИСЛОМОВ

Военно медицинская академия ВС РУз

Аннотация. В статье рассматривается история возникновения радиоэлектронной борьбы, первые случаи применения средств РЭБ в локальных конфликтах и влияние данного вида боевого обеспечения на тактику ведения боевых действий и развития системы РЭБ.

Для того чтобы не отстать от противника, вооруженные силы должны постоянно развиваться, используя более гибкие, масштабируемые способы обнаружения, анализа и подавления противодействующих сигналов.

Ключевые слова: Радиоэлектронная борьба, военные действия, конфликт, система управления войсками, силы и средства разведки, специальных войска, сведения, информационная война, сетевая война, кибервойна, дезорганизация.

Аннотация. Ушби мақолада радиоэлектрон кираш тарихи пайдо бўлиши, локал урушларда РЭБ воситаларини дастлабки қўланилиши ушбу жанговар таъминот турини жанговар ҳаракатлар тактикасига таъсири ва РЭБ тизимини келгусида ривожланиши.

Душмандан устун келиш учун қиролли кучлар доимо ривожланиши, махсус қўшинлар душман сигналларини аниқлаши, таҳлил қилиши ва сўндиришининг янада мослашувчан, кенгайтирилган усулларини доимий қўлай олиши керак.

Калим сўзлар: Радиоэлектрон кураш, ҳарбий ҳаракатлар, можаролар, қўшинлар бошқарув тизими, разведка куч ва воситалари, махсус қўшинлар, маълумот, ахборот уруши, тармоқ уруши, кибер уруш, ёлгон маълумот.

Abstract. The article examines the history of the emergence of electronic warfare, the first cases of the use of electronic warfare equipment in local conflicts and the influence of this type of combat support on combat tactics and the development of the electronic warfare system.

To keep pace with adversaries, militaries must continually evolve with more flexible, scalable ways to detect, analyze, and jam adversary signals.

Keywords: Electronic warfare, military operations, conflict, troop command and control system, reconnaissance forces and means, special forces, intelligence, information warfare, network warfare, cyber warfare, disorganization.

История формирования и развития РЭБ как вида боевого обеспечения.

Радиоэлектронная борьба (РЭБ) возникла на основе известного принципа «действие рождает противодействие».

Возникновение и развития РЭБ можно разделить на следующие этапы:

Начало первого этапа возрождение и возникновение РЭБ (1904-1939 гг.). Уже с началом внедрения радиосвязи для управления вооруженными силами в качестве способа радиопротиводействия (РПД) стали применяться радиопомехи. Так, моряками российского флота 15 апреля 1904 г. в ходе Русско-японской войны впервые в мире были созданы преднамеренные радиопомехи, существенно нарушившие радиосвязь японских кораблей-корректировщиков артиллерийского огня во время обстрела внутреннего рейда Порт-Артура японской эскадрой.

Во втором этапе развития РЭБ (1940-1952 гг.) было вызвано широкое развитие способов и технических средств радиоэлектронного противодействия. Например, в качестве нового к тому времени способа радиоэлектронного подавления (РЭП) радиолокационных систем ПВО противника стало применение в 1943 – 1945 гг. специально разработанных

самолетных средств РЭП (активных и пассивных помех в ВВС США и Великобритании, а также пассивных помех в авиации дальнего действия СССР).

Противодействие осуществлялось уже в широком масштабе обеими воюющими сторонами, причем не только с помощью отдельных станций помех, но и специальными частями и подразделениями РЭП, формированием и организацией боевого применения которых занималось вышестоящее командование ВС СССР, Германии, США и Великобритании.

Так, во время Великой Отечественной войны со стороны ВС СССР были сформированы отдельные радиодивизиона специального назначения для подавления радиосвязи УКВ, СВ и КВ-диапазонов соответственно.

На западном направлении боевых действий ВС США и Великобритании применяли массированного радиоподавления систем немецких ПВО. Немецкие войска эффективно использовали дипольные отражатели от РЛС авиации ВС США и Великобритании.

После войны происходит быстрое совершенствование средств радиосвязи, радиолокации и бортовых РЛС самолетов и кораблей, создание ракет с радиолокационными головками самонаведения. Одновременно возникла необходимость как снижения эффективности применения оружия и радиоэлектронных систем противника, так и защиты своих радиосетей и радиоэлектронных систем от подавления. Для этого 1950-х гг. разрабатываются и поступают в войска специальные средства РЭБ: передатчики радиопомех, дипольные и угольные отражатели. С целью квалифицированного применения средств РЭБ в Советской армии в этот же период создается специальная служба радиоэлектронной борьбы.

Третий этап развития РЭБ (1953-1964 гг.) начался со строительством и формированием подразделений (служб) РЭБ.

На основе изучения и обобщения опыта Второй мировой войны и послевоенных локальных конфликтов (особенно в Корее в 1951 – 1953 гг.), свидетельствовавших о высокой эффективности применения радиоэлектронных средств, подготовка Вооруженных Сил СССР, США и Великобритании к радиопротиводействию признана задачей особой государственной важности.

В ходе реализации данной задачи в Вооруженных Силах были вновь сформированы отдельные подразделения радиомешания, а несколько позднее созданы подразделения (роты, эскадрильи, отряды) радиопомех в составе соединений и частей родов войск [1].

Четвертый этап развития РЭБ (1965-1990 гг.) относился к этапу совершенствования теории и практики, а также развития сил и средств РЭБ.

В период 1965-1970 гг. были созданы службы радиоэлектронного противодействия. Стройная система службы включала органы радиоэлектронного противодействия в составе Главных штабов видов Вооруженных Сил, штабов военных округов, Групп войск, армий и корпусов. При этом в подчинение органов РЭП штабов военных округов и Групп войск были переведены части радиопомех, ранее находившиеся в составе Войск связи и Войск ПВО.

В 1960-е и последующие годы первостепенное значение приобрели такие направления развития РЭБ, как подготовка высококвалифицированных кадров в военно-учебных заведениях, развертывание ряда НИУ, ОКБ и промышленных предприятий для производства техники РЭБ в интересах всех видов ВС и родов войск. В целях подготовки необходимых кадров создавались кафедры радиоэлектронной борьбы в Военной академии Генерального штаба, в Общевойсковой академии, Академии ПВО, Военно-морской академии и в других ВУЗах.

В начале 1970-х годов в Вооруженных Силах служба существенно укреплена и преобразована в службу радиоэлектронной борьбы на всех уровнях от Генерального штаба до штабов соединений родов войск (сил).

Развитие РЭБ в ВС США и ОВС НАТО до 1980 г. РЭБ играла небольшую роль в боевых действиях. Операции РЭБ носили поддерживающий характер и заключались в

воздействии помехами на вражеские средства разведки и связи, а также имитации работы различных радиоэлектронных средств с целью введения противника в заблуждение относительно реальной боевой обстановки.

