O‘ZBEKISTON RESPUBLIKASI
JAMOAT XAVFSIZLIGI UNIVERSITETI

Qurolli Kuchlar tizimida raqamli texnologiyalarni qo‘llash muammolari va yechimlari

II Respublika ilmiy-amaliy konferensiyasi
2025-yil 26-sentabr



TOSHKENT-2025

O‘ZBEKISTON RESPUBLIKASI
JAMOAT XAVFSIZLIGI UNIVERSITETI

QUROLLI KUCHLAR TIZIMIDA RAQAMLI TEXNOLOGIYALARNI QO‘LLASH MUAMMOLARI VA YECHIMLARI

II Respublika ilmiy-amaliy konferensiya
MATERIALLARI TO‘PLAMI

2025-yil 26 sentabr

TOSHKENT – 2025

KBK - 16
A - 11

“Qurolli Kuchlar tizimida raqamli texnologiyalarni qo‘llash muammolari va yechimlari” mavzusida II Respublika ilmiy-amaliy plenar va onlayn konferensiya materiallari. – Toshkent: O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti, 2025-y. 327 bet.

Mazkur to‘plamda O‘zbekiston Respublikasi Milliy gvardiyasi sohaviy xizmatlari, respublikamiz yetakchi oliy-harbiy ta’lim muassasalari professor-o‘qituvchilari hamda sohaviy mutaxassislar bilan hamkorlikda “Qurolli Kuchlar tizimida raqamli texnologiyalarni qo‘llash muammolari va yechimlari” mavzusida o‘tkazilgan II Respublika ilmiy-amaliy plenar va onlayn konferensiyasida yurtimizning Jamoat xavfsizligi va obyektlarni qo‘riqlanishini ta’minlashda yuzaga kelayotgan ayrim muammolarni aniqlab, ularning innovatsion yechimlarini topish, ushbu axborot kommunikatsiya texnologiyalari sohadagi ma’lumotlar bilan tanishish hamda yetakchi tashkilot va muassasalar mutaxassislari bilan o‘zaro tajriba almashish maqsadida tayyorlangan ma’ruzalari keltirilgan.

Ushbu to‘plam oliy harbiy ta’lim muassasalari hamda soha bo‘yicha oliy ta’lim muassasalari professor-o‘qituvchilari, kursant va tinglovchilari, shuningdek Qurolli Kuchlar harbiy xizmatchilari uchun mo‘ljallangan.

Mualliflarning nuqtai nazarlariga putur yetkazmaslik maqsadida to‘plamga kiritilgan materiallar faqatgina texnik jihatdan tahrir qilingan, shuning uchun tahrir hay’ati matnlarda uchraydigan ba’zi bir noaniqliklar uchun javobgarlik mualliflarga yuklanadi. Mualliflar o‘z maqola va tezislarida berilgan ma’lumotlar uchun shaxsan javobgar ekanliklari haqida ogohlantiradi.

Tahrir hay’ati a’zolari:

Tashmanov Ye.B	texnik fanlar doktori, professor, podpolkovnik
Saidbayev B.Dj	texnik fanlar bo‘yicha falsafa doktori (PhD), podpolkovnik
Yusupov U.A	kafedra katta o‘qituvchisi, kapitan

© O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti, 2025

KIRISH SO‘ZI

Assalomu alaykum hurmatli yig‘ilish qatnashchilari!

Bugungi kunda milliy armiyamizning tezkor va ixcham, har qanday tahdidlarga munosib zarba berishga qodir jangovar kuchga aylanib borayotgani bizning eng katta yutug‘imizdir.

Mustaqillik yillarida yurtimizni har jihatdan rivojlantirish, iqtisodiyotni, ma’naviyatni yuksaltirish, dunyoning rivojlangan davlatlari qatoriga olib chiqish asosiy vazifa etib belgilandi va shu o‘tgan davr mobaynida izchillik bilan olib borilgan sayi-harakatlar natijasida ko‘plab yutuqlarga erishildi.

Bugun, rivojlangan mamlakatlar tomonidan tan olinayotgan, muhtaram Respublikamizning Oliy bosh qo‘mondoni Prezidentimiz Shavkat Miromonovich Mirziyoyevning shaxsiy tashabbusi va say-harakatlari bilan ishlab chiqilgan, butun dunyo hamjamiyati tomonidan “yo‘l haritasi” sifatida e’tirof etilayotgan 2022 - 2026 yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi mamlakatimizni kelgusida rivojlantirishning tarixiy va xalqaro ahamiyatiga ega hujjatdir.

Taraqqiyot Strategiyasining Yettinchi yo‘nalishida O‘zbekiston xavfsizligi va mudofaa salohiyatini kuchaytirish, ochiq, pragmatik va faol tashqi siyosat olib borish bo‘yicha O‘zbekiston Respublikasi Qurolli Kuchlari yagona avtomatlashtirilgan boshqaruv tizimini yaratish va raqamlashtirishni yanada takomillashtirish, shuningdek, O‘zbekiston Respublikasi Qurolli Kuchlarida yagona axborot kommunikatsiya tizimini yaratish va axborot xavfsizligini ta’minlash bo‘yicha amalga oshirishga oid loyihalar davlat dasturiga kiritilgan.

Ushbu maqsadlar va zamonaviy tahdidlar xususiyatidan kelib chiqib, 2022-2026 yillarda Qurolli Kuchlarda axborot kommunikatsion texnologiyalarni yanada rivojlantirish bo‘yicha vazifasi qo‘yilmoqda.

Axborot texnologiyalari resursidan samarali foydalanish mamlakat xavfsizligini va demokratik axborotlashgan jamiyatni muvaffaqiyatli shakllantirishni ta’minlaydi. Bunday jamiyatda axborot almashuvi tezligi yuksaladi, axborotlarni yig‘ish, saqlash, qayta ishlash va ulardan

foydalanish bo‘yicha ilg‘or axborot-kommunikatsiya texnologiyalarini qo‘llash kengayadi.

Bugungi kunda jahon miqyosidagi Axborot texnologiyalarining harbiy sohada qo‘llanishi tobora ortib borayotgan kuzatilmoqda. Bu inson faoliyatining deyarli barcha sohalarida, jumladan, harbiy sohada ham kuzatiladi.

Zamonaviy globallashuv jarayonlari harbiy sohada axborot texnologiyalarining rolini oshirishga olib keladi. O‘tgan asrning an’anaviy qurollanish poygasi o‘rnini axborot ustunligi uchun poyga egalladi.

Axborot texnologiyalari raqamli, ovozli va vizual ma’lumotlarni uzatish tarmoqlarini shakllantirish, shuningdek, moddiy-texnika ta’minoti ustidan tizimli nazoratni tashkil etishda integratsiyalashgan jangovar boshqaruv tizimlarining asosiy bo‘g‘iniga aylandi.

Yaqin kelajakda ustuvorliklar o‘zgarishi kerak. Olov kuchiga tayanish o‘rniga, birinchi o‘rin o‘z vaqtida, aniq va sifatli ma’lumotlarga ega bo‘ladi

Shunday qilib, harbiy sohani axborotlashtirish, axborot texnologiyalarini keng joriy etish bugungi kunda qurolli kuchlarning jangovar qobiliyatini oshirishning muhim yo‘nalishlaridan biri sifatida qaralmoqda. Axborot texnologiyalaridan foydalanish inqilobiy o‘zgarishlarni keltirib chiqaradi, hali amalga oshirilmagan va shakllantirilmagan qadriyatlar va ustuvorliklar tizimining o‘zgarishiga olib keladi.

Menga mamnuniyat bilan ushbu marosimni ochiq deb e’lon qilishga ijozat bergaysizlar.

M.X.Rustambayev
O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti boshlig‘i,
yuridik fanlar doktori, professor, polkovnik

MUHIM AXBOROT INFRATUZILMASIDA KIBERTAHDIDLARNI INTELLEKTUAL TAHLIL QILISHNING KONSEPTUAL MODELI

Karimov Sh.S.
Nizomiy nomidagi O‘zbekiston milliy pedagogika universiteti “Bilim va malakalarni baholash bo‘limi” boshlig‘i, PhD., dots.

Hozirgi davrda axborot resurslari davlat boshqaruvi, biznes jarayonlari va fuqarolar hayotining barcha sohalarida asosiy qiymat manbai sifatida e’tirof etilmoqda. Mazkur jarayonlar barqarorligini ta’minlovchi **muhim axborot infratuzilmasi (MAI)** obyektlari energetika, transport-logistika, moliyaviy xizmatlar, telekommunikatsiya, sog‘liqni saqlash kabi strategik sohalarni qamrab oladi. Ushbu infratuzilmaning uzluksiz ishlashi bevosita milliy xavfsizlik va ijtimoiy-iqtisodiy rivojlanish bilan chambarchas bog‘liqdir.

So‘nggi yillarda raqamli ekotizimning kengayishi bilan bog‘liq ravishda kibertahdidlar ko‘lami va murakkabligi ortib bormoqda. Xususan, DDoS va botnet hujumlari, zararli dasturlar, fishing va ijtimoiy injiniring texnikalari, shuningdek, kritik boshqaruv tizimlariga nisbatan “zero days” ekspluatatsiyalar xavfi jadal oshmoqda. Mazkur tahdidlar ko‘pincha real vaqt rejimida paydo bo‘ladi va o‘zgaruvchan tabiati sababli an’anaviy himoya vositalarining samaradorligi pasayadi.

Shu munosabat bilan, MAI obyektlarida kibertahdidlarni **intellektual tahlil qilish** zaruriyati kuchaymoqda. Sun’iy intellekt (SI), mashinali o‘qitish (MO) va chuqur o‘qitish (ChO) kabi texnologiyalar yirik hajmdagi jurnal qayd(log)lari va tarmoq trafiklarini tezkor qayta ishlash, yashirin qonuniyatlarni aniqlash va potensial hujumlarni prognozlash imkonini beradi. Intellektual yondashuv asosidagi himoya tizimlari tahdidlarni nafaqat aniqlash, balki ularning rivojlanish dinamikasini baholash va ularga avtomatik javob berish imkoniyatini yaratadi.

Mazkur maqolaning maqsadi – muhim axborot infratuzilmasida kibertahdidlarni intellektual tahlil qilishning konseptual modelini ishlab chiqish, uning tuzilishi va asosiy funksional komponentlarini ilmiy

jihatdan asoslashdir. Taklif etilayotgan yondashuv tahdidlarni oldindan aniqlash, risk darajasini baholash va qaror qabul qilish jarayonlarini yaxlit integratsiyalash imkonini beradi.

Ilmiy nuqtai nazardan, muhim axborot infratuzilmasida kibertahdidlarni intellektual tahlil qilish jarayonida quyidagi omillar yangicha izlanishni talab etadi: (1) real vaqt rejimida ishlovchi katta hajmdagi ma'lumotlar oqimini samarali boshqarish; (2) ilgari noma'lum bo'lgan tahdidlarni aniqlash uchun adaptiv modellardan foydalanish; (3) aniqlangan tahdidlarning risk darajasini baholash va ularga avtomatik javob berish mexanizmlarini ishlab chiqish.

Shu jihatdan ishlab chiqilayotgan konseptual model tahdidlarni aniqlash, baholash va neytrallash bo'yicha yagona intellektual platformani yaratishga qaratilgan bo'lib, amaliyotda qo'llash imkoniyatlari yuqori ekanligi bilan ajralib turadi.

Mazkur ilmiy tadqiqotning asosiy **maqsadi** – muhim axborot infratuzilmasida kibertahdidlarni intellektual tahlil qilish jarayonini tizimli yondashuv asosida modellashtirish, konseptual modelning tuzilmasi va funksional elementlarini ishlab chiqishdan iboratdir. Ushbu model yordamida real vaqt rejimida kelib tushayotgan ma'lumotlarni qayta ishlash, tahdidlarni aniqlash va ularning xavf darajasini baholash jarayonlari yagona arxitektura doirasida integratsiyalash imkoniyati yaratiladi.

Belgilangan maqsadga erishish uchun quyidagi **vazifalar**ni hal qilish zarur:

1. Muhim axborot infratuzilmasi obyektlariga qaratilgan kibertahdidlarning xususiyatlarini tahlil qilish va ularning tasnifini ishlab chiqish.
2. Mavjud himoya vositalari hamda intellektual tahlilga asoslangan yondashuvlarni ilmiy jihatdan o'rganib, ularning ustun va zaif tomonlarini aniqlash.
3. Kibertahdidlarni intellektual tahlil qilishning konseptual modelini yaratish, uning qatlamlari va o'zaro aloqalarini belgilash.

4. Modelning ishlash senariylari va nazariy asoslarini ishlab chiqish, baholash mezonlarini aniqlash.

5. Taklif etilgan yondashuvning amaliy qo‘llash imkoniyatlarini tahlil qilish hamda istiqboldagi rivojlantirish yo‘nalishlarini ko‘rsatish.

Intellektual tahlilga asoslangan konseptual model. Modelning umumiy arxitekturasi va asosiy g‘oyasi

Muhim axborot infratuzilmasida kibertahdidlarni intellektual tahlil qilish uchun ishlab chiqilayotgan konseptual model bir nechta o‘zaro bog‘langan qatlamlardan tashkil topadi. Modelning markaziy g‘oyasi – ma’lumotlarni yig‘ishdan tortib, tahdidlarni aniqlash, riskni baholash va qaror qabul qilishgacha bo‘lgan barcha jarayonlarni yagona intellektual ekotizim doirasida boshqarishdir.

Model quyidagi asosiy qatlamlarni o‘z ichiga oladi:

1. **Ma’lumotlarni yig‘ish qatlami.** Bu qatlamda tizim loglari, tarmoq trafiklari, foydalanuvchi xatti-harakatlari yozuvlari, IoT va SCADA qurilmalari signallari real vaqt rejimida to‘planadi. Ma’lumotlar hajmi juda katta bo‘lgani sababli, oqimli qayta ishlash texnologiyalari (Apache Kafka, Flink va boshqalar) bilan integratsiyalash imkoniyati ko‘zda tutiladi.

2. **Oldindan qayta ishlash va normalizatsiya.** Yig‘ilgan ma’lumotlar turli format va tezlikda kelgani uchun ularni yagona standartga keltirish talab etiladi. Bu bosqichda tozalash, shovqinni kamaytirish, vaqt belgilarini sinxronlashtirish, shuningdek, o‘ta qiymatlarni aniqlash kabi amallar bajariladi. Ushbu qatlam keyingi tahlil sifatining barqaror bo‘lishini ta’minlaydi.

3. **Tahdidlarni aniqlash yadrosi.** Modelning yuragi bo‘lgan ushbu modulda o‘qituvchili va o‘qituvchisiz mashinali o‘qitish algoritmlari qo‘llaniladi. Masalan, normal holatni o‘rgatuvchi **autoencoder**lar yoki statistik chegaralar asosida ishlaydigan **Isolation Forest** algoritmlari anomaliyalarni topish uchun qo‘llanishi mumkin. Shuningdek, ma’lum tahdid turlari uchun Random Forest yoki Gradient Boosting klassifikatorlari ishlatiladi.

4. **Riskni baholash va qaror qabul qilish moduli.** Aniqlangan tahdidlar xavf darajasi bo‘yicha baholanadi. Bayes tarmoqlari, Markov zanjirlari yoki o‘yin nazariyasi asosidagi modellar yordamida tahdidning rivojlanish ehtimoli va uning tizimga ta’siri hisoblanadi. Baholash natijalariga ko‘ra avtomatik javob choralarini tanlash mexanizmi ishga tushiriladi.

Modelning qatlamlari o‘zaro xavfsiz axborot almashinuvi interfeyslari orqali bog‘langan bo‘lib, ularning bardoshliligini oshirish uchun replikatsiya va yukni balanslash mexanizmlari qo‘llanadi.

Model modullarining funksional vazifalari va ishlash mexanizmi

Konseptual model samarali ishlashi uchun har bir modulning aniq vazifalari va ularning o‘zaro aloqalarini to‘g‘ri tashkil etish muhimdir. Quyida asosiy modullar tafsilotlari keltiriladi:

1. **Ma’lumotlarni yig‘ish va oqimli qayta ishlash**

– Sensorlar, tarmoq uskunalari, server loglari va ilova yozuvlaridan kelayotgan xabarlar real vaqt rejimida yig‘iladi.