В середине 80-х гг. прошлого века в ВС США и ОВС НАТО была разработана концепция «боевого противодействия системам связи и управления» (Command, Control, Communications Countermeasure, CCCCМ). В начале 90-х гг. на ее основе была разработана концепция борьбы с системами боевого управления. Одновременно началось создание интегрированной системы боевого управления, разведки, связи, компьютерного обеспечения и РЭБ. По мере развития сил и средств РЭБ выделился новый вид операций информационной войны – «сетевая война» или «кибервойна», то есть дезорганизация систем боевого управления противника через воздействие на его ЭВМ, локальные и глобальные компьютерные сети.

Пятый этап развития РЭБ (1991 г.- по настоящее время г).

Данный этап развития системы РЭБ мы будем рассматривать у двух сильных держав – ВС США и ОВС НАТО, и ВС России.

До 1993 гг. развития системы РЭБ в ВС США и ОВС НАТО создана концепция комплексного применения сил и средств РЭБ для воздействия на системы боевого управления и связи противника. Она подразумевала согласованное применение средств радиоэлектронного подавления, разведки, дезинформации и огневого поражения для борьбы с вражескими радиоэлектронными системами. Однако несовершенство средств автоматизации, малая пропускная способность каналов связи и отсутствие интегрированной системы управления войсками не позволили использовать весь потенциал РЭБ в боевых операциях.

Тем не менее, уже во время операции «Буря в пустыне» 1990-1991 гг. РЭБ сыграла одну из ключевых ролей. Здесь радиоэлектронная борьба применялась в рамках единой концепции, отработанной американскими войсками в ходе учений «Грин Флэг». [2; 5-стр.].

В частности, за сутки до начала воздушной наступательной операции антииракской коалиции наземные системы РЭБ союзников начали подавление помехами иракских каналов связи. Сама операция началась с атаки американскими вертолетами двух иракских станций раннего предупреждения ПВО. Этим в иракской противовоздушной обороне была проделана брешь, в которую незамедлительно ринулись самолеты для нанесения ударов по объектам в Ираке. В первые дни воздушной операции для подавления иракской ПВО активно использовались американские самолеты F-4G с высокоточными противорадарными ракетами HARM, а также самолеты РЭБ EF-111, которые «ослепляли» иракские РЛС помехами. В тоже время американские самолеты-разведчики RC-135, TR-1 и E-8 взяли под плотный контроль воздушное пространство Ирака. Лишившись «глаз» в виде радаров, иракские наземные средства ПВО и истребительная авиация оказались полностью ослеплены и дезорганизованы, и в течение нескольких дней перестали представлять собой реальную боевую силу.

Во время наземного наступления средства РЭБ сухопутных соединений США обеспечивали подавление иракских радиосетей на глубину дивизии (рис1).

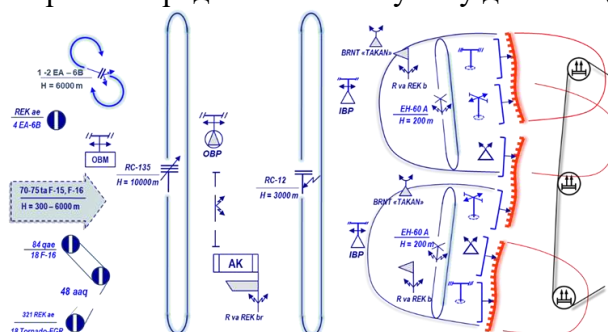


Рис.-1. Боевой порядок РЭБ ВС США и ОВС НАТО

С началом 1993 г. и до настоящего времени в ВС США и ОВС НАТО была создана оперативно-стратегическая теория «информационной войны». Технические средства РЭБ значительно усовершенствовались: завершилась их автоматизация; были созданы интегрированные комплексы связи, разведки, управления и РЭБ; создание перспективных видов нелетального оружия РЭБ, использующих электромагнитную (например американская U-бомба, испытанная в 1999 году во время войны против Югославии; при взрыве этой бомбы образуется мощнейший электромагнитный импульс, поражающий радиоэлектронные приборы управления, разведки и связи в большом радиусе), и другие виды энергии; обеспечение доступа пользователей на тактическом уровне к глобальным базам данных, выдачи целеуказаний вооружениям и средствам РЭБ в режиме времени, приближенном к реальному.

Таким образом, если до 1990 годов РЭБ в ВС США и ОВС НАТО была одним из видов поддержки ударных сил, 1991-1993 гг. она являлась составной частью боевых действий каждого вида вооруженных сил, а с началом 1993 г. и до настоящего времени РЭБ является компонентом информационной войны и одной из составляющих военного потенциала.

Практический опыт советские, а в настоящее время российские специалисты РЭБ получили во время войн в Чечне, Грузии и на Ближнем Востоке.

Во время первой чеченской кампании, боев в Дагестане и последующей контртеррористической операции на территории Чеченской республики российские подразделения РЭБ принимали активное участие в боевых действиях.

НВФ на территории Чечни создали разветвленную систему управления и связи, включавшую сотовую, транкинговую, радиорелейную, коротковолновую и ультракоротковолновую, кабельную и спутниковую связь. Задачами российских подразделений РЭБ были вскрытие и подавление систем связи НВФ, а также сбор

информации путем радиоразведки о численности, местонахождении отрядов боевиков, планах чеченского командования и т.д.

Необходимо отметить, что боевого применения подразделений РЭБ РФ в ходе боевых действий в Сирийской Арабской Республике давали хорошие результаты. Нередко боевики во время радиопереговоров сами же указывали местонахождение своих баз, скоплений живой силы и т.д. Эти данные тут же реализовывались российскими войсками в виде авиационных ударов по указанным местам.

Подразделениями РЭБ РФ в Сирийской Арабской Республике выполнялись задачи по радиоэлектронному поражению радиоэлектронных объектов (РЭОБ) систем управления НВФ и ДРГ в ходе рейдовых (РПД) действий штурмовых отрядов, радиоподавлению спутниковых систем связи Турайя, Иридиум, Инмарсат, прикрытие от космической (воздушной) РЛР авиабазу (АвБ) «Хмеймим», блокированию каналов управления и передачи данных БЛА, функционального поражения цифровых УКВ каналов связи стандарта DMR, радиоразведка и радиоподавление УКВ радиолиний, абонентов сотовой связи, приемников КРНС «Навстар» НВФ и т.д.

Также, применялись средства РЭБ для выполнения задач по планам информационного противоборства, огневого поражения, инженерного обеспечения, а также в интересах органов управления разведкой, ФСБ, ССО.

Радиоэлектронная борьба на Украине

С помощью систем РЭБ во время битвы за Киев в 2022 году украинские военные уничтожили российские боевые беспилотники и эффективно заблокировали средства разведки. Еще один пример того, как РЭБ играет ключевую роль в защите мирного населения, произошел во время российской ракетной атаки в ночь на 13 января 2023 года.