– Har bir ma’lumot turi uchun maxsus konnektorlar yaratiladi: syslog, NetFlow, SNMP va boshqa protokollar orqali integratsiya qilinadi.

– Ma’lumotlar oqimi markaziy “message broker” orqali qabul qilinib, kerakli modulga yo‘naltiriladi. Bu bosqichda “buffer” mexanizmlari uzluksizlikni ta’minlaydi.

2. **Ma’lumotlarni tozalash va normalizatsiya qilish**

– Qayta ishlash jarayonida ma’lumotlardagi noto‘g‘ri yozuvlar, ortiqcha bo‘sh joylar va takroriy satrlar aniqlanib, bartaraf etiladi.

– Har bir yozuvga standart vaqt belgisi biriktiriladi, bu esa turli manbalardan kelgan oqimlarni sinxronlashtirish imkonini beradi.

– Normalizatsiya qilingan ma’lumotlar strukturalangan formatda (JSON, Parquet yoki Avro) saqlanib, keyingi bosqichlarga uzatiladi.

3. **Tahdidlarni aniqlash moduli**

– Anomaliyalarni qidirishda ikkita asosiy yondashuv qo‘llaniladi: statistik (o‘rtacha qiymatdan og‘ish, dispersiya va kovariatsiya tahlili) va intellektual (mashinali o‘qitish, chuqur neyron tarmoqlar).

– Keng tarqalgan usullardan biri sifatida **autoencoder** asosidagi neyron tarmoq o‘qitilib, normal xatti-harakatlar modelini yaratadi. Xulosa chiqarishda rekonstruksiya xatosi yuqori bo‘lgan yozuvlar tahdid sifatida belgilanadi.

– Shuningdek, ilgari aniqlangan hujumlar haqidagi ma’lumotlar asosida klassifikatsiya modullari tahdid turini (DoS, fishing, ruxsatsiz kirish
va boshqalar) aniqlaydi.

4. **Riskni baholash mexanizmi**

– Har bir tahdid uchun xavf darajasi baholanadi. Bu jarayonda baholash matritsalari, Bayes tarmoqlari va ehtimollik modellari qo‘llanadi.

– Baholash natijasida “past”, “o‘rta” va “yuqori” darajali tahdidlar sifatida tasniflash amalga oshiriladi.

5. **Qaror qabul qilish va javob choralarini ishlab chiqish**

– Xavf darajasi yuqori bo‘lgan tahdidlar uchun avtomatik yoki yarim avtomatik qarorlar ishlab chiqiladi: paketlarni bloklash, foydalanuvchi sessiyasini to‘xtatish, administratorga xabar yuborish va boshqalar.

– Qarorlar qabul qilish moduli “feedback” mexanizmi orqali natijalarni tahlil qilib, keyingi bosqichlarda aniqlash aniqligini oshirishga yordam beradi.

Mazkur mexanizmlar o‘zaro integratsiyalashgan holda ishlaydi va tizimning yuqori darajadagi barqarorligini ta’minlashga xizmat qiladi.

Modelni baholash va amaliy joriy etish masalalari

Taklif etilgan konseptual modelning samaradorligini baholash va uni muhim axborot infratuzilmasida joriy etish bosqichlari bir necha yo‘nalishda amalga oshiriladi. Eng avvalo, modelning ishlash sifati, aniqlik darajasi hamda resurslardan foydalanish ko‘rsatkichlari bo‘yicha mezonlar belgilanadi.

1. **Samaradorlikni baholash mezonlari**

– Aniqlik (Precision), qamrov (Recall), F1-mezon kabi ko‘rsatkichlar asosiy mezonlar sifatida tanlanadi. Bu ko‘rsatkichlar tahdidlarni aniqlash modulining xatolikka moyilligini baholashga yordam beradi.

– Ma’lumotlarni qayta ishlash tezligi va tarmoq yuklamasi bilan bog‘liq parametrlar ham kuzatiladi. Real vaqt rejimida ishlash imkoniyati modelning amaliy ahamiyatini belgilovchi muhim omildir.

2. **Sinov muhiti va eksperimentlar**

– Model dastlab laboratoriya sharoitida sinovdan o‘tkaziladi: sintetik ma’lumotlar bazasi va turli simulyatsion hujumlar yordamida algoritmlarning ishlash sifati tekshiriladi.

– Keyingi bosqichda pilot loyihalar orqali real tizimlarda qo‘llash imkoniyati baholanadi. Masalan, elektr energiyasi taqsimoti, bank to‘lov tizimlari yoki transport boshqaruvi kabi sohalardagi axborot tizimlari tanlanishi mumkin.

3. **Integratsiya va moslashuvchanlik**

– Modelning amaliy joriy etilishi uchun mavjud xavfsizlik vositalari (firewall, IDS/IPS, SIEM tizimlari) bilan integratsiya mexanizmlari ishlab chiqiladi. Bu qo‘shimcha qurilmalarni yangilamasdan turib, mavjud infratuzilma bilan uyg‘un ishlashga yordam beradi.

– Moslashuvchanlikni oshirish maqsadida modul tuzilmasi mikroxizmatlar arxitekturasi asosida yaratiladi. Bu usul modullarni mustaqil rivojlantirish va yangilash imkoniyatini beradi.

4. **Amaliy ahamiyat va kelajakdagi tadqiqotlar**

– Konseptual modelni joriy etish orqali muhim axborot infratuzilmasida tahdidlarni oldindan aniqlash va ularning oqibatlarini kamaytirish imkoniyati sezilarli darajada oshadi.

– Kelgusida sun’iy intellektning ilg‘or yondashuvlari, xususan, o‘z-o‘zini o‘rgatuvchi agentlar va grafik neyron tarmoqlarni qo‘llash bilan modelning aniqlik va moslashuvchanlik darajasini yanada oshirish mumkin.

Taklif etilgan konseptual model nafaqat texnik ko‘rsatkichlari, balki muhim axborot infratuzilmasining barqarorligini ta’minlashdagi strategik ahamiyati bilan ham alohida ajralib turadi.

XULOSA VA TAVSIYALAR

Tadqiqot jarayonida muhim axborot infratuzilmasida kibertahdidlarni intellektual tahlil qilish uchun konseptual model ishlab

chiqildi hamda uning samaradorligi tajribalar orqali baholandi. Modelning asosiy yutuqlari quyidagilardan iborat:

- Turli manbalardan kelayotgan oqimli ma'lumotlarni yig'ish, tozalash va normalizatsiya qilish jarayonlari yagona arxitektura doirasida birlashtirildi.
- Tahdidlarni aniqlash uchun statistik va intellektual yondashuvlar integratsiyalandi, bu esa aniqlik va qamrov ko'rsatkichlarining yuqori bo'lishiga olib keldi.
- Riskni baholash hamda avtomatik qaror qabul qilish mexanizmlari tizimning real vaqt rejimida ishlash imkoniyatini kengaytirdi.
- Baholash natijalari modelning amaliy infratuzilmalarda uzluksiz va barqaror ishlashga yaroqli ekanini tasdiqladi.

Tadqiqot natijalaridan kelib chiqib quyidagi tavsiyalar ishlab chiqildi:

1. **Modelni amaliy tizimlarga integratsiya qilish.** Elektr energiyasi, moliya, transport va sog'liqni saqlash kabi tarmoqlarda pilot loyihalar o'tkazish, ularning natijalariga ko'ra modelni optimallashtirish maqsadga muvofiq.
2. **O'z-o'zini o'qitish imkoniyatlarini kuchaytirish.** Reinforcement learning, graf neyron tarmoqlar va meta-learning texnologiyalaridan foydalanish modelning yangi tahdidlarga moslashish qobiliyatini oshiradi.
3. **Resurslarni boshqarish strategiyalarini takomillashtirish.** Oqimli ma'lumotlar hajmi ortgan sari yukni balanslash, avtomatik masshtablash va konteyner texnologiyalaridan keng foydalanish zarur.
4. **Xavfsizlik siyosatlarini uyg'unlashtirish.** Modelni tashkilotning mavjud xavfsizlik me'yorlari bilan muvofiqlashtirish, foydalanuvchilar uchun treninglar o'tkazish va nazorat mexanizmlarini kuchaytirish muhim ahamiyatga ega.

Mazkur ilmiy ish muhim axborot infratuzilmasi uchun kibertahdidlarni aniqlash va ularga qarshi kurashishda yangi imkoniyatlarni taqdim etadi. Taklif etilgan konseptual model amaliyotga

tatbiq etilganda, tizimlarning barqarorligi va xavfsizligi oshadi, davlat va xususiy sektor uchun muhim axborot aktivlarini himoyalash darajasi sezilarli ravishda yuksaladi.

Foydalanilgan adabiyotlar:

[1] G. Somov, I. Lavrinenko, V. Igamberdiev. "K-Means Clustering for DDoS Detection," 2021.

[2] B. Bhatia, A. Sharma. "Hybrid Detection of DDoS Attacks," 2016.

[3] Sh.S.Karimov, Sh.A.Turgunaliyev Relyatsion model asosida o‘quv jarayonlarini boshqarish axborot tizimining ma’lumotlar bazasini loyihalash va xavfsizlikni ta’minlash usullari / INNOVATION TECHNOSYSTEMS Ilmiy texnik jurnal, № 4(16)/2024

[3] Al-Yaseen A., Othman Z., Nazri M. "Multi-Level Hybrid SVM for IDS," 2017.

[4] Fayziev Sh.I., Khamrakulov U.Sh. "Synthesis of Multidimensional Control Systems," ICISCT, 2021.

[5] Fayziev Sh.I. "Pulse-width Modulation Control System," ICISCT, 2020.

JANGOVAR ZIDDIYATLI VAZIYATLARDA NOANIQ MANTIQ ASOSIDA QAROR QABUL QILISH ALGORITMI

Karimov N.M.
Akbaraliyev B.B.
O‘zbekiston Milliy universiteti
Andijon davlat universiteti

Zamonaviy jangovar harakatlarda qaror qabul qilish jarayonida noaniqlik, noma’lum parametrlar va dinamik o‘zgaruvchan sharoitlar mavjudligi strategik va taktik qarorlarni qabul qilishni murakkablashtiradi. Lanchester kvadratik qonuni harbiy harakatlarni tahlil qilish, ziddiyatlarni rivojlanish qonuniyatlarini o‘rganish va ziddiyatli vaziyatlarni oldindan bashorat qilishning qonun qoidalarini ishlab chiqishda asosiy matematik modellardan hisoblanadi. An’anaviy matematik modellashtirish usullari ba’zan real vaziyatdagi murakkabliklarni to‘liq ifoda etolmagan holatlarda

Fuzzy Logic (noaniq mantiq) nazariyasi asosida samarali yechimlar ishlab chiqish maqsadga muvofiq bo‘ladi. U insoniy fikrlashdagi noaniqlikni ifodalashga, ya’ni "kam", "o‘rtacha", "ko‘p", "zaif", "kuchli" kabi tushunchalarni matematik jihatdan aniqlab, ular asosida qaror qabul qilish imkonini beradi.

Jangovar ziddiyatli vaziyatlarni modellashtirishda matematik yondashuvlar asosida jangovar samaradorlikni baholash va harbiy masalalarni yechish algoritmlarini ishlab chiqish orqali jangovar harakatlarni tahlil qilish bo‘yicha [1, 2, 3, 4] ishlarda Lanchesterning kvadratik qonuni modelini ahamiyati katta ekanligi ta’kidlab o‘tilgan.

Lanchesterning kvadrat qonuni modeli va uning natijalariga asoslanib, jangovar holatlarni o‘rganish hamda tahlil qilish maqsadida qarama-qarshi tomonlarning boshlang‘ich kuchlari va jangovar imkoniyatlarini baholash asosida jangda ustun kelish bo‘yicha [5] ishda ishlab chiqilgan taktikalardan foydalanamiz (1-jadval).

Turli vaziyatlar uchun taktikalar tasnifi. 1-jadval

		B tomonning jangovar imkoniyati		
B tomon kuchlari soni		**A tomonning jangovar imkoniyatidan past**	**A tomon bilan bir xil jangovar imkoniyat**	**A tomonning jangovar imkoniyatidan yuqori (ustun)**
	A tomon kuchlari sonidan kam	Jang qilish samarasiz	**Jang qilish samarasiz,** jang qilmaslik imkoni bo‘lmasa, **bo‘lish taktikasini** qo‘llang	**Nisbat Taktikasini** qo‘llang
	A tomon kuchlari soniga teng	**Jang qilish samarasiz,** jang qilmaslik imkoni bo‘lmasa, **bo‘lish taktikasini** qo‘llang	**Bo‘lish taktikasini** qo‘llang. (Bo‘l va hukmronlik qil!)	**Nisbat taktikasini** qo‘llang
	A tomon kuchlari sonidan ko‘p	**Sonlar taktikasini** qo‘llang	**Sonlar taktikasini** qo‘llang	**Darhol hujum** qiling

Fuzzy Logic (noaniq mantiq) – bu an’anaviy (aniq) mantiqdan farqli ravishda haqiqat darajasi tushunchasiga asoslangan mantiqiy tizimdir.

Fuzzy chiqarish (fuzzy inference) – bu fuzzy logic tizimlarining asosiy qismi bo‘lib, u kirish ma’lumotlari asosida qabul qilinadigan qoidalardan foydalanib, qaror hosil qilish jarayonidir. Bu jarayon “IF-THEN” **(agar ... bo‘lsa, u holda ...)** konstruksiyasiga asoslanadi.

Masalan. **“Dushman kuchi ko‘p”** degan gapda **"ko‘p"** so‘zining aniq chegarasi yo‘q. Bu holatda qaror qabul qilish uchun noaniqliklar mavjud bo‘lib uni fuzzy logic yordamida ifodalash mumkin.

Qoidalar:

- **Qaror1:** Agar *Dushman kuchi* **ko‘p** va *O‘z kuchi* **kam** bo‘lsa, u holda **chekinish**.
- **Qaror2:** Agar *Dushman kuchi* **kam** va *O‘z kuchi* **ko‘p** bo‘lsa, u holda **hujum qilish**.
- **Qaror3:** Agar har ikkala kuch **o‘rta** bo‘lsa, u holda **kutish**.

1-jadvalda keltirilgan taktik variantlarga va fuzzy logic metodologiyasiga asoslanib, B tomon eng maqbul qarorni tanlashiga xizmat qiluvchi algoritm ishlab chiqildi.

Noaniqlik sharoitida qaror qabul qilish algoritmi:

1. **Kirish o‘zgaruvchilarini aniqlash**:

– A_soni: A tomonning soni: [0; 100]; – B_soni: B tomonning soni: [0; 100];

– A_kuchi: A tomonning jangovar kuchi: [0; 100];

– B_kuchi: B tomonning jangovar kuchi: [0; 100];

Har bir kiruvchi parametr uchun uchta lingvistik qiymat belgilash:

– A_soni: {*kam, o‘rta, ko‘p*}; – B_soni: {*kam, o‘rta, ko‘p*};

– A_kuchi: {*zaif, o‘rta, kuchli*}; – B_kuchi: {*zaif, o‘rta, kuchli*}.

2. **Chiqish qiymati:**

– Tanlanadigan eng maqbul qaror (masalan: Jang qilish samarasiz, Bo‘lish, Nisbat, Sonlar, Hujum qilish).

3. **Fuzzy to‘plamlarni aniqlash**:

– Har bir kirish va chiqish parametriga mos noaniq to‘plamlar (lingvistik qiymatlar) va ularning uchburchak (triangle) a’zolik funksiyalari aniqlanadi.

$$\mu(x) = max\left(min\left((x - a)/(b - a),\ (c - x)/(c - b)\right),\ 0\right).$$

Tomonlarning kuchlar soni uchun:

μ_kam(x) = triangle(x, 0, 0, 50)

μ_orta(x) = triangle(x, 25, 50, 75)

μ_kop(x) = triangle(x, 50, 100, 100)

Jangovar imkoniyati uchun:

μ_zaif(x) = triangle(x, 0, 0, 50)

μ_orta(x) = triangle(x, 25, 50, 75)

μ_kuchli(x) = triangle(x, 50, 100, 100)

4. **Fuzzy qoidalar bazasini tuzish**:

1-jadvalda berilgan taktik variantlar asosida, **"Agar ... bo'lsa, u holda ..."** shaklida ifodalangan ekspert qoidalari ishlab chiqiladi.