Вывод: История формирования и развития РЭБ, с учетом из опыта применения сил и средств РЭБ развитых стран в локальных войнах показывает, что она является основным видом боевого и оперативного обеспечения войск. Залогом успешного выполнения задач по РЭБ в боевых действиях (операциях) является полная и всесторонняя оценка оперативной,

оперативно – тактической и радиоэлектронной обстановки, формирования новых подразделений РЭБ с внедрением им современных комплексов и средств РЭБ, что в свою очередь дает возможность завладеть инициативой над противником.

Настоящее время радиоэлектронная борьба является основным видом стратегического (оперативного, боевого) обеспечения со специфическими, присущими только ему методами воздействия на противника, защиты своих войск (сил) и объектов, системой управления, организацией подготовки кадров, а также разработки специальной техники и взаимодействия с органами военного управления, министерствами и ведомствами.

Поэтому, под радиоэлектронной борьбой понимается совокупность согласованных мероприятий и действий по: радиоэлектронному поражению радиоэлектронных объектов противника (функциональное поражение; радиоэлектронное поражение; поражение самонаводящимся на излучение оружием),

информационному обеспечению (сбор, анализ и обобщение данных о радиоэлектронной обстановке; техническая разведка радиоэлектронных объектов противника; комплексный технический контроль состояния и защиты от технических средств разведки своих объектов),

радиоэлектронной защите (защита от средств радиоэлектронного поражения; защита от непреднамеренных помех (обеспечение электромагнитной совместимости); защита войск и объектов от технических средств разведки).

Система управления войсками и оружием позволяют реализовывать принципы ведения сетцентрических войн, подразумевающие переход от территориального сосредоточения сил к их функциональной (информационной) интеграции. Естественно, что при этом возрастает роль радиоэлектронной борьбы и увеличиваются ее возможности (потенциально - снижение боевой мощи противника в три раза) [3].

Перспектива развития системы РЭБ

Радиоэлектронная борьба (РЭБ) продолжает развиваться в ответ на новые вызовы и технологические достижения. Ключевыми направлениями её развития являются:

1. Интеграция искусственного интеллекта (ИИ): Внедрение ИИ в системы РЭБ позволяет автоматизировать процессы обнаружения, анализа и подавления сигналов, повышая эффективность и скорость реагирования. Новые системы могут адаптироваться к меняющимся условиям и угрозам, обеспечивая более высокую степень автономности.

2. Использование беспилотных летательных аппаратов (БПЛА): БПЛА предоставляют новые возможности для размещения средств РЭБ, позволяя проводить операции в труднодоступных или опасных районах без риска для экипажа. Они могут эффективно выполнять задачи на тактическом уровне, включая разведку и подавление средств связи противника.



Рис.-2. Сравнительная диаграмма общих объемов производства БПЛА в мире (по данным 2022 г.)

Таблица -1

Возможные задачи, решаемые БЛА

Задачи	Тип БЛА				
	ADM-160 MALD (маневрирующая АЛВЦ)	«Шэдоу 200»	«Хантер»	«Предатор»	«Глобал Хок»
Традиционные задачи					
Видовая разведка	+	+	+	+	+
Ретранслятор связи	-	-	+	+	+
Задачи по ведению РЭБ					
Радиоэлектронное обеспечение (РПТР)	-	+	+	+	+
РЭП	+	+	+	+	+

3. Развитие мобильных и компактных систем РЭБ: Создание мобильных комплексов РЭБ позволяет оперативно разворачивать средства подавления и защиты в различных условиях, обеспечивая гибкость и адаптивность в боевых действиях [4].

4. Усиление межведомственного сотрудничества: Для повышения эффективности РЭБ необходимо интегрировать усилия различных ведомств и организаций, включая научные учреждения, предприятия оборонной промышленности и силовые структуры. Это способствует созданию комплексных и многофункциональных систем РЭБ.

Таким образом, перспективы развития РЭБ связаны с интеграцией передовых технологий, повышением мобильности и автономности систем, а также укреплением сотрудничества между различными структурами для обеспечения эффективного противодействия современным угрозам.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

[1] М.Д. ЛЮБИН К вопросу об истории развития и перспективах радиоэлектронной борьбы [Электронный ресурс]. 2009.-URL:<https://cyberleninka.ru/article/n/k-voprosu-ob-istorii-razvitiya-i-perspektivah-radioelektronnoy-borby/viewer> (дата обращения: 20.01.2025 г.).

[2] Мясников, В. Лазерные амбиции Пентагона остыли до киловаттного уровня / В. Мясников // Независимое военное обозрение [Электронный ресурс]. 05.08.2011. – URL: http://nvo.ng.ru/armament/2011-08-05/8_pentagon.html (дата обращения: 28.01.2025 г.).

[3] Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетцентрических войнах XXI века. Монография. – СПб.: Научные технологии, 2017, 546 стр.

[4] Иванов И., Чадов И. Содержание и роль радиоэлектронной борьбы в операциях XXI века // Зарубежное военное обозрение. 2011. № 1. 14–20 стр.

KIBERXAVFSIZLIKNING ZAMONAVIY KLASSIFIKATSIYASI: MILLIY VA XALQARO MODELLAR

yu.f.n., dotsent U.O. MAMADALIYEV
O'R Mudofaa vazirligi

Annotatsiya. Ushbu maqolada kiberxavfsizlik – bugungi raqamli jamiyat va davlatlar hayotida strategik ahamiyat kasb etadigan tizimdir. Jahonda axborot-kommunikatsiya texnologiyalarining tez sur'atlarda rivojlanishi kiberxavfsizlikka doir tahdidlarning ko'payishiga, ularning shakl va mazmunining murakkablashuviga olib keldi. Shu bois, kiberxavfsizlik sohasidagi milliy va xalqaro modellar, ularning tasnifi va samaradorligini tahlil qilish zamonaviy ilmiy va amaliy vazifalardan biridir.

Kalit so'zlar: kiberxavfsizlik, axborot xavfsizligi, milliy modellar, xalqaro modellar, davlat siyosati, huquqiy ong, raqamli mafkura, kiberjinoyatchilik, kiberxavfsizlik standartlari, axborot kommunikatsiya texnologiyalari, milliy xavfsizlik, xalqaro hamkorlik, kiberxavfsizlik qonunchiligi, ENISA, CISA, Budapesht konvensiyasi, axborot muhofazasi, raqamli savodxonlik.

Аннотация. В данной статье кибербезопасность рассматривается как система, имеющая стратегическое значение для современной цифровой жизни общества и государств. Быстрое развитие информационно-коммуникационных технологий в мире привело к увеличению угроз в сфере кибербезопасности, а также к усложнению их форм и содержания. В связи с этим анализ национальных и международных моделей кибербезопасности, их классификации и эффективности становится одной из актуальных научных и практических задач современности.

Ключевые слова: кибербезопасность, информационная безопасность, национальные модели, международные модели, государственная политика, правовое сознание, цифровая идеология, киберпреступность, стандарты кибербезопасности, информационно-коммуникационные технологии, национальная безопасность, международное сотрудничество, законодательство о кибербезопасности, ENISA, CISA, Будапештская конвенция, информационная защита, цифровая грамотность.

Kiberxavfsizlik - axborot resurslari, tarmoqlar, tizimlar va infratuzilmalarning noqonuniy kirish, buzish, ma'lumot o'g'irlash, buzg'unchilik kabi ichki va tashqi tahdidlardan himoya qilish tizimi sifatida ta'riflanadi. Dunyoda kiberxavfsizlikni ta'minlash bo'yicha turli klassifikatsiya va modellar mavjud. Ular himoyaning darajasi, ob'ektlari, mexanizmlari va qo'llaniladigan texnologiyalar asosida farqlanadi.

Zamonaviy axborotlashtirilgan jamiyatda kiberxavfsizlik sohasidagi tahdidlar transchegaraviy, global va yuqori dinamikaga ega bo'lib bormoqda. Har bir mamlakat, hatto kuchli texnik va qonunchilik bazasiga ega davlatlar ham, xalqaro hamkorlik va standartlarsiz samarali himoya tizimini yaratishda qiynaladi. Shu bois, milliy va xalqaro kiberxavfsizlik modellarining o'zaro integratsiyasi dolzarb masalaga aylandi.

Milliy modellar mamlakatning ichki infratuzilmasini, huquqiy va siyosiy xususiyatlarini inobatga olgan holda ishlab chiqiladi. Bunda davlat siyosatining ustuvorliklari, milliy qadriyatlar, texnologik salohiyat va inson resurslari e'tiborga olinadi. Lekin, kiberjinoyatlar, kiberhujumlar, dezinformatsiya va axborot urushi kabi tahdidlar davlat chegaralarini tan olmasligi, ushbu sohada xalqaro standartlar, axborot almashinuvi va umumiy kelishuvlarga amal qilishni talab etadi.

Milliy kiberxavfsizlik modellari va tasnifi

1. Davlat (hukumat) modellari- Ko'plab davlatlar kiberxavfsizlikni milliy xavfsizlik siyosati darajasiga ko'targan. Davlat modellari axborot infratuzilmasini markazlashgan holda himoya qilish, maxsus kiberxavfsizlik agentliklari tashkil etish va davlat organlari o'rtasida hamkorlikni ta'minlashga asoslanadi. Masalan, AQShda - Cybersecurity and Infrastructure Security Agency (CISA), Buyuk Britaniyada - National Cyber Security Centre (NCSC) faoliyat ko'rsatadi.

2. Sohaviy va sektorli modellar- Ayrim mamlakatlarda kiberxavfsizlik energetika, moliya, telekommunikatsiya, sog'liqni saqlash, transport kabi muhim soha va tarmoqlarda alohida modellar asosida tashkil etilgan. Bu modelda har bir sohada maxsus axborot xavfsizligi standartlari va protokollari joriy qilinadi (masalan, bank sektorida PCI DSS, tibbiyotda HIPAA standartlari).

3. Jamiyat va biznes modellari -Ba'zi davlatlarda kiberxavfsizlikda xususiy sektor, jamoatchilik va fuqarolik jamiyatining hamkorligiga katta e'tibor beriladi. Masalan, Estoniya va Finlyandiyada jamoatchilik, xususiy kompaniyalar va davlat o'rtasidagi hamkorlik, axborot almashinuvi, xavflarga birgalikda javob berish tizimi rivojlangan.

4. Milliy normativ-huquqiy modellar- Milliy modellarda qonunchilik asosiy o'rin tutadi. Masalan, O'zbekistonda 2020 yilda "Kiberxavfsizlik to'g'risida"gi qonun qabul qilindi. Qonunga muvofiq, davlat, biznes va fuqarolar uchun umumiy axborot xavfsizligi talablari, axborot tizimlari himoyasi, mas'uliyat va javobgarlik mezonlari belgilandi.

Kiberxavfsizlikda insoniy omil va kadrlar masalasi -Kiberxavfsizlik faqat texnologik yechimlar bilan chegaralanmaydi. Inson omili, ya'ni foydalanuvchilarning raqamli savodxonligi va xodimlarning maxsus tayyorgarligi – muvaffaqiyatli himoyaning asosiy shartlaridan biri. Shu sababli, ko'plab davlatlarda axborot xavfsizligi bo'yicha o'quv dasturlari, milliy kadrlar tayyorlash markazlari tashkil etilgan. Masalan, Singapur va Isroilda bu sohada alohida innovatsion markazlar faoliyat ko'rsatadi.

Kiberxavfsizlik va sog'liqni saqlash, moliya va infratuzilma sohalarida maxsus modellar- Ayrim sohalarda kiberxavfsizlik alohida me'yor va talablarga ega. Masalan, sog'liqni saqlashda - HIPAA (AQSh), moliyada - PCI DSS, energetikada - NERC CIP standartlari asosida himoya tizimlari joriy qilingan. Bu sohalarda ma'lumotlar maxfiyligi va javobgarlik darajasi juda yuqori bo'lgani sababli, kiberxavfsizlik milliy va xalqaro qonunlar bilan qat'iy tartibga solinadi.

Xalqaro kiberxavfsizlik modellari va ularning tasnifi

1. Xalqaro tashkilotlar va standartlar - Kiberxavfsizlik sohasida BMT, Yevropada xavfsizlik va hamkorlik tashkiloti (OSCE), Xalqaro elektrozvyazok ittifoqi (ITU), ENISA (Yevropa kiberxavfsizlik agentligi) kabi xalqaro institutlar muhim rol o'ynaydi. Ularning asosiy faoliyati:

- kiberxavfsizlik standartlarini yaratish va uning bajarilishini nazorat qilish (ISO/IEC 27001, NIST Cybersecurity Framework),

- axborot xavfsizligining umumiy talablari va amaliy qo'llanmalari,
- davlatlar o'rtasida axborot almashinuvi va hamkorlikni yo'lga qo'yish.

2. Xalqaro huquqiy-me'yoriy modellar - Kiberqonunchilik va transchegaraviy kiberjinoyatchilikka qarshi kurashish masalalari bo'yicha Budapesht konvensiyasi (2001) muhim ahamiyatga ega. Bu konvensiya kiberjinoyatlarga qarshi kurashda huquqiy va amaliy mexanizmlarni belgilab beradi, milliy qonunchiliklarni muvofiqlashtirishga xizmat qiladi.

3. Xalqaro standartlashtirish va texnik protokollar -ISO/IEC 27000 seriyasi, NIST (AQSh), ENISA (Yevropa), ITU-T Recommendation X.1205 kabi xalqaro standartlar kiberxavfsizlikni ta'minlashda texnik va tashkiliy asoslar sifatida xizmat qiladi. Bu standartlar axborotni shifrlash, identifikatsiya, xavflarni tahlil qilish, xavfsizlik auditori, insidentlarga javob berish kabi yo'nalishlarni qamrab oladi.