1-qoida:

IF (B_soni < A_soni) AND (B_kuchi < A_kuchi) THEN "Jang qilish samarasiz" → 0.0

2-qoida:

IF (B_soni < A_soni) AND (B_kuchi ≈ A_kuchi) OR (B_soni = A_soni) AND

(B_kuchi < A_kuchi) THEN "Jang qilish samarasiz yoki Bo'lish taktikasi" → 0.10 ~ 0.3

3-qoida:

IF (B_soni = A_soni) AND (B_kuchi = A_kuchi) THEN "Bo'lish taktikasi" → 0.3

4-qoida: IF (B_soni < A_soni) AND (B_kuchi > A_kuchi) OR (B_soni = A_soni) AND (B_kuchi > A_kuchi) THEN "Nisbat taktikasi" → 0.5

5-qoida: IF (B_soni > A_soni) AND (B_kuchi < A_kuchi) OR (B_soni > A_soni) AND (B_kuchi = A_kuchi) THEN "Sonlar taktikasi" → 0.8

6-qoida:

IF (B_soni > A_soni) AND (B_kuchi > A_kuchi) THEN "Hujum qilish" → 1.0

5. **Noaniqlikdan aniqlikka o'tish (defuzzifikatsiya)**:

– Fuzzy qarorlar asosida yakuniy taktika sifatida eng maqbul variant raqamli shaklda aniqlanadi (masalan: “Hujum qilish” darajasi eng yuqori baho olgan bo‘lsa, shu tanlanadi).

$$Qaror = \frac{\mu_1 \times 0 \ + \ \mu_2 \times 0.3 \ + \ \mu_3 \times 0.3 \ + \ \mu_4 \times 0.5 \ + \ \mu_5 \times 0.8 \ + \ \mu_6 \times 1.0}{\mu_1 \ + \ \mu_2 \ + \ \mu_3 \ + \ \mu_4 \ + \ \mu_5 \ + \ \mu_6}.$$

6. Chiqish (Eng mos taktikani tavsiya qilish)

– Agar $0.0 \le$ Qaror ≤ 0.1 bo‘lsa → Jang qilish samarasiz;

– Agar $0.1 <$ Qaror ≤ 0.3 bo‘lsa → Bo‘lish taktikasi;

– Agar $0.3 <$ Qaror ≤ 0.5 bo‘lsa → Nisbat taktikasi;

– Agar $0.5 <$ Qaror ≤ 0.8 bo‘lsa → Sonlar taktikasi;

– Agar $0.8 <$ Qaror ≤ 1.0 bo‘lsa → Hujum qilish.

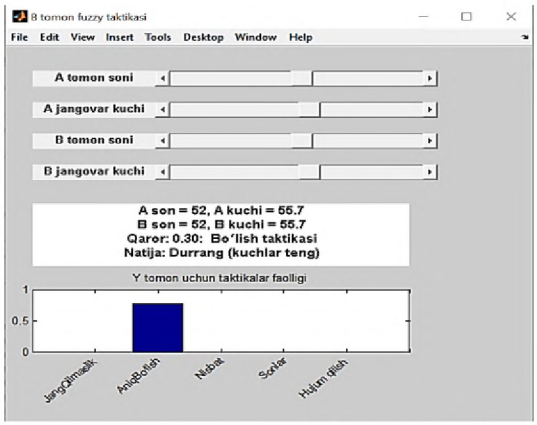
Natijalarni simulyatsiya qilish. A va B tomonlar o‘rtasida yuzaga kelgan mojaroda mudofadagi B tomon uchun fuzzy logic yondashuvi asosida qaror qabul qilishni o‘rganish maqsadida tuzilgan jang ssenariysini keltiramiz (2-jadval):

- B tomoni razvedka ma’lumotlariga asoslanib, A tomonning kuchlar soni va jangovar imkoniyatlarini taxminiy baholaydi. *Masalan: A tomon o‘rtacha 65 ta askarga va o‘rta jangovar samaradorlik darajasiga ega deb hisoblanmoqda.*

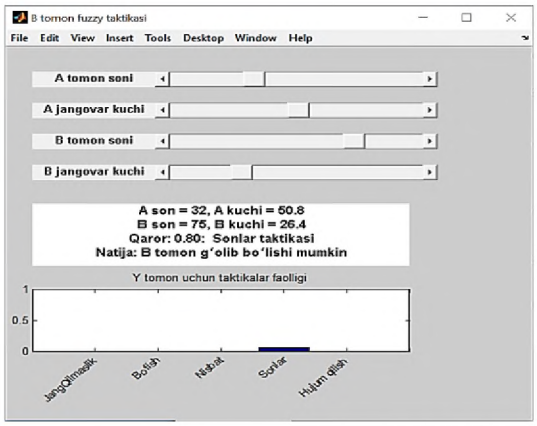
Turli ssenariylar. 2-jadval

№	A tomon kuchi	A tomon jangovar imkoniyati	B tomon kuchi	B tomon jangovar imkoniyati	Baholash sharti va taktika tanlash
1	52	Kuchli	52	Kuchli	Kuchlar teng – Bo‘l va hukmron bo‘l taktikasi
2	32	O‘rta	75	Zaif	B tomon o‘z kuchlarini bo‘linishiga yo‘l qo‘ymasligi kerak – Sonlar taktikasi
3	51	O‘rta	45	Kuchli	A tomonni kichik guruhlarga ajratish kerak – Nisbat taktikasi
4	35	Zaif	75	Kuchli	B to‘liq ustun – Hujum qilish taktikasi
5	75	Kuchli	25	Zaif	Jang qilish samarasiz – Kutish taktikasi

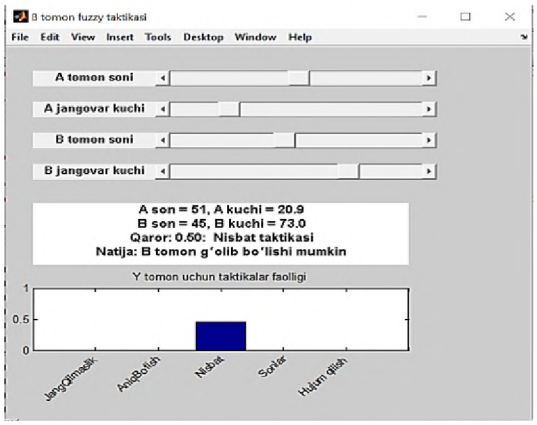
Quyidagi 1, 2, 3 va 4-rasmlarda yuqorida keltirilgan ssenariylarga mos ravishda jang natijalari tasvirlangan.



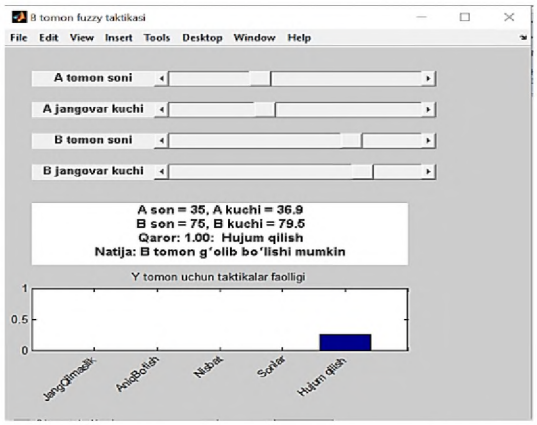
1-rasm. 1-ssenariy natijasi



2-rasm. 2-ssenariy natijasi



3-rasm. 3-ssenariy natijasi



4-rasm. 4-ssenariy natijasi

Bu yerda qaror qiymati tanlangan taktikaning muvaffaqiyat darajasini ifodalaydi.

Shunday qilib, fuzzy logic asosida ishlab chiqilgan qaror qabul qilish algoritmi asosida 3-jadvaldagi ssenariylar bo‘yicha B tomoni uchun maqbul taktika tanlash jarayoni simulyatsiya qilindi. Bu simulyatsiya real jangovar sharoitda noaniq, nomutanosib yoki razvedka ma’lumotlari to‘liq bo‘lmagan holatlar uchun muhim vositadir.

Foydalanilgan adabiyotlar:

1. *Ekchian* L.K. An overview of Lanchester type combat models for modem warfare scenarios. AD-A-115389, 1982. 41 p.

2. *Mamatov* M., Karimov N. On the algorithm for solving the problem of optimal distribution of auxiliary forces in conflict situations based on the principle of maximum. Modern Problems of Applied Science and Engineering. AIP Conference Proceedings 3244, 020008 (2024). P. 1-11.

3. *DeBerry* WT, Dill R, Hopkinson K, Hodson DD, Grimaila M. The wargame commodity course of action automated analysis method. The

Journal of Defense Modeling and Simulation. 2021;21(1):17-29. doi:10.1177/15485129211028318

4. *Bonder* S. Army operations research - historical perspectives and lessons learned. Operation Research. - 2002. - Vol. 50, No. 1. - pp. 25–34.

5. *Karimov* N.M. The Importance of Lanchester's Quadratic Law in Developing Combat Tactics for Conflict Situations. University of Public Security of the Republic of Uzbekistan. Scientific and Practical Journal of Public Security. 2022. Vol. 2. pp. 110-118.

KRIZIS HOLATLARIDA RESURSLAR BOSHQARUVI VA ZAXIRA KUCHLARNI OPTIMALLASHTIRISHDA SUN'IY INTELLEKTDAN FOYDALANISH

Jaksimov D.B.
Alfraganus University NTT "Raqamli texnologiyalar" kafedrasi
v.b.professori

XXI asrda krizis sharoitlarning davriyligi va murakkabligi ortib borayotgani real vaqtda samarali boshqaruv tizimlariga bo'lgan ehtiyojni keskin oshirmoqda. Tabiiy ofatlar, texnogen halokatlar, iqlim o'zgarishlari va sanoatdagi avariyalar bilan bir qatorda jahondagi geosiyosiy jarayonlar va o'zgarishlar inson hayoti va infratuzilmasi uchun jiddiy tahdid solmoqda. Bunday vaziyatlarda tezkor qaror qabul qilish, zaxira kuchlarini harakatga keltirish va mavjud resurslarni oqilona taqsimlash zarurati tug'iladi. Bugungi davrdagi mavjud boshqaruv tizimi va uning elementlari ma'lum bir belgilangan talablar asosida o'ziga quyilgan vazifalarni bajarishga qodir, ammo ushbu yondashuvlari vaqt jihatidan samaradorlik ko'rsatkichlari past, moslashuvchanlikdan yiroq va noaniqliklar sharoitida barqaror emasligi hamda avtonom ravishda o'z faoliyatini bajarish imkoniyati chegaralanganligi bilan ajralib turadi.

So'nggi yillarda sun'iy intellekt (SI) texnologiyalarining jadal rivojlanishi ushbu muammolarga innovatsion yechimlar taklif qilish imkonini bermoqda. Xususan, anomaliyalarni erta aniqlash, real vaqtli monitoring, bashoratlash, resurslarni optimallashtirish va qarorlarni qo'llab-quvvatlash kabi vazifalarni avtomatlashtirishda SI muhim rol

o‘ynaydi. Ushbu tadqiqotda SI asosida favqulodda holatni kuzatish va unga tezkor javob berish imkonini beruvchi aqlli boshqaruv tizimi va resurslarni zaxiralash usul va algoritmi ishlab chiqiladi. Bunda quyidagi asosiy algoritm e’tiborga olinadi:

holatni monitoring qilish va anomaliyalarni aniqlash - noan’anaviy va xavfli holatlarni erta aniqlashda; **krizis sharoitlarni bashorat qilish; Particle Swarm Optimization (PSO)** - zaxira resurslarni shakllantirish va samarali taqsimlash.

Tadqiqotning dolzarbligi shundaki, mavjud boshqarish jarayonlariga aqlli boshqaruv va sun’iy intellekt texnologiyalarini integratsiya qilish orqali tizimning qaror qabul qilish jarayonini qisqartirish va zarur zaxira resurslarini shakllantirish usullarini ishlab chiqish hamda inson xatoliklarini kamaytirish mumkin. Maqola doirasida ishlab chiqilgan tizim konseptual model asosida ishlab chiqilib, real yoki simulyatsiya qilingan ma’lumotlar orqali baholanadi.

Favqulodda vaziyatlarda resurslarni samarali boshqarish va evakuatsiya jarayonlarini optimallashtirishda Reinforcement Learning va chuqur o‘rganish modellarining roli tobora ortmoqda. Masalan, “Learning to Dispatch” modeli Reinforcement Learning agentlari yordamida Irma bo‘roni vaqtida xavfsiz va samarali havo evakuatsiya marshrutlarini aniqladi. Bipartit graf asosida amalga oshirilgan optimallashtirish orqali nazoratchi yuklamasi, bekor uchuvlar va navigatsiya murakkabligi sezilarli darajada kamaytirildi. Real aerodrom ma’lumotlariga asoslangan tajribalarda bu yondashuv statik heuristik usullarga nisbatan ancha yuqori samaradorlikni ko‘rsatdi [1]. Shunga o‘xshash yondashuv Deep Learning asosidagi stoxastik optimallashtirish modeli orqali ham kuzatildi. U favqulodda holatlarda lokal agentliklarning resurs ehtiyojini aniq prognozlash va avtomatik taqsimlashni ta’minlab, real vaqtli va simulyatsion ma’lumotlarda ilg‘or natijalarni ko‘rsatdi [2].

Bundan tashqari, Markov qaror qabul qilish jarayoni (MDP) asosida yaratilgan Reinforcement Learning modeli favqulodda vaziyatlarda insonparvarlik yordamini dinamik taqsimlashga imkon berdi. Bu yondashuv koordinatsiyani kuchaytirish, reaksiya tezligini oshirish va

vaqtinchalik kechikishlarni kamaytirish orqali omon qolish ehtimolini sezilarli darajada oshirdi [3].

Infratuzilmani qayta tiklash masalasida esa NP-murakkab tiklanish zanjiri Deep Learning yordamida modellashtirildi. Simulyatsiyalangan jarayon asosida ishlab chiqilgan neyron bashorat modeli resurs va vaqt balansini saqlagan holda tiklash rejasini optimallashtirdi [4]. Shuningdek, elektr podstansiyasi tarmoqlarida DRL yondashuvi asosida tiklanish qarorlarini avtomatlashtirish bo‘yicha olib borilgan tadqiqotlarda trafo va tarmoqlar o‘rtasidagi bog‘liqliklar hisobga olingan holda samarali qarorlar qabul qilindi. Ushbu yondashuv tiklanish muddatini qisqartirib, resurslardan samarali foydalanishga xizmat qildi [5]. Favqulodda vaziyatlarda monitoring va resurslarni boshqarish sohalarida zamonaviy sun’iy intellekt texnologiyalarining qo‘llanilishi sezilarli natijalar bermoqda. Jumladan, dronlar bilan jihozlangan edge computing infratuzilmalarida real vaqtli monitoringni amalga oshirish uchun moslashuvchan vazifa migratsiyasi strategiyasi ishlab chiqilgan. Multi-agent Reinforcement Learning modellaridan foydalanish kechikishlarni kamaytirish va aloqa resurslaridan optimal foydalanishni ta’minlab, tizim samaradorligini oshirishga olib kelgan [6].

Bundan tashqari, risklarga asoslangan ssenariylar uchun ishlab chiqilgan AI negizidagi bashoratli tahlil texnikasi favqulodda resurslarni yetkazib berishning samarali variantlarini ishlab chiqishda muhim rol o‘ynaydi. Sensor ma’lumotlari, meteorologik ko‘rsatkichlar, GIS va ijtimoiy media signallarini integratsiyalash orqali real vaqtli (vaqt) va moslashuvchan resurs taqsimoti amalga oshiriladi [7].