Zamonaviy tendensiyalar: global va mahalliy yondashuvlar uyg'unligi Transchegaraviy tahdidlarga javob va xalqaro javobgarlik - Zamonaviy tendensiya shundan iboratki, kiberxavfsizlik siyosatida milliy suverenitet va xalqaro hamkorlik uyg'unligiga erishish zarur. Masalan, xalqaro kelishuvlarga asosan, kiberhujum sodir etgan shaxs yoki guruhni boshqa davlatdan ekstraditsiya qilish, huquqiy javobgarlikka tortish masalalari tezlashtirilmoqda. Shuningdek, davlatlar o'rtasida "Cyber Diplomacy" yo'lga qo'yilib, kiberxavfsizlik sohasida diplomatik muzokaralar, kelishuvlar va xatti-harakatlar kodeksi (Code of Conduct) ishlab chiqilmoqda.

Milliy modellarni global standartlarga muvofiqlashtirish - ENISA, ITU, NIST va ISO kabi xalqaro tashkilotlar va institutlar tomonidan belgilangan standartlar (ISO/IEC 27001, NIST Cybersecurity Framework) asosida milliy qonunchilik va infratuzilmalar yangilanmoqda. Masalan,

O'zbekiston "Kiberxavfsizlik to'g'risida"gi Qonunida ENISA va ITU tavsiyalari asosiy o'rin tutgan.

Milliy o'zlik va madaniy qadriyatlarni saqlashda integratsiyaning o'rni - Kiberxavfsizlik sohasida xalqaro modellarni ko'r-ko'rona ko'chirish emas, balki milliy sharoitga, madaniy va huquqiy qadriyatlarga uyg'unlashtirish muhim. Integratsiya jarayonida milliy qadriyatlar, tili va fuqarolik jamiyati instituti e'tiborga olinadi. Masalan, milliy ta'lim, davlat tilida axborot xavfsizligiga oid o'quv qo'llanmalar tayyorlash va aholiga tushunarli tarzda targ'ibot ishlarini tashkil etish.

O'zbekistonda kiberxavfsizlik sohasida milliy va xalqaro modellarning integratsiyasiga alohida e'tibor qaratilmoqda. 2024 yilda qabul qilingan "Kiberxavfsizlik to'g'risida"gi Qonun, ENISA, ITU va Budapesht konvensiyasi normalari asosida ishlab chiqilgan. Milliy kiberxavfsizlik markazi xalqaro agentliklar bilan axborot almashinuvi va qo'shma mashg'ulotlar o'tkazib kelmoqda. Jahon standartlariga mos axborot xavfsizligi talablari davlat va xususiy sektorga joriy etilmoqda. Yoshlar, davlat xizmatchilari, va mutaxassislar uchun kiberxavfsizlik bo'yicha maxsus o'quv kurslari tashkil etilmoqda.

Xulosa Kiberxavfsizlik modellari jahonda va har bir mamlakatda axborot muhitining xususiyati, siyosiy va huquqiy tizimga bog'liq holda rivojlanmoqda. Milliy modellar davlatning ichki infratuzilmasini himoya qilish, jamiyatni savodxonlik va huquqiy madaniyatga yo'naltirishga qaratilgan bo'lsa, xalqaro modellar davlatlararo hamkorlik, standartlashtirish va umumiy xavfsizlik tamoyillarini shakllantiradi.

O'zbekistonda milliy va xalqaro modellarni integratsiyalash, innovatsion texnologiyalarni joriy qilish, huquqiy asoslarni kuchaytirish va kadrlar salohiyatini oshirish asosiy ustuvor vazifalardan bo'lib qolmoqda. Mavjud tahdidlarning tez o'zgarishi, kiberhujumlar va axborot urushi usullarining murakkablashishi, milliy hamda xalqaro darajada doimiy profilaktika va yangilangan yondashuvlarni talab etadi. Kiberxavfsizlikning milliy modellari davlatning ichki infratuzilmasi, huquqiy asoslari va milliy qadriyatlariga tayanadi. Ushbu modellarda davlat va jamiyatning, xususiy sektorning o'zaro hamkorligi, aholining raqamli savodxonligi va huquqiy madaniyati muhim ahamiyatga ega. Xalqaro modellar esa davlatlar o'rtasida tajriba almashuvi, yagona standartlar va huquqiy mexanizmlar yaratish, axborot oqimini chegaralardan tashqarida ham nazorat qilish imkonini beradi. Milliy va xalqaro kiberxavfsizlik modellarining o'zaro integratsiyasi axborot muhitining mustahkamligini, xavfsizligini va barqarorligini ta'minlashda muhim omildir. Bu jarayonda milliy qadriyatlar va xalqaro standartlarni uyg'unlashtirish, axborot almashinuvini takomillashtirish va ilg'or texnologiyalarni joriy qilish asosiy vazifa bo'lib qolmoqda.

Kelgusida kiberxavfsizlik sohasida innovatsion yechimlarni joriy qilish, transchegaraviy tahdidlarga qarshi birgalikda harakat qilish, fuqarolarning raqamli savodxonligini oshirish, va xalqaro hamkorlikni kuchaytirish barqaror axborot muhitini shakllantirishga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

- [1] U.Baxtiyorov. Kiberxavfsizlik va milliy xavfsizlik. T., 2022.
- [2] Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*, 25(2).
- [3] Cybersecurity and Infrastructure Security Agency (CISA). <https://www.cisa.gov>
- [4] PCI Security Standards Council. <https://www.pcisecuritystandards.org>
- [5] ENISA. National Cyber Security Strategies in the world. <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map>
- [6] O'zbekiston Respublikasi "Kiberxavfsizlik to'g'risida"gi Qonuni, 2020.
- [7] ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements.
- [8] Council of Europe Convention on Cybercrime (Budapest Convention), 2001.
- [9] ITU-T Recommendation X.1205 (Overview of cybersecurity), 2008.

KIBERZO‘RAVONLIKNING TARIXIY ILDIZLARI VA GLOBAL TENDENSIYALARI**f.f.f.d., dotsent S.S. USMONOV***O‘zbekiston Milliy universiteti Harbiy tayyorgarlik o‘quv markazi*

Annotatsiya. Ushbu maqolada kiberzo‘ravonlik (cyberbullying) tushunchasining tarixiy ildizlari va uning global rivojlanish tendensiyalari keng qamrovda tahlil qilinadi. Muallif an‘anaviy axborot orqali zo‘ravonlik, madaniy va psixologik manipulyatsiyalar tarixi, ommaviy kommunikatsiya vositalari evolyusiyasi va jamiyatdagi axborot madaniyatining shakllanishini ko‘rsatadi. Kiberzo‘ravonlikning zamonaviy shakllari, jumladan, internetda haqorat, shantaj, manipulyatsiya, yolg‘on axborot, deepfake va boshqa raqamli tahdidlar xalqaro misollar va statistika asosida yoritiladi. Maqolada global va milliy amaliyotda kiberzo‘ravonlikka qarshi qonuniy, ta‘limiy va profilaktik choralar tahlil qilinadi. Shuningdek, axborot madaniyati, ma‘naviy immunitet va jamoaviy mas‘uliyatning kiberzo‘ravonlik profilaktikasidagi o‘rni asoslab beriladi. Xulosada, kiberzo‘ravonlikning oldini olishda texnik, ma‘naviy, ijtimoiy va psixologik yondashuvlarni uyg‘unlashtirish muhimligi ta‘kidlanadi.