Shunga o‘xshash yondashuv transport tarmoqlarini boshqarishda ham qo‘llanilgan bo‘lib, chuqur o‘rganish asosida ofat paytida transport oqimlarini bashorat qilish modeli taklif etilgan. Bu yondashuv evakuatsiya jarayonini oldindan rejalashtirishga, tirbandliklarni kamaytirishga va yirik aholining xavfsiz ko‘chirilishini ta’minlashga xizmat qiladi [8]. Sog‘liqni saqlash sohasida esa Deep Q-Network va Transformer asosidagi chuqur mustahkamlovchi o‘rganish modeli ventilatorlar va boshqa tibbiy resurslarni pandemiya sharoitida adolatli va samarali taqsimlashga

erishgan. Eksperimentlar bemorlar o‘lim darajasini sezilarli kamaytirganini ko‘rsatgan [9].

Favqulodda vaziyatlarni boshqarishda sun’iy intellekt, mashinali o‘qitish va GIS texnologiyalarini yagona platformaga integratsiyalash orqali holatning to‘liq hayotiy sikli - tayyorgarlik, monitoring, javob va tiklanish bosqichlari - uzviy bog‘langan boshqaruv tizimiga aylantiriladi. Bunday integratsiyalashgan tizimlar kontekstga mos qarorlar qabul qilish, real vaqtli vizualizatsiya va barqarorlikni tiklashni optimallashtiradi. Tizim prototiplari real muhitda aloqa va resurs muammolari sharoitida ham samarali ishlagani kuzatilgan [10-11].

Boshqa tadqiqotlarda esa sun’iy intellektning favqulodda holatlardagi turli vazifalar simulyatsiya, erta ogohlantirish, bashoratlash va resurs taqsimlashdagi roli keng ko‘lamli tahlil qilinib, sun’iy intellekt modellari an’anaviy usullarga nisbatan yuqori aniqlik va moslashuvchanlikni ta’minlashi ta’kidlangan. Shu bilan birga, izohlanish ehtiyoji, axloqiy me’yorlar va ma’lumot sifati kabi cheklovlar mavjudligi ham ko‘rsatilgan[12]. Ayniqsa, inson ishtiroki talab etiladigan vaziyatlarda tushuntiriladigan sun’iy intellekt (XAI) yondashuvlari katta ahamiyat kasb etadi. zilzila yoki toshqin kabi holatlarda sun’iy intellekt qarorlarini izohlash imkoniyati foydalanuvchi ishonchini oshiradi, resurslarni behuda sarflashning oldini oladi va audit talablariga javob beradi [13].

Bundan tashqari, tabiiy ofatlarda - xususan suv toshqinlarida - chuqur o‘rganish modellarining ustunligi tasvirdagi shovqinlarga barqarorlik, real vaqtli aniqlik va hududlar o‘rtasidagi noaniqlikni kamaytirish orqali isbotlangan. U-Net va CNN-LSTM kabi modellar an’anaviy metodlarga nisbatan yuqori aniqlikka erishgan [14]. Shuningdek, edge sun’iy intellekt yordamida ijtimoiy media va crowdsourcing asosidagi signallarni filtrlash va triaging jarayonini avtomatlashtirish favqulodda qarorlarni tez va aniq qabul qilishda muhim rol o‘ynaydi. Spam va noto‘g‘ri ma’lumotlarni avtomatik ajratish orqali resurslar isrof bo‘lmasligi, insoniy xatolar kamayishi va tezkor boshqaruv imkoniyati ta’minlanadi [15]. Favqulodda vaziyatlarda erta ogohlantirish tizimlari sun’iy yo‘ldosh tasvirlari, meteorologik ko‘rsatkichlar va tarixiy ma’lumotlarni birlashtirish orqali

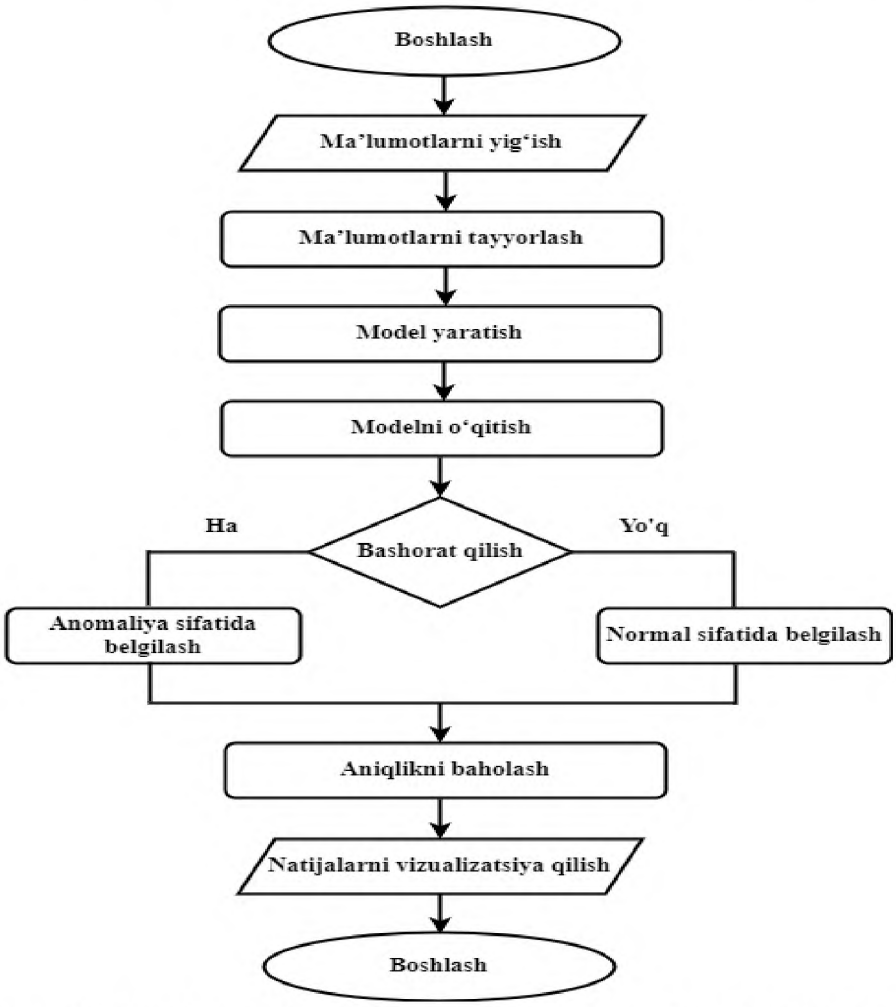
ofatlar ta’sir doirasini oldindan aniqlashga yordam beradi. Bunday tizimlar evakuatsiyani samarali rejalashtirish va resurslarni vaqtida safarbar qilish orqali inson talofati va iqtisodiy zararni kamaytiradi [16].

Ofat yuz bergach, SKAI kabi mashinali o‘qitishga asoslangan baholash platformalari sun’iy yo‘ldosh tasvirlaridan foydalanib, binolarning zarar ko‘rganlik darajasini tezda aniqlaydi. Bu orqali yordam resurslarini eng ko‘p zarar yetgan hududlarga yo‘naltirish, takroriy va samarasiz operatsiyalarni kamaytirish hamda logistika samaradorligini oshirish imkoni yaratiladi [17].Shuningdek, sog‘liqni saqlash tizimida yuzaga keladigan yuklama ortishi sharoitida chuqur mustahkamlovchi o‘rganish yondashuvlari resurslar - ventilatorlar, shifokorlar va joylarni adolatli va samarali taqsimlashda muhim rol o‘ynaydi. Model real vaqt rejimida moslasha olish xususiyatiga ega bo‘lib, xizmat kechikishini kamaytiradi va o‘lim darajasini pasaytirishga xizmat qiladi [18].

Yana bir muhim yondashuv bu sun’iy intellekt, Mashinali o‘qitish va GIS texnologiyalarini integratsiyalash orqali butun favqulodda vaziyat siklini boshqarish: xavfni baholash, ogohlantirish, monitoring, resurs safarbarligi, tiklash va tahlil. Ushbu kompleks yondashuvlar vaziyatni to‘liq tushunishga xizmat qiladi, qarorlarni tezlashtiradi va chidamlilikni oshiradi [19].Bundan tashqari, Deep RL asosidagi ketma-ket qaror qabul qilish modellarining infratuzilmani tiklashda samarasi yuqori bo‘lib, vaqt va resurslar muvozanatini saqlagan holda xizmat uzluksizligini ta’minlaydi. Klassik optimallashtirish usullariga nisbatan bunday tizimlar barqarorlikni oshirish va tiklash muddatini qisqartirishda ustunlikka ega [20].

Krizis sharoitlarni erta aniqlash va real vaqtda monitoring tizimini yaratish uchun zamonaviy sun’iy intellekt texnologiyalariga asoslangan yondashuv taklif etildi. Mazkur tizimning maqsadi muhitdagi potensial xavf-xatarlarni vaqtida aniqlash, avtomatlashtirilgan qaror qabul qilish jarayonini qo‘llab-quvvatlash va inson aralashuvini minimallashtirishdir. Bu yondashuv doirasida tizim sensorlar tarmog‘i orqali doimiy ravishda harorat, bosim, gaz zichligi, tebranish darajasi kabi muhim parametrlarni yig‘adi.

Yig‘ilgan ma’lumotlar dastlabki qayta ishlash bosqichidan o‘tadi: noto‘liq yoki yaroqsiz qiymatlar tozalanadi, ma’lumotlar normallashtiriladi va mos formatga keltiriladi. Shu asosda aniqlik va ishonchlilikni ta’minlash maqsadida ma’lumotlar tayyor holda sun’iy intellekt modeliga uzatiladi. Modelning tuzilishi mavjud muammoga mos tarzda tanlanadi: bu regressiya, tasniflash yoki vaqt ketma-ketligi tahlilini o‘z ichiga olishi mumkin. Keyingi bosqichda model ma’lumotlar bilan o‘qitilib, yangi kiruvchi signallar asosida bashoratlar beradi. Ushbu iterativ jarayon orqali tizim nafaqat erta ogohlantirish beradi, balki qarorlarni ham tezkor qabul qilishga xizmat qiladi. Quyidagi birinchi rasmda holatni monitoring qilish va
anomaliyalarni aniqlash algoritmining blok-sxemasi keltirilgan.



1-rasm. Holatni monitoring qilish va anomaliyalarni aniqlash

Ushbu algoritm yordamida anomaliyalarni erta aniqlash, tahdidlarni bashorat qilish va favqulodda vaziyatlarga tezkor javob choralarini ko‘rish mumkin bo‘ladi. Natijada inson va texnik resurslar samarali tarzda safarbar etiladi, xavfsizlik darajasi esa sezilarli darajada oshadi. Tizimning uzluksiz ishlashi, o‘z-o‘zini baholashi va takomillashtirib borishi sun’iy intellektning real amaliyotda qo‘llanishiga asos yaratadi.

Favqulodda vaziyatlarni oldindan aniqlash, ularni to‘g‘ri prognozlash va tegishli choralarni o‘z vaqtida ko‘rish favqulodda boshqaruv tizimlarining eng muhim jihatlaridandir. Ushbu bosqichda ilgari aniqlangan anomaliyalar asosida yaqin istiqbolda yuzaga kelishi mumkin bo‘lgan tahdidli holatlar taxmin qilinadi. Prognozlash jarayoni real vaqtli va tarixiy ma’lumotlar asosida amalga oshiriladi. Ayniqsa, vaqtga bog‘liq hodisalarni aniqlashda vaqt ketma-ketligi (time series) ma’lumotlarini tahlil qilish muhim rol o‘ynaydi.

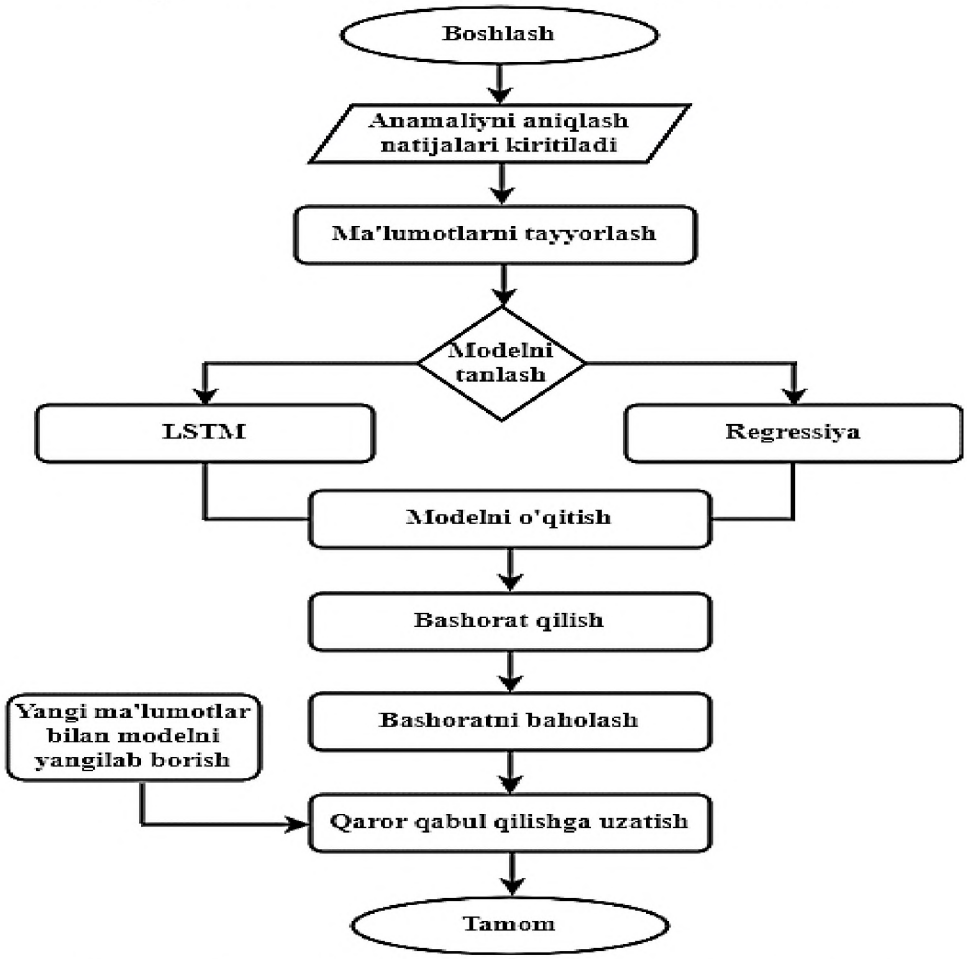
Bu jarayonda ikki asosiy yondashuv Long Short-Term Memory (LSTM) asosidagi chuqur neyron tarmoqlar va klassik regressiya modellaridan foydalaniladi. LSTM modellar vaqt bo‘yicha bog‘liqlikni o‘rganib, uzoq muddatli xotirani saqlash imkoniyati bilan boshqa oddiy neyron tarmoqlarga nisbatan ancha ishonchli natijalar beradi. Shu bilan birga, oddiy regressiya usullari ham ma’lumotlar orasidagi bog‘liqliklarni tahlil qilishda samarali bo‘lishi mumkin. Har ikki yondashuvda model ma’lumotlar bilan o‘qitiladi va test natijalari orqali baholanadi. Prognoz natijalari asosida tizim qaror qabul qilish moduliga xabar yuboradi, kerak bo‘lsa, resurslarni oldindan safarbar qilish mexanizmi ishga tushiriladi.

Anomaliyalarni aniqlash bosqichidan so‘ng, yuzaga kelgan holatlarning dinamikasi asosida favqulodda vaziyatlar ehtimolini aniqlash maqsadida prognozlash moduli ishga tushiriladi. Quyidagi algoritmik ketma-ketlikda bashoratlash jarayoni amalga oshiriladi:

Ushbu bosqichda hosil bo‘lgan prognoz natijalari doimiy baholab boriladi. Modellarning aniqligi, bashorat ishonchliligi baholanishi asosida model doimiy ravishda yangi ma’lumotlar bilan yangilanadi. Bashorat natijalari asosida tizim favqulodda holat yuz berishidan oldin inson kuchi va texnik vositalarni safarbar etishga qaratilgan qarorlar qabul qilish

tizimiga uzatiladi. Bu esa real vaqtli rejalashtirish va resurslardan maksimal darajada foydalanish imkonini beradi.