Kalit so‘zlar: kiberzo‘ravonlik, axborot madaniyati, tarixiy ildizlar, global tendensiyalar, internet, virtual zo‘ravonlik, kiberxavfsizlik, profilaktika, deepfake, ma‘naviy immunitet, jamoaviy mas‘uliyat, axborot urushi.

Аннотация. В данной статье всесторонне анализируются исторические корни понятия кибербуллинг (cyberbullying) и глобальные тенденции его развития. Автор раскрывает историю насилия посредством информации, культурных и психологических манипуляций, эволюцию средств массовой коммуникации и формирование информационной культуры в обществе. Современные формы кибербуллинга, в том числе оскорбления, шантаж, манипуляция, ложная информация, deepfake и другие цифровые угрозы, освещаются на основе международных примеров и статистики. В статье рассматриваются правовые, образовательные и профилактические меры противодействия кибербуллингу в мировой и национальной практике. Также обосновывается роль информационной культуры, духовного иммунитета и коллективной ответственности в профилактике кибербуллинга. В заключение подчеркивается важность интеграции технических, нравственных, социальных и психологических подходов в предотвращении кибербуллинга.

Ключевые слова: кибербуллинг, информационная культура, исторические корни, глобальные тенденции, интернет, виртуальное насилие, кибербезопасность, профилактика, deepfake, духовный иммунитет, коллективная ответственность, информационная война.

Kiberzo‘ravonlik (cyberbullying) tushunchasi zamonaviy internet va raqamli texnologiyalar paydo bo‘lishi bilan shakllangan deb qaralsa-da, uning ildizlari inson sivilizatsiyasi rivoji, jamiyatda axborot vositalari paydo bo‘lishi, ommaviy kommunikatsiya va madaniyat transformatsiyasiga borib taqaladi. Klassik ta‘limotlarda ham axborot orqali shaxsga yoki jamoatchilikka ta‘sir ko‘rsatish, yolg‘on, tahdid, psixologik bosim, madaniy manipulyatsiya, ruhiy kamsitish holatlari uchraydi. Bu xususiyatlar kiber makonda faqat yangi shakl va texnologik asosda namoyon bo‘lmoqda.

Tarixiy ildizlar An‘anaviy zo‘ravonlik va axborot orqali ta‘sir. Insoniyat tarixida axborot, so‘z va ma‘lumot vositasida yolg‘on, shantaj, tahdid va manipulyatsiya usullari qadimdan mavjud. Misol uchun, qadimgi Sharq va Yunon falsafasida, ayniqsa, Forobiy, Ibn Sino va Yusuf Xos Hojib asarlarida jamoaviy ongga ta‘sir qilish, yolg‘on axborot tarqatish, mazmunni burib ko‘rsatish kabi holatlar axloqiy muammo sifatida yoritilgan. O‘rta asrlarda ham jamoatchilikka bosim o‘tkazish, kamsitish va “ma‘lumot urushi” (“informationsnaya voyna”) holatlari maktublar, risolalar, minbar va jamoaviy so‘zlar orqali amalga oshirilgan.

Ommaviy axborot vositalari va zo‘ravonlik evolyusiyasi XIX–XX asrlarda gazeta, radio, televidenie, kino va ommaviy axborot vositalari paydo bo‘lishi bilan axborot orqali psixologik va ma‘naviy zo‘ravonlik yangi qirraga ega bo‘ldi. Jamiyatda yolg‘on axborot tarqatish, jamoaviy kamsitish va manipulyatsiya holatlari ommaviy axborot vositalari yordamida katta tezlik va ko‘limga ega bo‘ldi. Ayniqsa, XX asrning o‘rtalarida “psixologik urushi”, “mafkuraviy tahdidlar” va “axborot urushi” atamaları ilmiy muomalaga kirdi.

Kiberzo‘ravonlikning zamonaviy ko‘rinishlari va global tendensiyalari Internet va raqamli muhitda kiberzo‘ravonlikning kengayishi 1990-yillardan boshlab internet, elektron pochta, ijtimoiy tarmoqlar va mobil ilovalar ommalashgan sari, zo‘ravonlikning yangi - virtual (kiber) shakllari jahon jamiyatida to‘liq taraqqiy etdi. S. Hinduja va J.W. Patchin tadqiqotlarida ta‘kidlanishicha, 2000-yillarda Yevropa va Amerikada maktab yoshli bolalarning 30-40 foizi kamida bir marta kiberbulling qurboni bo‘lgan, yoki onlayn zo‘ravonlikka guvoh bo‘lganligini ta‘kidlaydilar.

Global muammo: yoshlar, ayollar va ijtimoiy guruhlarda kiberzo‘ravonlik - bu nafaqat yoshlar, balki katta yoshlilar, ayollar, yetakchi jamoat faollari, ma‘rifiy xodimlar, hatto siyosatchilar o‘rtasida ham keng tarqalgan global ijtimoiy muammodir. UNICEF va UNESCOning 2022 yilgi hisobotlariga ko‘ra, jahon bo‘yicha internet foydalanuvchilarining 37 foizi turli shakldagi kiberzo‘ravonlik, tahdid, kamsitish, psixologik bosim yoki shantajga duch kelgani aniqlangan. Ayniqsa, o‘smirlar, maktab va kollej o‘quvchilari, onlayn o‘quvchilar, ayollar va ozchilik guruhlar kiber makondagi zo‘ravonlikning asosiy qurbonlaridir.

Kiberzo‘ravonlikning tiplari va formalari jahon amaliyotida kiberzo‘ravonlikning turli shakllari - internetda haqorat va tahdid, shantaj, manipulyatsiya, yolg‘on axborot tarqatish, intim ma‘lumotlar tarqatish, shaxsiy shaxsiyatni yo‘qotish, onlayn bulling, kiberstalking, “gruppa lynch” (“group lynch”), dezinformatsiya va axborot urushi - keng tarqalgan. Amerika, Yevropa, Yaponiya va Rossiyada maktab va universitetlarda maxsus monitoring guruhleri, onlayn xavfsizlik platformalari va psixologik qo‘llab-quvvatlash markazlari tashkil etilgan.