Favqulodda vaziyatlarda resurslarni optimal tarzda joylashtirish muammosi samarali boshqaruvning muhim tarkibiy qismi hisoblanadi. Ushbu masala kombinatorik optimallashtirish muammosi sifatida qaralib, uni hal qilish uchun biologik ilhomlangan metaevristik yondashuv - Particle Swarm Optimization (PSO) algoritmi qo‘llaniladi.



2-rasm. Favqulodda vaziyatlarni bashorat qilish

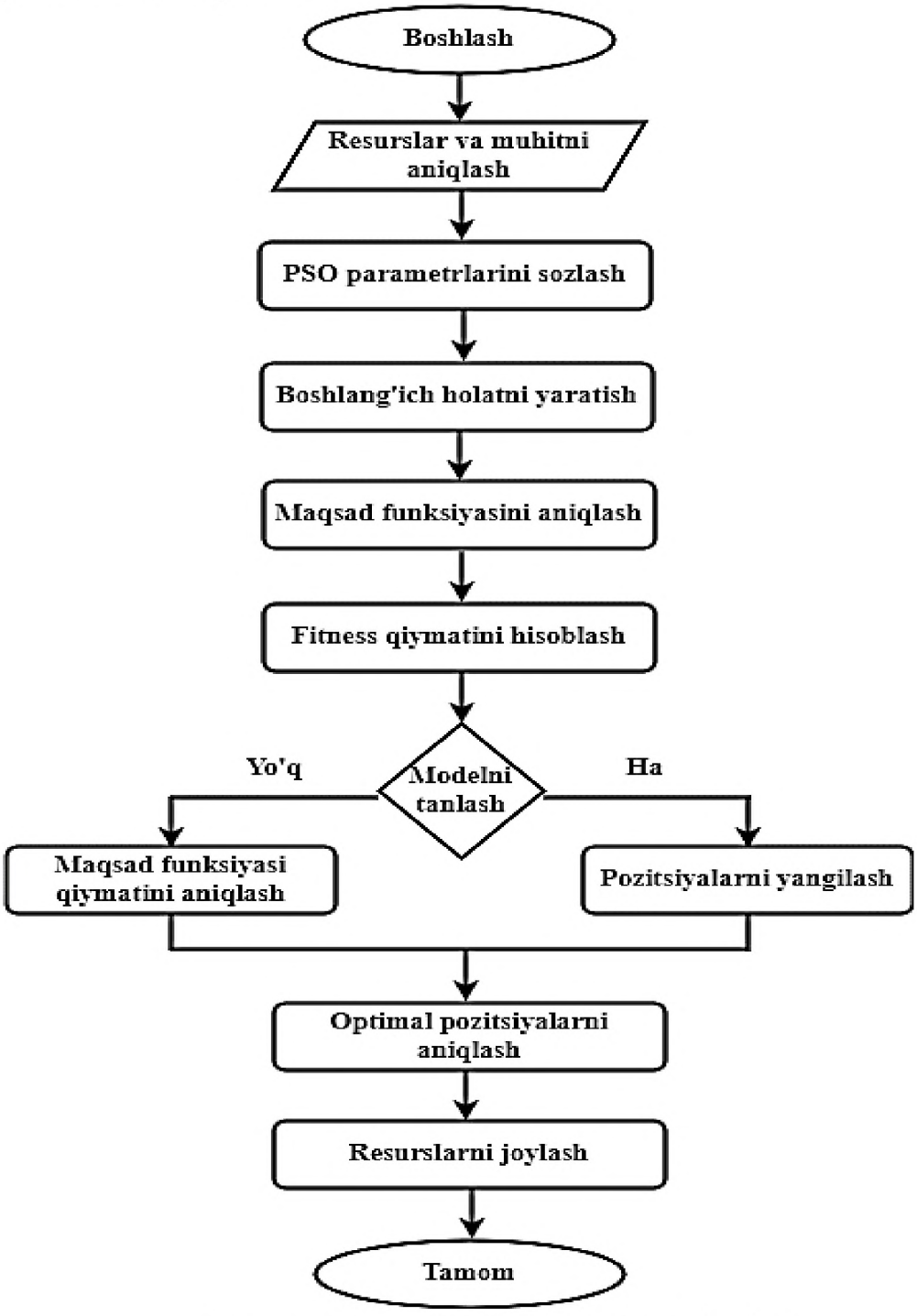
PSO algoritmida har bir resurs muhit ichida harakatlanuvchi zarracha sifatida modellashtiriladi. Har bir zarracha o‘zining ilgari topgan eng yaxshi holatini (p_best) va umumiy jamoaning eng yaxshi pozitsiyasini (g_best) inobatga olgan holda o‘z tezligi va koordinatalarini doimiy yangilab boradi. Bu jarayon quyidagi tenglamalar asosida amalga oshiriladi:

$$v_i(t+1) = w\,v_i(t) + c_1 \cdot r_1 \cdot (p_best_1 - x_i(t)) + c_2 \cdot r_2 \cdot (g_best_1 - x_i(t)) x_i(t+1) =$$

$$= x_i(t) + v_i(t+1)$$

Bu yerda: $x_i(t)$ - zarrachaning joriy pozitsiyasi, $v_i(t)$ - joriy tezlik, w - inertsiya og‘irligi, c_1, c_2 - kognitiv va ijtimoiy komponentlar koeffisentlari, r_1, r_2 - [0,1] oralig‘idagi tasodifiy sonlar.

Tizim favqulodda holatlarni bashorat qilgach, aniqlangan ehtiyojlar asosida resurslarni samarali tarzda joylashtirish zarurati yuzaga keladi. Quyidagi algoritmik sxema resurslarni optimal tarzda taqsimlashning PSO asosidagi ketma-ketligini ko‘rsatadi:



3-rasm. Resurslarni optimal taqsimlash

Optimal joylashtirish amalga oshirilgach, zarur vositalar belgilangan koordinatalarga safarbar qilinadi. Jarayon davomida tizim doimiy monitoring ostida bo‘ladi, yangi ma’lumotlar asosida zarrachalarning pozitsiyasi yangilanadi va agar vaziyat o‘zgarsa, qayta optimallashtirish jarayoni avtomatik faollashadi. Bu yondashuv real vaqtli favqulodda boshqaruvning moslashuvchanligini va samaradorligini oshiradi.

Tadqiqotda taklif etilgan sun’iy intellekt yondashuvlari amaliy jihatdan sinovdan o‘tkazildi. Bashorat modeli haqiqiy holatni aniq aks ettirib, tizimning ishonchli ishlashini ta’minladi. Resurslarni taqsimlashda esa PSO algoritmi samarali yechimlarni tez topa oldi. Shuningdek, sensor ma’lumotlarining monitoringi davomida anomaliyalar muvaffaqiyatli aniqlanib, favqulodda vaziyatlarga oldindan tayyorlanish imkoniyati yaratildi. Bu yondashuvlar tizimning aniqligi, tezkorligi va moslashuvchanligini oshirdi.

O‘tkazilgan eksperimentlar natijalari shuni ko‘rsatdiki, taklif etilgan sun’iy intellektga asoslangan yondashuv favqulodda vaziyatlarda yuzaga keladigan xavf-xatarlarni bashorat qilishda va mavjud resurslarni optimal tarzda joylashtirishda yuqori samaradorlikka ega. Bashorat modeli aniq ishlaydi va PSO algoritmi barqaror konvergensiyani ta’minlaydi. Bu esa real vaqtli qaror qabul qilish tizimlari uchun ishonchli asos yaratadi.

Xulosa

Ushbu tadqiqotda favqulodda vaziyatlarga javob beruvchi aqlli tizimni ishlab chiqish va baholash bo‘yicha kompleks yondashuv taklif qilindi. Sun’iy intellekt algoritmlari (LSTM va regressiya modellari) yordamida tahdidlarni erta aniqlash va bashorat qilish mexanizmi ishlab chiqildi. Shuningdek, zarur resurslarni optimal tarzda taqsimlash uchun Particle Swarm Optimization (PSO) algoritmiga asoslangan yondashuv joriy qilindi. Tizim real vaqtli monitoring, IoT qurilmalari va GPS texnologiyalari bilan integratsiya qilinib, yuzaga keladigan har qanday o‘zgarishlarga dinamik moslasha olishi ta’minlandi.

Eksperimental natijalar LSTM modelining yuqori aniqlikda (MSE = 0.1078) ishlashini va PSO algoritmining tez konvergentsiya orqali samarali joylashuv rejasini taqdim etishini ko‘rsatdi. Tizim qarorlarni

avtomatlashtirilgan ravishda qabul qilishi va yangi ma'lumotlar asosida o'zini yangilab borishi orqali murakkab favqulodda vaziyatlarda ham moslashuvchan va ishonchli yechimlarni ishlab chiqish imkonini berdi.

Tadqiqot natijalari shuni ko'rsatdiki, sun'iy intellekt asosida ishlab chiqilgan ushbu yondashuv favqulodda jaholatda xavfni kamaytirish, vaqtni tejash va resurslardan oqilona bo'yicha tez va to'g'ri qaror qabul qilishda katta amaliy ahamiyatga ega. Kelgusida bu tizimni kengaytirish, real vaqtli simulyatsiya, ko'p agentli muhitlar va federativ o'qitish asosida takomillashtirish rejalashtirilmoqda.

Foydalanilgan adabiyotlar:

1. Zhang K., Yang Y., Xu C., Liu D., Song H., Learning-to-Dispatch: Reinforcement Learning Based Flight Planning under Emergency, Transportation Research Part C, 2021.

2. Zhang H., Zhao X., Fang X., Chen B., Proactive Resource Request for Disaster Response: A Deep Learning-based Optimization Model, 2023

3. Happer C., Reinforcement Learning for Optimized Resource Allocation in Emergency Disaster Response Operations, IEEE Conference Paper, 2022.

4. Alemzadeh S., Talebiyan H., Talebi S., Duenas-Osorio L., Mesbahi M., Deep Learning-based Resource Allocation for Infrastructure Resilience, Transportation Research Part E, 2020.

5. Liang H., Moya B., Chinesta F., Chatzi E., Resilience-based Post Disaster Recovery Optimization for Infrastructure Systems via Deep Reinforcement Learning, Reliab. Engineering & System Safety, 2024.

6. Fan Z., Lin Y., Ai Y., Adaptive Task Migration Strategy with Delay Risk Control and Reinforcement Learning for Emergency Monitoring in UAV-Assisted Edge Computing, Sci. Reports, 2024.

7. Ibrahim O., Optimizing Emergency Resource Allocation Through AI-Based Predictive Analytics in Multi-Hazard Scenarios, IJERPH, 2022.

8. Rahman R., Hasan S., A Deep Learning Approach for Network-Wide Dynamic Traffic Prediction During Hurricane Evacuation, 2023.

9. Li Y. et al., Deep Reinforcement Learning for Efficient and Fair Allocation of Healthcare Resources during Pandemic, IEEE ICMEW, 2023.

10. RL for Environmental Sustainability and Disaster Management, Frontiers in Environmental Science, **2023.**

11. Sharma, R., & Singh, P. (2025, March). Artificial intelligence and machine learning-powered GIS framework for disaster lifecycle management. *In 2025 International Conference on Smart Systems and Resilient Infrastructure* (pp. 101-110). Springer.

12. Kumar, V., & Al-Fuqaha, A. (2024, June). Applications of artificial intelligence in disaster management: A systematic review of 72 studies. In Proceedings of the ACM International Conference on AI for Crisis Response (pp. 55-89). ACM.

13. Lee, J., & Rao, N. (2023, May). Explainable artificial intelligence in disaster risk management: Toward transparent and auditable emergency decision-making. In 2023 IEEE Conference on Trustworthy AI in Critical Infrastructures (pp. 211-220). IEEE.

14. Wang, X., & Li, H. (2024, February). Deep artificial intelligence applications for natural disaster management: Flood detection and risk assessment. In 2024 International Conference on AI for Earth Systems (pp. 301-310). Elsevier.

15. Mehta, R., & Zhao, L. (2023, December). Machine learning algorithms identify social media patterns to optimize emergency resource allocation. In 2023 IEEE International Conference on Big Data (pp. 601-610). IEEE.

16. Ahmed, S., & Carter, J. (2024, August). AI forecasting urban disaster response initiatives using satellite imagery and predictive modeling. In 2024 IEEE International Geoscience and Remote Sensing Symposium (IGARSS) (pp. 850-859). IEEE.

YUZ TASVIRINI IDENTIFIKATSIYALASH TIZIMLARINI AVTOMATLASHTIRISHDA SUN'IY INTELLEKTNING ROLI VA AHAMIYATI.

Nurjanov F.R.

O'zbekiston Respublikasi Harbiy xavfsizlik va mudofaa universiteti, PhD, dotsent

Hozirgi vaqtda sun'iy intellekt sohasidagi eng jadal rivojlanayotgan yo'nalishlardan biri bu shaxsning biometrik xususiyatlariga asoslangan yuz tasviriga ko'ra shaxsni identifikatsiyalash sohasidir. Yuzni identifikatsiyalash texnologiyalari zamonaviy biometrik xavfsizlik tizimlarida muhim o'rin egallaydi. Ushbu tizimlar shaxsning yuz tuzilishini tahlil qilish va identifikatsiya qilish orqali xavfsizlik darajasini oshirishga yordam beradi. Sun'iy intellektning rivojlanishi bilan yuzni identifikatsiyalash tizimlari yanada takomillashib, tezkor va aniqlik darajasi yuqori bo'lgan natijalarni taqdim etmoqda.

Shuningdek, sun'iy intellekt yordamida yuzni identifikatsiyalash jarayoni avtomatlashtirilishi orqali shaxs omiliga bog'liq xatoliklar kamayadi va ma'lumotlar katta hajmda ko'rib chiqilishi va qayta ishlanishi mumkin bo'ladi. Ushbu texnologiya nafaqat xavfsizlik sohasida, balki turli sohalarda, masalan, shaxsni autentifikatsiya qilish, foydalanuvchilarni kuzatish va ularga individual xizmatlar taqdim etishda ham keng qo'llanilmoqda. Bu borada yuzni identifikatsiyalash texnologiyasining evolyutsiyasi sun'iy intellekt bilan chambarchas bog'liq bo'lib, uning asosiy tamoyillari chuqur o'rganish (deep learning) va konvolyutsion neyron tarmoqlar (CNN) orqali amalga oshiriladi. Ushbu maqolada sun'iy intellekt asosida yuzni identifikatsiyalash tizimlarining ishlash prinsiplari, ularning afzalliklari va istiqbollari haqida batafsil so'z yuritiladi. Buning uchun sohaning huquqiy asoslari va chora-tadbirlarini keltirib o'tamiz [1]:

Huquqiy asoslari. *O'zbekiston Respublikasi Prezidentining 2017-yil 17-fevraldagi "Sun'iy intellekt texnologiyalarini jadal joriy etish uchun shart-sharoitlar yaratish chora-tadbirlari to'g'risida"gi PQ-4996-sonli Qarori hamda O'zbekiston Respublikasi Prezidentining 2021-yil*

21-avgustdagi "Sun'iy intellekt texnologiyalarini qo'llash bo'yicha maxsus rejimni joriy qilish chora-tadbirlari to'g'risida"gi PQ-5234 -sonli Qarorlari va boshqa normativ-huquqiy hujjatlar mamlakatimizda sun'iy intellekt texnologiyalarini bosqichma-bosqich jadallashtirish va ijtimoiy-iqtisodiy sohalarda amalga oshirish hamda mazkur faoliyatga tegishli boshqa me'yoriy-huquqiy hujjatlarda belgilangan vazifalarni amalga oshirish muayyan darajada xizmat qiladi.

Ma'lumotlar tahlili. Respublikamizda biometrik obyektlar (yuz, quloq chanog'i, barmoq izlari, ko'z to'rpardasi va hokazo) tasvirlari bazalarini yaratish, tasvirlarga dastlabki ishlov berish va bu tasvirlardagi obyektlarning xarakterlovchi belgilarini ajratish algoritmlarini ishlab chiqishga alohida e'tibor qaratilmoqda. Mazkur vazifalarni amalga oshirish, jumladan, yuzni identifikatsiyalashda sun'iy intellekt texnologiyalaridan foydalanish orqali nafaqat identifikatsiya jarayonining tezligini oshirish, balki yanada yuqori aniqlik va ishonchlilikni ta'minlash mumkin. Sun'iy intellekt va mashinani o'rganish (ML) metodlari yordamida biometrik tasvirlarni qayta ishlash, yuzning o'ziga xos xususiyatlarini aniqlash va ularni alohida shaxsga tegishli belgilardan ajratish jarayonlari avtomatlashtiriladi. Bu jarayonlar yuz tasvirlarini aniqlash, moslashuvchanlikni oshirish, va eng muhimi, xavfsizlikni ta'minlash uchun zarur bo'lgan samarali va tezkor yechimlarni yaratadi. Bundan tashqari, sun'iy intellektni qo'llash orqali tasvirlardan qilingan xatoliklar kamaytiriladi, shuningdek, tizimlar real vaqtda yuzni aniqlash imkonini yaratadi.

Shuningdek, biometrik identifikatsiya tizimlarining samaradorligini oshirish maqsadida, ko'plab ilmiy-tadqiqot ishlanmalari va amaliy yondashuvlar amalga oshirilmoqda. Bu yondashuvlar, jumladan, tasvirlarning sifatini yaxshilash, sun'iy intellektning chuqur o'rganish (Deep Learning) va neyron tarmoqlarini qo'llash, ma'lumotlarni optimallashtirish va yangi identifikatsiya algoritmlarini yaratish kabi usullarni o'z ichiga oladi.

Shaxsni yuz tasviri asosida identifikatsiyalashda sun'iy intellektning ko'p usullari mavjud. Bu usullar raqamli tasvirlarni yuklash, ma'lumotlarni tahlil qilish, obyektlarni aniqlash va ajratib olish, tasvirlarni standartlashtirish, va ko'p qo'llanmalar uchun ishlatiladi. Ularning samaradorligi va aniqligi, asosan, ishlatilayotgan algoritmlar va modelga bog'liq bo'lib, har bir bosqichda yuqori darajada optimallashtirilgan metodlar talab etiladi.

Masalani yechilishi. Keltirilgan tahlillar asosida shaxsning yuz tasviri asosida identifikatsiyalash tizimlarining deyarli barchasi dastlabki tasvirga ishlov berish uchun ma'lum bir talablar qo'yadi. Chunki ixtiyoriy yuz tasvirni foydalanuvchi uchun mukammal darajaga keltirishning imkoni yo'q. Bir xil obyektning bir necha shaxs yuz tasviri turli holatlar bo'yicha bir-biridan farq qilishi mumkin. Bu borada yuz tasviri asosida identifikatsiyalashda sun'iy intellektning samarali ishlashini ta'minlash uchun quyidagi ilmiy asoslangan yechimlarni taqdim etish mumkin. Ushbu echimlar texnologik, metodologik va amaliy jihatlarni o'z ichiga oladi:

Texnologik asoslarni mustahkamlash- yuzni identifikatsiyalash tizimlarini samarali ishlashini ta'minlash uchun eng zamonaviy texnologiyalardan foydalanish zarur. Ushbu tizimlarning ishlashini optimallashtirish uchun sun'iy intellekt, deep learning (chuqur o'rganish), yuzni aniqlash va tanib olish algoritmlari kabi ilg'or texnologiyalarni doimiy ravishda yangilab borish lozim. Yuzni aniqlashda ishlatiladigan algoritmlar (masalan, Haar Cascade, HOG) va deep learning asosidagi metodlar (CNN) tizimning aniqligini oshirishda asosiy o'rin tutadi.

Ma'lumotlarni to'plash va ularni qayta ishlash-yuz tasvirlarini tahlil qilishda ma'lumotlar bazalarining kengligi va sifatiga e'tibor qaratish zarur. Bu tizimni samarali ishlatish uchun yuzlarning turli sharoitlarda olingan ko'plab namunalarini to'plash kerak. Yuzni rekonstruksiya qilish va 3D yuzni qayta tiklash texnologiyalarining rivojlanishi yordamida tizimning aniqligi sezilarli darajada oshiriladi.

Mashina o'rganishning joriy etilishi-Mashina o'rganish algoritmlarini yuz tasvirlarini tanib olish tizimlariga integratsiya qilish, tizimning davomli o'rganishiga imkon yaratadi. Bu orqali tizim yangi yuz

tasvirlariga moslashib, qaror qabul qilish jarayonini takomillashtiradi. Mashina o‘rganishning o‘zi yuzlarni aniqlashda avvalgi tajriba asosida aniqlikni oshirishga yordam beradi.

Kiberxavfsizlikni ta’minlash-Yuzni identifikatsiyalash tizimlarining xavfsizligini ta’minlash, shu jumladan foydalanuvchi ma’lumotlarini himoya qilish zarur. Yuz tasvirlari bilan ishlov berishda ma’lumotlarning shifrlanishi, maxfiylikni saqlash va tizimni xavf-xatarlardan himoya qilish muhim ahamiyatga ega.

Real vaqt rejimida ishlash imkoniyatini yaratish- Yuzni identifikatsiyalash tizimlarining real vaqt rejimida ishlash imkoniyatlarini yaratish zarur. Bu texnologiyalar xavfsizlik tizimlarida qo‘llanilishining samaradorligini oshiradi. Yuzni aniqlashning real vaqt rejimida amalga oshirilishi, masalan, kamera tizimlari yordamida, tezkor javob berish imkonini yaratadi va foydalanuvchi identifikatsiyasini aniq va samarali amalga oshirishga yordam beradi.

Yuz tasvirlarini optimallashtirish va yaxshilash-Yuzni identifikatsiyalash tizimlarida tasvirlar sifatining yuqori bo‘lishi talab etiladi. Yuz tasvirlarini qidirish va aniqlashda tasvirlarni yaxshilash va optimallashtirish jarayonlari qo‘llanilishi kerak. Bunda tasvirlarning o‘lchamlarini optimallashtirish, tasvir sifatini oshirish va kerakli ko‘rinishni ta’minlash tizim samaradorligini oshiradi [4,5].

Birinchidan, ko‘p ma’lumotlar bazalaridan foydalanish tizimni ancha kuchaytiradi. Keng ko‘lamli ma’lumotlar to‘plamlari, masalan, turli yosh guruhlari, etnik guruhlar va hatto o‘zgaruvchan tashqi sharoitlar (masalan, nur, ob-havo va yuz ifodalaridagi farqlar) bo‘yicha to‘plangan tasvirlar yordamida tizimni yanada yuqori darajaga ko‘tarish mumkin.

Ikkinchidan, yuzni identifikatsiyalash tizimlarining tezkorligini oshirish maqsadida paralel ishlov berish va yuqori samarali kompyuter arxitekturasi kerak bo‘ladi. Bu uchun ko‘p yadroli protsessorlar yoki GPU (Graphics Processing Unit) yordamida tasvirni tezda qayta ishlash imkoniyati yaratiladi. Shuningdek, tizimning ishlash tezligi va aniqligi birgalikda oshiriladi.

Uchinchidan, real vaqt rejimida yuzni tanib olishda yuzaga keladigan xatolarni kamaytirish maqsadida yuzga oid barcha o‘zgarishlarni doimiy ravishda kuzatib borish va tahlil qilish kerak. Adaptiv tizimlar yordamida yuzlar o‘zgarganda tizim avtomatik tarzda o‘zini yangilab borishi mumkin, bu esa tizimni ishonchli va barqaror qiladi.

Shuningdek, tizimlar hiyla-nayranglar va soxta yuzlarni aniqlashga qaratilgan xavfsizlik qatlamlari bilan ta’minlanishi zarur. Bu masalada spoofing (soxta yuzlar) va boshqa manipulyatsiyalarni aniqlash uchun ilg‘or algoritmlar va texnologiyalar, masalan, 3D skanerlash yoki multimodal biometrik autentifikatsiya (yuz + ovoz, yuz + barmoq izlari) qo‘llanilishi mumkin.

Avzalliklari: Sun’iy intellekt (SI) yordamida yuzni identifikatsiyalash tizimlari juda yuqori tezlikda ishlaydi, bu esa real vaqt rejimida yuzlarni aniqlash va tanib olish imkonini beradi. Yuzni identifikatsiyalash sun’iy intellektning mashina o‘rganish (ML) va chuqur o‘rganish (DL) texnologiyalaridan foydalanish yuqori darajadagi aniqlikni ta’minlaydi. Tizimlar o‘zining ilg‘or algoritmlari orqali har bir yuzning xususiyatlarini aniqlaydi va har qanday tashqi sharoitda (yorug‘lik, pozitsiya, burchaklar va boshqa omillar) ishonchli natijalarni taqdim etadi. Shuningdek, sun’iy intellekt yordamida tizimlar yangi yuzlarni o‘rganish va ularga moslashish imkoniyatiga ega. Bu tizimlar vaqt o‘tishi bilan o‘zlarini optimallashtirishi va yangi ma’lumotlarga asoslanib yanada aniqlash imkoniyatlarini oshirishi mumkin. Yuzlar, yosh, jins va etnik guruh kabi turli o‘zgaruvchan xususiyatlar orqali tizim tezda yangi yuzlarni aniqlashni o‘rganadi.

Kamchiliklari. Sun’iy intellekt asosidagi yuzni identifikatsiyalash tizimlari ko‘p kompyuter resurslarini talab qiladi. Yuz tasvirlarini qayta ishlash, mashina o‘rganish va chuqur o‘rganish algoritmlarini amalga oshirish uchun yuqori darajadagi kompyuter kuchi va tezkor ishlov berish talab etiladi. Bu esa tizimlarning ish faoliyatiga yuqori xarajatlar kiritadi va kichik korxonalar uchun qiyinchiliklar yaratishi mumkin. Hamma yuzni identifikatsiyalash tizimlari soxta yuzlarni aniqlashda mukammal emas. Spoofing (soxta yuzlar) va boshqa manipulyatsiyalarni aniqlash uchun ilg‘or texnologiyalar kerak bo‘ladi, lekin ba’zi tizimlar hali ham soxta

yuzlarni aniqlashda muvaffaqiyatli bo‘lmaydi. Bu tizimlar uchun qo‘shimcha himoya qatlamlarini yaratish va yanada ilg‘or texnologiyalarni qo‘llash zarur.

Xulosa. Yuqoridagi masalalar yuzni identifikatsiyalash tizimlarini samarali va xavfsiz amalga oshirish uchun muhim qadamlar hisoblanadi. Bu tizimlar doimiy rivojlanib borishi va yangi texnologiyalar bilan takomillashishi kerak, shunda ular har qanday sharoitda yuqori aniqlik va ishonchlilikni ta’minlash imkoniyatiga ega bo‘ladi. Asosan yuzni identifikatsiyalash tizimlarining samarali va xavfsiz ishlashi uchun, ularni rivojlantirish jarayonida bir nechta muhim jihatlarni hisobga olish zarur.

Foydalanilgan adabiyotlar:

1. Брюхомицкий Ю.А. Биометрические технологии идентификации личности. – Ростов-на-Дону: ЮФУ, 2017.

2. https://lex.uz. O‘zbekiston Respublikasi qonunchilik ma’lumotlari milliy bazasi.

3. Zaynidinov X.N., Nurjanov F.R. Shaxs yuz tasviriga ko‘ra parametrlarini identifkatsiyalash usullarini ishlab chiqish .Toshkent -2019. - B. 251-254. 4.

4. Nurjanov F.R. Sun’iy intellekt texnologiyalari . O‘quv-qo‘llanma. – T.: “Ozbekiston Respublikasi Qurolli Kuchlari Akademiyasi nashriyoti”, 2024.

5. Грузман И.С. и др. Цифровая обработка изображений в информационных системах. – Новосибирск: НГТУ, 2002. – С. 352

6. Nurjanov F.R. Method and algorithm for identifying the parameters of the image face person // International Journal of Science and Research (IJSR). Volume 8 Issue 6, June 2019, India 08/06/2019. 7 page. Research Gate Impact Factor (2018):0.28/ SJIF(2018)7.426

HARBIY FAOLIYATDA ROBOT TIZIMLARINING RIVOJLANISH TENDENSIYALARI

Parpiyeva A.J.
O‘zbekiston Respublikasi Harbiy xavfsizlik va mudofaa universiteti
Quruqlikdagi qo‘shinlar instituti
Istiqbolli harbiy texnologiyalar kafedrasi Sun’iy intellekt va kiberxavfsizlik sikl katta o‘qituvchisi, t.f.f.d., dotsent

XX-XXI-asrlarda sodir bo‘lgan harbiy mojarolar tajribasini tahlil qilish shuni ko‘rsatadiki, tarmoqqa asoslangan urush konsepsiyasiga muvofiq olib boriladigan zamonaviy harbiy harakatlar quyidagi asosiy xususiyatlar bilan tavsiflanadi: axborot urushining roli ortib borishi, jangovarlikning noan’anaviy shakllaridan foydalanish, qurol-yarog‘larning aniqligi va selektivligini oshirish; modellashtirish. Ushbu xususiyatlardan kelib chiqqan holda, qurol ishlab chiqarishning umumiy texnologik tendensiyalari quyidagilardir: intellektuallashtirish, miniatyuralashtirish, energiya sarfini kamaytirish, ko‘p funksiyalilik, avtonomiya, og‘irlikni kamaytirish va yetkazib berish qulayligi [1].

Mahalliy va xalqaro ekspertlarning fikricha, robotlashtirilgan harbiy tizimlar yuqorida qayd etilgan hududlarning aksariyat qismini o‘zida mujassamlashtirgan holda kelajakdagi jangovar qurol va harbiy texnikaning eng istiqbolli turlaridan bo‘ladi. Ba’zi ekspertlar, shuningdek, robotlar va robototexnika texnologiyalarining keng joriy etilishi ilg‘or qurol va harbiy texnika tizimlarining operatsion usullari va texnik dizaynini o‘zgartiradi, ularning samaradorligini oshiradi va xodimlarning yo‘qotishlarini kamaytiradi [1].

2030 yilga kelib, uchuvchisiz transport vositalari ekipaj tarkibidagi jangovar transport vositalarining 52 foizini va jami jangovar transport vositalarining 30 foizini tashkil qilishi kutilmoqda. Amerikalik harbiy ekspertlarning hisob-kitoblariga ko‘ra, ushbu yangi turdagi bo‘linmalarning jangovar qobiliyati 2-2,5 baravar oshadi [1].

Harbiy robot tizimlarining rivojlanishi ilg‘or robot tizimlarining to‘liq majmuasini yaratish uchun zarur bo‘lgan asosiy texnologiyalarni

sezilarli darajada rivojlantirishni talab qiladi. Oddiy harbiy robotni funksional jihatdan o‘zaro bog‘langan elementlar to‘plami sifatida ko‘rsatish mumkin. Xususan [2]:

tayanch tashuvchi - bu har xil muhitda foydalanish uchun mo‘ljallangan har qanday konfiguratsiyaning shassisi yoki tanasi bo‘lishi mumkin;

olinadigan foydali yuk (maqsadli) modullar to‘plami ko‘rinishidagi maxsus qo‘shimchalar (o‘rnatilgan) uskunalar;

robotni ishlatishga tayyorlash va texnik ekspluatatsiya qilishda foydalaniladigan qo‘llab-quvvatlash va texnik xizmat ko‘rsatish uskunalari.

Ixtisoslashtirilgan uskunaning tarkibi robotning funksional maqsadiga qarab belgilanadi va quyidagilarni o‘z ichiga olishi mumkin:

- razvedka uskunalari;
- qurol;
- navigatsiya qurilmalari;
- maxsus texnologik uskunalar;
- telekommunikatsiya;
- dasturiy ta’minot va algoritmik yordamga ega ixtisoslashtirilgan kompyuterlar;
- elektron urush (EW) uskunalari;
- himoya vositalari.