Global tendensiyalar va milliy tajriba dunyoning ko‘plab mamlakatlarida kiberzo‘ravonlikka qarshi huquqiy va profilaktik tizimlar yaratilmoqda:

- AQSh va Yevropa Ittifoqida “kiberbullingga qarshi qonunlar”, onlayn-himoya platformalari, bolalar va yoshlar uchun maxsus “kiberpolitsiya” guruhleri tashkil etilgan;

- Yaponiyada maktab o‘quvchilari uchun virtual profilaktika dasturlari va onlayn psixokonsultatsiyalar tizimi joriy etilgan;

- Rossiya, Qozog‘iston, Koreya, O‘zbekistonda axborot madaniyati va kiberxavfsizlik fanlari, “Kiberxavfsiz oila”, “Axborot madaniyati” kabi milliy loyihalar amalga oshirilmoqda.

Kiberzo‘ravonlikning evolyusiyasi: yangi maydonlar va yangi tahdidlar Virtual madaniyat va jamoaviy psixologiya ta‘siri Kiberzo‘ravonlikning tarqalishi axborot makonidagi “virtual madaniyat” va jamoaviy psixologiyaning o‘zgarishi bilan ham uzviy bog‘liq. Anonimlik va ijtimoiy tarmoqlarda shaxsiy mas‘uliyatning zaifligi, guruh effekti, “onlayn lynch” (“online lynch mob”) holatlari natijasida zo‘ravonlik ko‘pincha jamoaviy, ommaviy xususiyat kasb etadi. Masalan, 2017 yilda Koreya Respublikasida bo‘lib o‘tgan “onlayn kiberhujumlar” natijasida bir necha tanlangan shaxslar jamoaviy bulling qurboni bo‘lib, sud va jamoatchilik muhokamasiga sabab bo‘ldi.

Texnologik inqilob va yangi tahdidlar zamonaviy kiberzo‘ravonlik faqat ijtimoiy tarmoq va chatlar bilan cheklanib qolmaydi. Bugungi kunda “deepfake” texnologiyalari, botlar orqali shantaj, virtual shaxsiyatni qalbakilashtirish, virtual reallik (VR) va sun‘iy intellekt asosidagi manipulyatsiya holatlari paydo bo‘ldi. 2021–2022 yillarda Yevropa Ittifoqi va AQShda deepfake orqali shantaj va qasos voqealariga oid sud ishlari keskin ko‘paydi. Masalan, Germaniyada 2022 yilda deepfake vositasida qilingan 27 ta qonunbuzarlik holati rasmiy qayd etilgan.

Global infodemiya va pandemiya sharoitida kiberzo‘ravonlik COVID-19 pandemiyasi davrida dunyodagi internet foydalanuvchilari soni va ular o‘rtasidagi onlayn muloqotning ortishi natijasida kiberzo‘ravonlik holatlari ham keskin oshdi. 2020–2021 yillarda AQSh, Buyuk Britaniya, Fransiya va Yaponiya maktablarida o‘tkazilgan so‘rovlar natijalariga ko‘ra, maktab o‘quvchilari va talabalarning kamida 48%i onlayn zo‘ravonlikning bir necha shakliga duch kelganini ma‘lum

qilishgan. Infodemia, ya'ni yolg'on axborot oqimi, konspirologiya, yolg'on yoyilishining kuchayishi kiberzo'ravonlikning ommaviylashuviga yanada katta turtki berdi.

Kiberzo'ravonlikning iqtisodiy va siyosiy oqibatlari. Zamonaviy dunyoda kiberzo'ravonlik va axborot urushi nafaqat shaxsiy, balki siyosiy, iqtisodiy va davlat miqyosida ham jiddiy salbiy oqibatlarga olib kelmoqda. Masalan, 2022 yili Fransiyada prezident saylovlari oldidan keng miqyosli kiberhujumlar, yolg'on axborot tarqatish va jamoaviy shantaj orqali siyosiy raqiblarni obro'sizlantirish, jamoatchilik ongiga ta'sir qilish holatlari qayd etildi. O'zbekistonda ham 2023 yilda ayrim bloger va jamoat arboblari qarshi virtual shantaj, "kiberkampaniyalar" orqali bosim o'tkazish holatlari rasmiy OAVda muhokama qilindi.

Profilaktika va jamoaviy choralar global va milliy amaliyotda kiberzo'ravonlikning oldini olish uchun bir necha muhim yo'nalishlar shakllanmoqda:

- ta'lim muassasalarida axborot madaniyati, kiberxavfsizlik va internet-etika bo'yicha maxsus dasturlar;

- davlat va jamoat tashkilotlari tomonidan profilaktika, monitoring va qo'llab-quvvatlash markazlari;

- ota-ona va o'qituvchilar uchun interaktiv ma'rifiy loyihalar;

- qonunchilikni takomillashtirish va onlayn huquqiy himoya mexanizmlari;

- psixologik xizmatlar va onlayn maslahat markazlari.

Yaponiyada maktablar uchun "onlayn xavfsizlik" va "kiberbullingga qarshi qo'llanma", AQSh va Yevropa Ittifoqida "kiberpolitsiya" va "kiberetikal" treninglar, O'zbekistonda esa "Kiberxavfsiz oila", "Yoshlar va axborot madaniyati" dasturlari amaliyotga joriy etilgan. O'zbekistonda 2020-2024 yillarda "Kiberxavfsizlik to'g'risida"gi Qonun, Axborot xavfsizligi konsepsiyasi, maktab va OTM larda axborot madaniyati va kiberxavfsizlik bo'yicha maxsus darslar, profilaktika treninglari, "Kiberxavfsiz oila" loyihasi, davlat va nodavlat tashkilotlar hamkorligida onlayn profilaktika markazlari tashkil etildi. Axborot texnologiyalari va kiberxavfsizlik bo'yicha maxsus magistratura dasturlari yo'lga qo'yildi.

Tarixiy tahlil va zamonaviy tendensiyalar shuni ko'rsatadiki, kiberzo'ravonlik - bu insoniyat ma'naviy taraqqiyoti va axborot makonidagi barqarorlik uchun jahon miqyosidagi eng dolzarb muammolardan biriga aylangan. Kiber makondagi tahdidlar va zo'ravonlik shakllari nafaqat texnik, balki falsafiy, ijtimoiy, psixologik va madaniy yechimlarni, jamiyatda axborot madaniyati, ma'naviy immunitet va fuqarolik mas'uliyatini kuchaytirishni talab etadi. Kiberzo'ravonlikning tarixiy ildizlari va global tendensiyalari tahlili shuni ko'rsatadiki, axborot makonidagi zo'ravonlik - bu faqat yangi texnologik reallik emas, balki inson sivilizatsiyasi va jamiyat ma'naviy-madaniy taraqqiyotining uzluksiz davomi hisoblanadi. An'anaviy axborot urushi va psixologik bosimlar raqamli muhitda yangi shakl va tezlikda namoyon bo'lib, shaxs, jamoatchilik va butun davlat xavfsizligiga jiddiy tahdid solmoqda. Internet, ijtimoiy tarmoqlar, mobil platformalar va zamonaviy media muhit kiberzo'ravonlikni global masalaga aylantirib, jamiyatda axborot madaniyati va ma'naviy immunitetning ustuvorligini talab qiladi. Zamonaviy kiberzo'ravonlik nafaqat psixologik, balki iqtisodiy, siyosiy, madaniy va falsafiy oqibatlarga ega. Shu tariqa, kiberzo'ravonlikka qarshi kurashish uchun nafaqat texnik, balki jamiyatning ma'naviy-axloqiy barqarorligini ta'minlash, jamoaviy mas'uliyatni oshirish, davlat, ta'lim, oila va jamoatchilik institutining uyg'un sa'y-harakatlari zarur. Jahon tendensiyalari va O'zbekiston amaliyoti bu sohada tizimli, falsafiy va profilaktik yondashuvlarning ustuvor ahamiyatini tasdiqlaydi.