Bundan tashqari, robototexnika qo‘llab-quvvatlash va texnik xizmat ko‘rsatishni talab qiladi, ya’ni kompleksga qo‘shimcha ravishda [2] kiradi:

- axborotni boshqarish, monitoring qilish va qayta ishlash uchun boshqaruv markazi;
- yetkazib berish, tashish va uchirish apparatlari;
- uskunalar, yonilg‘i quyish va zaryadlash uskunalari;
- maxsus o‘quv jihozlari;
- yo‘l-yo‘riqli hujjatlar to‘plami;
- ehtiyot qismlar to‘plami.

energiya;

- yangi materiallar va moddalarni yaratish va qo‘llash;

- geoaxborot va aniq global joylashuvni aniqlash;
- ilg‘or sensor tizimlari va ularning elementlarini yaratish;
- optik va optoelektron vositalarni yaratish.

Bunday texnologiyalarga ega bo‘lish UUAlar, yerdagi robotlashtirilgan transport vositalari va avtonom dengiz transport vositalarining zarur avtonomligi va razvedka darajasini ta’minlashda muvaffaqiyat kalitidir. Oksford universiteti xodimlari tomonidan taklif qilingan vizual tasnifdan foydalanib, robotlarning "qobiliyatlarini" to‘rt avlodga tizimlashtirish mumkin [3]:

- "kaltakesak darajasi" - birinchi avlod universal robotlari protsessorlarining ishlash tezligiga mos keladi, bu soniyada 3000 dan 1 million ko‘rsatma (MIPS) oralig‘ida. Bunday robotlarning asosiy maqsadi oldindan dasturlashtirilgan faqat bitta vazifani qabul qilish va bajarishdir;
- "sichqoncha darajasi" - moslashuv xatti-harakatlarini, ya’ni vazifalarni bajarish jarayonida bevosita o‘rganishni amalga oshira oladigan ikkinchi avlod robotlari;
- "maymun darajasi" - uchinchi avlod robotlari, ular 10 million MIPS protsessorlari asosida qurilgan. Bunday robotlarning o‘ziga xosligi shundaki, topshiriq va mashg‘ulotni qabul qilish uchun faqat namoyish yoki tushuntirish kerak;
- "inson darajasi" - robotlarning to‘rtinchi avlodi, ular o‘ylash va mustaqil qaror qabul qilish qobiliyatiga ega bo‘lishi kerak.

Ish jangovar robotlarning shaxsga (operatorga) bog‘liqligi yoki aniqrog‘i mustaqillik darajasiga ko‘ra tasnifini taqdim etadi[4]:

- 1-avlod robotlari - bular dasturiy ta’minot va masofadan boshqarish pulti bilan faqat uyushgan muhitda ishlashga qodir qurilmalar;

2-avlod robotlari - moslashuvchan, sintetik "sezgi" organlarga ega va ilgari noma’lum sharoitlarda ishlashga qodir va atrof-muhit o‘zgarishlariga moslashadi;

- 3-avlod robotlari - aqlli, sun’iy intellekt elementlariga ega boshqaruv tizimiga ega (hozircha faqat laboratoriya modellari ko‘rinishida yaratilgan). G‘arb mutaxassislari robotlarni uch toifaga ajratadilar [4]:

human-in-the-loop - bu toifa nishonlarni mustaqil ravishda aniqlash va tanlashga qodir bo‘lgan uchuvchisiz uchish apparatlarini o‘z ichiga oladi, lekin ularni yo‘q qilish to‘g‘risidagi qarorni faqat inson operatori qabul qiladi;

human-on-the-loop - bu toifaga maqsadlarni mustaqil ravishda aniqlash va tanlash, shuningdek ularni yo‘q qilish bo‘yicha qarorlar qabul qilish qobiliyatiga ega tizimlar kiradi, ammo kuzatuvchi sifatida ishlaydigan inson operatori, istalgan vaqtda aralashib, ushbu qarorni tuzatishi yoki blokirovka qilishi mumkin;

human-out-of-the-loop - bu toifaga inson aralashuvisiz nishonlarni mustaqil ravishda aniqlash, tanlash va yo‘q qilishga qodir robotlar kiradi. Bugungi kunda eng keng tarqalgan birinchi avlod jangovar robotlari (boshqariladigan qurilmalar) va ikkinchi avlod tizimlari (yarim avtonom qurilmalar) tez takomillashtirilmoqda. Uchinchi avlod jangovar robotlaridan (avtonom qurilmalar) foydalanishga o‘tish uchun mutaxassislar sun’iy intellektga ega bo‘lgan o‘z-o‘zini o‘rganish tizimini ishlab chiqmoqdalar, u navigatsiya, obyektlarni vizual aniqlash, sun’iy intellekt, qurol-yarog‘lar, mustaqil quvvat manbalari, odamlarning jangovar tezligini sezilarli darajada kamaytirish va hokazolar sohasidagi eng ilg‘or texnologiyalarning imkoniyatlarini birlashtiradi. atrof-muhitni (har qanday hududda) tan olish, shuningdek, vaziyatning o‘zgarishiga javob berish tezligi va aniqligida [4, 5]. Rivojlangan mamlakatlarda mikroelektronikaning hozirgi holati allaqachon robot vositalaridan insonning minimal ishtiroki bilan to‘liq vazifalarni bajarishga imkon beradi. Biroq, yakuniy maqsad - qaror qabul qilish tezligi, xotira hajmi va adekvat harakatlar algoritmi nuqtai nazaridan bir xil imkoniyatlarga ega bo‘lgan odamni uning virtual nusxasi bilan to‘liq almashtirishdir [3].

Sun’iy neyron tarmoqlarga asoslangan tizimlar allaqachon alohida obyektlarni tanib olishni o‘rgangan. Mutaxassislarning prognozlariga ko‘ra, to‘liq avtonom jangovar tizimlar 20-30 yil ichida yoki undan ham tezroq paydo bo‘lishi mumkin. Ayrim ekspertlarning fikricha, har qanday jangovar zonada: quruqlikda, dengizda, suv ostida yoki aerokosmik muhitda askarlarni almashtira oladigan android robotlar yaratiladi. Biroq,

avtonom jangovar robotlar, ularning sun'iy intellekti qanchalik murakkab bo'lishidan qat'iy nazar, qarshisidagilarning xatti-harakatlarini odamlar kabi tahlil qila olmaydi va shuning uchun jangovar bo'lmaganlar uchun xavf tug'diradi, degan xavotirlar bildirildi [4]. Amerikalik mutaxassislarning fikricha, agar biz inson imkoniyatlarini kompyuter bilan solishtirishga harakat qilsak, bunday kompyuter soniyada taxminan 100 trillion operatsiyani bajarishi va yetarlicha operativ xotiraga ega bo'lishi kerak bo'ladi. Hozirgi vaqtda mikroprotsessor texnologiyasining imkoniyatlari 10 barobar past. Shuning uchun ishlab chiqilayotgan mikroprotsessorlarning tezligini oshirish va miniatyuralashtirish asosiy ahamiyatga ega. Bugungi kunda silikon asosidagi protsessorlarning minimal o'lchamlari ultrabinafsha litografiyaga asoslangan ishlab chiqarish texnologiyalari bilan cheklangan. AQSH Mudofaa vazirining hisobotiga ko'ra, 0,1 mikronlik bu cheklovchi o'lchamlarga 2015-2020 yillarda erishilmoqda. Biroq, optik, biokimyoviy va kvant texnologiyalari, shu jumladan kalitlar va molekulyar protsessorlarni yaratish ultrabinafsha litografiyaga muqobil bo'lishi mumkin. Mutaxassislarning fikricha, kvant shovqin usullari yordamida ishlab chiqilgan protsessorlar hisoblash tezligini minglab marta, nanotexnologiyalar esa millionlab marta oshirishi mumkin. Bundan tashqari, robot tizimlarini ishlab chiqish, asosan, uchuvchisiz va robotli tizimlardan muvaffaqiyatli foydalanish uchun muhim elementlar bo'lgan ilg'or kommunikatsiyalarga jiddiy e'tibor berishni talab qiladi [3].

Hisoblash va aloqa tizimlarini rivojlantirish zarurati bilan bir qatorda, robototexnikani rivojlantirish [3] yaratish uchun eng zamonaviy texnologiyalardan foydalanishni talab qiladi:

- UUA jismlari va boshqa robotlashtirilgan transport vositalari uchun yaxshilangan yashirin xarakteristikaga ega o'ta yengil, o'ta kuchli, elastik materiallarni yaratishda foydalaniladigan transgen biopolimerlar;

- UUA elektron tizimlarida ishlatiladigan uglerod nanotubalari. Bundan tashqari, elektr o'tkazuvchan polimerlarning nanozarralaridan tayyorlangan qoplamalar robot va boshqa qurolli urush vositalari uchun dinamik kamuflyaj tizimini ishlab chiqish imkonini beradi;

- mikroelektronik va mikromexanik elementlarni birlashtirgan mikroelektromexanik tizimlar;

- robotlashtirilgan transport vositalarining shovqin darajasini kamaytirishga imkon beradigan vodorodli dvigatellar;

- tashqi ta'sirlar ta'sirida muayyan funksiyani bajaradigan "aqlli materiallar". Masalan, uchuvchisiz uchish apparatlari uchun DARPA tadqiqot va ishlanma dasturlari agentligi uchish rejimiga qarab o'zgarib turuvchi qanot konsepsiyasini ishlab chiqish bo'yicha tajribalar o'tkazmoqda, bu esa UUAlarning manevr qobiliyatini sezilarli darajada oshiradi; - magnit nanozarrachalar, bu ma'lumotlarni saqlash qurilmalari rivojlanishida yutuq bo'lishi mumkin, robot tizimlarining xotira hajmini sezilarli darajada kengaytiradi. 10-20 nm o'lchamdagi ixtisoslashtirilgan nanozarrachalardan foydalanish orqali erishilgan texnologiya salohiyati kvadrat santimetr uchun 400 Gbitni tashkil qiladi.

Ko'plab loyihalar va tadqiqotlarni ishlab chiqishning tubdan yangi tarmoqlarda rivojlanishining hozirgi iqtisodiy noqulayligiga qaramay, yetakchi xorijiy davlatlarning harbiy rahbariyati nafaqat shaxsiy tarkibni saqlab qolish va barcha jangovar tartibsiz tahdidlar, shuningdek, zamonaviy va kelajakdagi operatsiyalarni samarali amalga oshirish va qo'llab-quvvatlash vazifalarini olib borishni ta'minlashga umid qilib, istiqbolli robot va qurolli jang vositalarini rivojlantirish sohasida maqsadli, uzoq muddatli siyosat olib bormoqda. [3].

AQSH Qurolli Kuchlarining robotlashtirish rejalari robototexnika parametrlari bo'yicha quyidagi ish yo'nalishlarini nazarda tutadi:

- elektr ta'minoti;
- qiyin sharoitlarda ishlash qobiliyati;
- signallarni chiqarish usullari;
- aloqa protokoli tuzilmalari;
- obyektni tavsiflash tizimlari;
- insonni tan olish;
- inson va robot aloqasi;
- navigatsiya;
- to'siqlardan qochish;

- moslama va mexanizmlar drayvlari;
- manipulyatorlarning samaradorligini oshirish.

To‘liq avtonom harbiy robot tizimlarini yaratish yo‘lidagi eng murakkab va munozarali masala - bu odamni o‘ldirish huquqini mashinaga o‘tkazishning qonuniyligi va ma’naviy maqsadga muvofiqligi. Biroq, bu axloqiy masala, inson muammosi, robot muammosi emas, texnologiya masalasi emas. Ushbu muammoning yechimlaridan biri insondan mustaqil ravishda to‘liq avtonom harakat qila oladigan sun’iy intellektga ega jangovar robot arsenalidagi halokatli bo‘lmagan qurol bo‘lishi mumkin [6]. Bundan tashqari, robototexnikaning rivojlanishi inson va mashina o‘zaro ta’sirining bir qator yangi muammolarini dolzarb qiladi. Masalan, hozirda AQSH harbiylari “odamlar va robotlar o‘rtasida hamkorlik aloqalarini o‘rnatish, ularga sinergik jamoalarda ishlash imkonini berish”ga qaratilgan avtonom robot tizimlarini harbiy maqsadlarda qo‘llash konsepsiyalarini ishlab chiqmoqda. Ushbu konsepsiyalar 150 askar va ofitserlar taxminan 2000 robotdan iborat bo‘lgan jangovar bo‘linmalarni shakllantirish variantlarini ishlab chiqishni o‘z ichiga oladi. Shunga ko‘ra, bu yana bir muammoni keltirib chiqaradi: askarlar va robotlarning bunday "sinergetik jamoasi" bilan qanday va qanday kurashish kerak [6].

Robotlashtirish nafaqat harbiy qismlarning tashkiliy tuzilishi va taktikasini tubdan o‘zgartiribgina qolmay, balki bir qator muhim ijtimoiy-psixologik jihatlarga ham ta’sir ko‘rsatadi. Xususan, robotlashtirish natijasida yuzaga keladigan muammolar harbiy qismlarda ijtimoiy rollarni sezilarli darajada qayta taqsimlashni o‘z ichiga oladi. Ijtimoiy munosabatlarning yangi turi bilan bog‘liq muammolar allaqachon paydo bo‘lmoqda: "inson" va "sun’iy intellektga ega avtonom jangovar robot". Robotlashtirish "tirik" harbiy xizmatchilarni inson va inson o‘rtasidagi kurash sifatidagi psixologik tushunarli urush holatidan inson va odamlarni o‘ldirishga qaratilgan "aqlli mashina" o‘rtasidagi kurashga o‘tkazadi. Ushbu yangi sharoitda nafaqat robotlar va odamlarning jang maydonida qo‘shma harakatlarini tashkil etish, balki bu vaqtdan tashqari odamlar va robotlarni birgalikda joylashtirish va birgalikda jangovar tayyorgarlik muammosi ham alohida yechimni talab qiladi [7].

Yana bir murakkab masala, xususan, inson operatorlari va robot komandirlari o‘rtasidagi aloqa. Bu muammo robotlarning odamlar bilan hamkorlikdagi harakatlariga yetarlicha moslasha olmagani tufayli yanada kuchayishi mumkin. Shubhasiz, bu nafaqat ishqalanishga, balki ochiq qarama-qarshilikka ham olib kelishi mumkin [7]. Jang maydonida uzoq vaqt davomida jangovar robotlar bilan ham ittifoqchi, ham dushman sifatida o‘zaro aloqada bo‘lgan inson askarlarining ijtimoiy-psixologik moslashuvi ham kam qiyin bo‘lishi mumkin. Misol uchun, Afg‘oniston va Iroqdagi AQSH qo‘shinlari guruhlariga robotlarni faol joylashtirish paytida, askarlar o‘zlarining "homiylik" robotlariga qo‘shilib, ularni o‘rtoqlar yoki maskot sifatida ko‘rishlari haqida ko‘plab holatlar qayd etilgan. Harbiy xizmatchilar va ilg‘or sun’iy intellektga ega avtonom robotlar o‘rtasidagi kelajakdagi faol o‘zaro ta’sir bu muammoni yanada kuchaytirishi mumkin [7]. Rivojlangan mamlakatlar qurolli kuchlarini rivojlantirishning asosiy ustuvor yo‘nalishlaridan biri havo, quruqlik va dengizda foydalanish uchun jangovar robotlar va robot tizimlarini yaratishdir. Oxirgi 20 yil ichida AQSH, Buyuk Britaniya, Fransiya, Germaniya, Xitoy va Isroil kabi davlatlar jangovar robotlar va robot tizimlari uchun harbiy ilmiy-tadqiqot ishlarini moliyalashtirishni 20-30 barobarga oshirdi. Qo‘shma Shtatlar shubhasiz dunyo yetakchisi va bu sohadagi yirik harbiy dasturlarning tashabbuskori hisoblanadi (uning tadqiqot ulushi global jami 65-75% ni tashkil qiladi). Bugungi kunga qadar Qo‘shma Shtatlar harbiy robot tizimlarini ishlab chiqishda eng aniq natijalarga erishdi. Qo‘shma Shtatlarda harbiy robototexnikaning rivojlanishiga uzoq muddatli rejalashtirish va uning ushbu sohadagi ishining intensivligi yordam beradi. 1988 yilda AQSH Mudofaa vazirligi maxsus dastur doirasida jangovar robotlarni yaratishga qaratilgan keng ko‘lamli tadqiqotlarni boshladi. Keyingi 20 yil ichida mustaqil ravishda yoki masofaviy operatorning buyrug‘i bilan harbiy operatsiyalarni amalga oshirishga qodir bo‘lgan 200 dan ortiq prototipli jangovar transport vositalari ishlab chiqildi. Aksariyat robotlar patrullik, razvedka, minalardan tozalash, yuklarni yetkazib berish va boshqa turli harbiy

maqsadlar uchun mo‘ljallangan. Ba’zi modellar dushmanga o‘t ochish to‘g‘risida mustaqil ravishda qaror qabul qilishga qodir [8, 9, 10].