Zamonaviy axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida jamiyat hayotining barcha jabhalari raqamli muhitga ko'chmoqda. Bunday sharoitda ma'naviy immunitet va axborot madaniyati nafaqat shaxsiy, balki jamoaviy va davlat miqyosida barqarorlikni ta'minlovchi, milliy va umuminsoniy qadriyatlarni saqlovchi eng muhim omillardan biriga aylandi. Axborot makonida faol yoshlar va jamoatchilik har kuni minglab axborot oqimi, manipulyatsiya, feyk va mafkuraviy tahdidlarga duch kelmoqda. Bu esa ma'naviy immunitet va axborot madaniyati masalasini mamlakat ijtimoiy siyosati va milliy xavfsizligi darajasiga ko'tarmoqda. Ma'naviy immunitet — shaxs va jamoa axloqiy, madaniy, g'oyaviy qadriyatlarga sadoqati, dezinformatsiya

va yot mafkuraga qarshi bardosh, tanqidiy fikr, ijtimoiy mas'uliyat va fuqarolik pozitsiyasida namoyon bo'ladi. Dilbar Ismoilova ta'kidlaganidek, ma'naviy immunitet zaif jamiyatlarda feyk axborotga ishonish, mafkuraviy va ruhiy bo'shliq, axloqiy passivlik va ijtimoiy izolyatsiya muammolari kuchayadi. Saida Qurbonov fikricha, ma'naviy immunitetni shakllantirishda milliy g'oya, ta'lim, oila va jamoat tashkilotlarining hamkorligi hal qiluvchi ahamiyatga ega. Axborot madaniyati — bu axborotni saralash, tahlil qilish, manbalarni farqlash, raqamli xavfsizlik, axborot etikasi va kiber madaniyat ko'nikmalarining uyg'un tizimidir. Yusupov S.Sh. va Egamberdiev M. izlanishlarida ta'kidlanishicha, axborot madaniyati yetuk jamiyatlarda feyk yangiliklarga, manipulyatsiyaga, mafkuraviy tahdidlarga qarshi “axborot immuniteti” shakllanadi; tanqidiy fikrlash va ijtimoiy faollik oshadi; yoshlarda milliy qadriyatlarga, axloqiy prinsiplarga va umuminsoniy ideallarga sadoqat mustahkamlanadi. Ma'naviy immunitet va axborot madaniyatining o'zaro bog'liqligi o'ziga xos integratsiyaviy tizimni yaratadi. Bu ikki omil uyg'un rivojlanganda, axborot makonidagi mafkuraviy, axloqiy, ruhiy va ijtimoiy tahdidlarga samarali bardosh berish mumkin. Jumladan, axborot madaniyati tanqidiy fikrlash, axloqiy yetuklik, raqamli xavfsizlik va shaxsiy mas'uliyatni rivojlantirsa, ma'naviy immunitet esa milliy g'oya, axloqiy pozitsiya va jamoaviy hamjihatlikni ta'minlaydi. Bunday sinergetik ta'sir jamiyatda axborot urushi va dezinformatsiya, kiber tahdid va yot mafkuraviy ta'sirlarga qarshi mustahkam qalqon yaratadi. Milliy va xalqaro amaliyotda ham mazkur masalalarga katta e'tibor qaratilmoqda. O'zbekistonda “Ma'naviyat va ma'rifat markazi”, “Axborot madaniyati” va “Kiberxavfsizlik” fanlarining joriy qilinishi, yoshlar va ota-onalar uchun trening va chellenjlar tashkil etilishi bu sohada katta natijalar bermoqda. Kelgusida kiber makonda shaxs va jamoa munosabatlarini yanada sog'lomlashtirish uchun axborot madaniyati va ma'naviy immunitetni rivojlantirish, milliy va umuminsoniy qadriyatlarga asoslangan innovatsion pedagogika va jamoaviy hamkorlikni kuchaytirish talab etiladi.

Xulosa. Zamonaviy jamiyatda internet va raqamli texnologiyalar inson hayotining ajralmas qismiga aylandi. Bu jarayon axborot olish, fikr bildirish, ijtimoiy hamkorlik va shaxsiy erkinliklar uchun beqiyos imkoniyatlar yaratar ekan, bir vaqtning o'zida inson huquqlari va erkinliklariga oid yangi muammolar va tahdidlarni ham keltirib chiqarmoqda.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

- [1] Hinduja, S., & Patchin, J. W. (2014). Cyberbullying: Identification, Prevention, and Response. Cyberbullying Research Center.
<https://cyberbullying.org>
- [2] Livingstone, S., & Smith, P. K. (2014). Annual Research Review: Harms experienced by child users of online and mobile technologies: the nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of Child Psychology and Psychiatry*, 55(6), 635–654.
- [3] UNICEF. (2022). Cyberbullying: What is it and how to stop it.
<https://www.unicef.org/end-violence/how-to-stop-cyberbullying>
- [4] UNESCO. (2022). Global Education Monitoring Report: Technology in education – A tool on whose terms?
<https://en.unesco.org/gem-report/report/2023/technology>
- [5] O'zbekiston Respublikasi “Kiberxavfsizlik to'g'risida”gi Qonuni (2020).
- [6] Patchin, J. W., & Hinduja, S. (2020). Cyberbullying in the digital age: Prevention and intervention strategies. Routledge.
- [7] Park, S., Na, E. Y., & Kim, E. M. (2020). The digital literacy of children and young people: A meta-analysis. *Computers & Education*, 105, 835–850.
- [8] Ахмедов, Р. (2023). Киберзўравонлик ва ёшлар маънавияти: Ўзбекистон тажрибаси. *Axborot Madaniyati jurnali*, 2(1), 56–65.
- [9] O'zbekiston Respublikasi Vazirlar Mahkamasi (2022). Axborot xavfsizligi konsepsiyasi to'g'risida.

“INNOVATION TECHNOSYSTEMS” ilmiy texnik jurnali.
MV AKT va AHI, 2025-y. – 290 b.



Eslatma: Maqolalar mazmuniga javobgarlik mualliflar zimmasiga yuklatiladi.

© Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti, 2025-yil.

Terishga berildi: 23.16.2025.
Bosishga ruxsat etildi: 27.06.2025.
Qog‘ozga bichimi: 60/84 1/8.
Shartli bosma tabog‘i – 20.
Adadi – 4 nusxa.