Harbiy robototexnika uchuvchisiz uchish apparatlarini (UUA) rivojlantirish rejalari va dasturlarida AQSH Mudofaa vazirligi ularga asoslangan texnik vositalar va robot tizimlarining quyidagi toifalarini belgilaydi [10]:

- uchuvchisiz uchish apparatlari (UUA) - Unmanned Air Vehicles (UAV);

- harakatlanuvchi yer robotlari (MGR) - Unmanned Ground Vehicles (UGV);

- uchuvchisiz yer usti transport vositalari Unmanned Surface Vehicles (USV);

2007 yil dekabr oyida 2007-2032 yillarga mo‘ljallangan uchuvchisiz tizimlar yo‘l xaritasi tasdiqlandi, unda quruqlik, dengiz va havoda robot tizimlarini yaratishning maqsad va yo‘nalishlari belgilandi [1]. Qo‘shma Shtatlarda Qurolli Kuchlarni robotlashtirish davlat siyosati darajasiga ko‘tarildi. Amerikaliklar bitta qurol tizimini yangi, ilg‘orroq bilan almashtirish amaliyotidan asta-sekin voz kechib, o‘nlab an’anaviy qurol tizimlarini almashtiradigan yoki to‘ldiradigan robot tizimlarining butun majmualarini ishlab chiqishga o‘tmoqchi [9]. Ayni paytda AQSH Qurolli Kuchlari oxirgi harbiy mojarolarda jangovar harakatlarda harbiy robotlardan keng foydalanmoqda. Shunday qilib, Iroqda turli maqsadlar uchun 32 turdagi 365 ta robot ishlatilgan. Xususan, minalardan tozalash uchun masofadan boshqariladigan muhandislik avtomashinalaridan foydalanish qo‘shinlarning oldinga siljish tezligini ikki-uch barobar oshirish va shaxsiy yo‘qotishlarni sezilarli darajada kamaytirish imkonini berdi. Bundan tashqari, Afg‘oniston va Iroqdagi harbiy amaliyotlarda taktik razvedka uchun uchuvchisiz uchuvchi samolyotlardan foydalanish operatsiyaning jangovar bosqichi uchun zarur bo‘lgan vaqtni keskin qisqartirish imkonini berdi [1]. Yaqin vaqtgacha birlamchi robot-texnik vositalar FCS (Future Combat System)dasturi doirasida ishlab chiqilgan bo‘lib, u AQSH quruqlikdagi kuchlarining jihozlari va qurollarini to‘liq

miqyosda modernizatsiya qilish dasturining bir qismi bo‘lgan. Dastur [3] ni ishlab chiqishni o‘z ichiga oladi:

- razvedka signalizatsiya qurilmalari;
- avtonom raketa va razvedka-zarba tizimlari;
- uchuvchisiz uchish apparatlari;
- razvedka-patrul, zarba-hujum, portativ masofadan boshqariladigan, shuningdek, masofadan boshqariladigan yengil muhandislik va logistika vositalari.

Ushbu qurilmalarning barchasi bitta jangovar qo‘mondonlik, boshqaruv, aloqa, razvedka va kuzatuv tizimiga birlashtirilishi kerak edi, buning natijasida alohida elementlar real vaqt rejimida ma’lumot almashishi mumkin edi [9]. Biroq, qurolli kuchlarni robotlashtirish bir qator jiddiy cheklovlarga ega, hatto eng boy va rivojlangan davlatlar ham hisobga olishga majbur. Misol uchun, 2009 yilda Qo‘shma Shtatlar moliyaviy cheklovlar va texnologik muammolar tufayli 2003 yilda boshlangan FCC dasturini rejalashtirilgan amalga oshirishni to‘xtatdi. 2003 yil may oyidan 2006 yil dekabrigacha FCC xaridlari dasturining qiymati 91,4 milliard dollardan 160,9 milliard dollargacha oshdi. Xuddi shu davrda rejalashtirilgan 44 ta texnologiyadan faqat 2 tasi amalga oshirildi. 2006 yilda dasturning umumiy qiymati 203,3-233,9 milliard dollarga baholangan bo‘lsa, keyinchalik u deyarli 340 milliard dollarga etdi, shundan 125 milliard dollari ilmiy-tadqiqot ishlariga yo‘naltirilishi rejalashtirilgan edi. Oxir-oqibat, 18 milliard dollardan ortiq mablag‘ sarflanganidan so‘ng, FCC dasturi to‘xtatildi, garchi rejalarga ko‘ra, 2015 yilga kelib AQSH armiyasining jangovar kuchining uchdan bir qismi robot tizimlaridan iborat bo‘lishi kerak edi [11, 12]. Robot texnikasining moliyaviy qiyinchiliklariga qo‘shimcha ravishda, elektron urush va axborot qurollarining katta arsenaliga ega bo‘lgan dushmanga qarshi kurashda robot yoki qo‘shma inson-robot birliklarining samaradorligi noaniqligicha qolmoqda [8]. Shunga qaramay, AQSH Qurolli Kuchlarini robotlashtirish jarayoni davom etmoqda. FCC dasturi yopilgan bo‘lsa-da, innovatsion qurol tizimlarini, shu jumladan qo‘mondonlik va boshqaruv tizimlari va aloqalarni, shuningdek,

robotlashtirilgan va uchuvchisiz transport vositalarining ko‘p qismini ishlab chiqish Brigada jangovar guruhini modernizatsiya qilishning yangi dasturi doirasida saqlanib qoldi. 2010 yil oxirida AQSH Mudofaa vazirligi "2011-2036 yillarga mo‘ljallangan avtonom tizimlarni rivojlantirish va integratsiya rejasi"ni e’lon qildi. Ushbu hujjatga ko‘ra, havo, quruqlik va suv osti avtonom tizimlarining soni sezilarli darajada ko‘paytiriladi, ishlab chiquvchilarga dastlab ushbu qurilmalarni "nazorat qilinadigan avtonomiya" (ya’ni, ularning harakatlari shaxs tomonidan boshqariladi) va oxir-oqibat "to‘liq avtonomiya" bilan ta’minlash vazifasi yuklanadi. Shu bilan birga, AQSH Harbiy-havo kuchlari mutaxassislari istiqbolli sun’iy intellekt jangovar harakatlar paytida qonunni buzmaydigan mustaqil qarorlar qabul qilish imkoniyatiga ega bo‘lishiga ishonishadi [11, 12]. 2016 yilga kelib, AQSH Qurolli Kuchlari uchun 20 ga yaqin masofadan boshqariladigan quruqlikdagi transport vositalari allaqachon ishlab chiqilgan. Shu bilan birga, havo kuchlari va dengiz floti taxminan bir xil miqdordagi havo, yer usti va suv osti tizimlari ustida ishlamoqda [11, 12]

Piyoda va maxsus kuchlar bo‘linmalarini odamlar va robotlar bilan birgalikda tayyorlash g‘oyasi muhokama qilinmoqda. Yana bir g‘oya - isbotlangan va yangi texnologiyalarni birlashtirish. Masalan, transport samolyotlari va kemalaridan havo va dengizdagi uchuvchisiz transport vositalari guruhlari uchun "ona platforma" sifatida foydalanish ulardan foydalanish taktikasini o‘zgartiradi va ularning imkoniyatlarini oshiradi [11, 12]. Shunday qilib, AQSH misolida keltirilgan Qurolli Kuchlarni robotlashtirish tajribasi shuni ko‘rsatdiki, harbiy robot tizimlarini ishlab chiqish o‘ta murakkab ilmiy-texnik vazifa bo‘lib, tizimli yondashuv va keng ko‘lamli moliyalashtirishni talab qiladi. FCS tizimini yarata olmagan amerikaliklar aralash tizimlarni – “inson + robot” yoki “odam tomonidan boshqariladigan robot” ni tanladilar. Robotlarga odamlardan ko‘ra samaraliroq bajara oladigan yoki inson hayoti uchun xavf maqbul chegaralardan oshib ketadigan vazifalar beriladi. Yana bir maqsad qurol va harbiy texnika narxini pasaytirishdir.

2003 yilda Iroqqa bostirib kirish paytida AQSH Qurolli Kuchlarida atigi bir necha o‘nlab uchuvchisiz uchuvchi samolyotlar bo‘lgan, birorta

ham yer roboti yo‘q edi. 2009 yilda ular allaqachon 5300 ta, 2013 yilda esa 7000 dan ortiq UUAga ega edi. Iroqdagi qo‘zg‘olonchilar tomonidan qo‘lbola portlovchi qurilmalarning ommaviy qo‘llanilishi amerikaliklar tomonidan yerdagi robotlarni yaratishning keskin tezlashishiga olib keldi. 2009 yilda AQSH Qurolli Kuchlarida 12000 dan ortiq robotlashtirilgan yer usti vositalari mavjud edi [4].

AQSH tajribasi shuni ko‘rsatadiki, harbiy va fuqarolik robotlarini ishlab chiqishda sensorli qurilmalar, mashinani ko‘rish, nutqni aniqlash, mexanik manipulyatorlar, matematik dasturiy ta’minot va boshqalarning ilg‘or yutuqlariga asoslangan umumiy quyi tizimlar va elementlardan foydalaniladi. Bu avtomatlashtirilgan qurol tizimlarini, avtomatlashtirilgan ishlab chiqarish tizimlarini, shuningdek, bir xil ilmiy, texnik, sanoat bazasida iste’mol yoki tijorat tovarlarini yaratishga imkon beradi. Bunday yondashuv, bir tomondan, fuqarolik ilovalarida robototexnika bo‘yicha yangi harbiy ishlanmalarni amalga oshirishni ta’minlaydi, boshqa tomondan, harbiy mahsulotlar ishlab chiqarish ixtisoslashgan harbiy sanoatni talab qilmaydi. Xalqaro mudofaa tizimlari va qurol-yarog‘ ko‘rgazmalarida taqdim etilgan robot tizimlarining tahlili bu sohada fuqarolik va harbiy sektorlar deyarli birlashganligini aniq ko‘rsatmoqda [9]. Shuni inobatga olsak, quyidagi faktlar qiziq. Yaponiya fuqarolik robototexnika sohasida dunyoda yetakchi hisoblanadi. Sanoat robotlarining umumiy soni bo‘yicha (taxminan 350 ming dona) Yaponiya Germaniya va AQShdan ancha oldinda. Shuningdek, u avtomobil sanoatida ish bilan band bo‘lgan 10000 kishiga sanoat robotlari soni bo‘yicha ham yetakchi hisoblanadi, bu dunyodagi jami robotlar savdosining 40% dan ortig‘ini tashkil etadi. 2012 yilda yetakchilar uchun bu ko‘rsatkich: Yaponiya – 1562 birlik; Fransiya – 1137; Germaniya – 1133 nafar; AQSH - 1091. Xitoyda avtomobilsozlikda har 10000 xodimga 213 robot to‘g‘ri keladi. Shu bilan birga, barcha sohalarda band bo‘lgan har 10 000 kishiga sanoat robotlari soni bo‘yicha Janubiy Koreya yetakchi bo‘ldi, undan keyin Yaponiya – 332 va Germaniya – 273. 2012 yil oxirida sanoat robotlarining o‘rtacha global zichligi 58 birlikni tashkil etdi. Shu bilan birga, Yevropada bu ko‘rsatkich 80, Amerikada - 68, Osiyoda – 47

birlikni tashkil etdi. Rossiyada har 10000 ishchiga 2 ta sanoat roboti to‘g‘ri keldi. 2012 yilda AQShda 22411 ta sanoat robotlari, Rossiyada esa 307 ta sanoat robotlari sotilgan [6]. Xorijiy matbuot xabarlariga ko‘ra, 40 ga yaqin davlat, jumladan, AQSH, Rossiya, Buyuk Britaniya, Fransiya, Xitoy, Isroil va Janubiy Koreyada inson aralashuvisiz jang qila oladigan robotlar yaratilmoqda. Qo‘shma loyihalar asosida qator dasturlar amalga oshirilmoqda. Taxminlarga ko‘ra, bunday qurollar bozori 20 milliard AQSH dollariga yetishi mumkin. 2005 yildan 2012 yilgacha Isroil 4,6 milliard AQSH dollariga UUA sotgan. Harbiy robotlarni yaratish bilan jami 80 dan ortiq davlat mutaxassislari shug‘ullanadilar [4].

Ushbu loyihalarni amalga oshirishning asosiy tendensiyasi mavjud aktivlarni avtomatlashtirilgan ko‘rish tizimlari, avtomatlashtirilgan boshqaruv tizimlari, aloqa kanallari (radio va optik tolali), modulli prinsip asosida qurilgan harakatni boshqarish tizimlari bilan qayta jihozlashdir. Ushbu yondashuv ixtisoslashtirilgan bo‘linmalarda robot tizimlarini tezkorlik bilan amalga oshirish imkonini beradi.

Foydalanilgan adabiyotlar:

1. Буренок В. М., Ивлев А. А., Корчак В. Й. Развитие военних технологий ХХИ века: проблеми планирование, реализатсиЙ. – Твер: Издателство ООО «КУПОЛ», 2009. – 624 с.

2. Попов С. А. Робот стреляет первим // Военное обозрение [Электронний ресурс]. 28.02.2016. – УРЛ: ҳттпс://топwap.ру/91499-робот-стреляэтпервйм.ҳтмл (дата доступа 29.06.2016).

3. Кондратев А. Е. Боевие роботи США – под водой, в небесах и на суше // Независимое военное обозрение [Электронний ресурс]. 14.05.2010. – УРЛ: ҳттп://нво.нг.ру/армамент/2010-05-14/8_роботс.ҳтмл (дата доступа 23.06.2016).

4. Сизов В. Й. Какие боевие роботи нужни России? // Военное обозрение [Электронний ресурс]. 07.03.2016. – УРЛ: ҳттпс://топwap.ру/91962- какиэ-боэве-роботй-нузҳнй-россии.ҳтмл (дата доступа 29.06.2016).

5. Макаренко С. И. Интеллектуалние информационние системи: учебное пособие. – Ставропол: СФ МГГУ им. М. А. Шолохова, 2009. – 206 с.

6. Попов И. М. Военние конфликти: взгляд за горизонт // Независимое военное обозрение [Электронний ресурс]. 12.04.2013. УРЛ: ҳттп://нво.нг.ру/сонсэптс/2013-04-12/1_сонфлистс.ҳтмл (дата доступа 28.01.2016).

7. Постников А. Н., Хамзатов М. М. Сухопутние войска будушего // Независимое военное обозрение [Электронний ресурс]. 11.09.2015. – УРЛ: ҳттп://нво.нг.ру/сонсэптс/2015-09-11/4_футуре.ҳтмл (дата доступа 23.02.2016).

8. Бобков Й. Й., Тютюнников Н. Н. Консептуалние основи построения АСУ Сухопутними войсками ВС РФ: монографиЙ. – М.: Издателство «Палеотип», 2014. – 92 с.

9. Соколов Й. И. Риски високих технологий. – М.: ФГУ ВНИИ ГОЧС (ФС), 2009. – 312 с.

10. Сиденко К. С., Илларионов Г. Й. Применение автономних подводних роботов в войнах будушего // Арсенал. Военно-промишленное обозрение. 2008. № 2. С. 86-93.

11. Боевие роботи в будуших войнах: виводи экспертов (Част 2) // Зарубежное военное обозрение [Электронний ресурс]. 04.03.2016. – УРЛ: ҳттп://нво.нг.ру/армамент/2016-03-04/5_роботс2.ҳтмл (дата доступа 29.06.2016).

МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СЛУЖБЫ СВЯЗИ СИЛОВЫХ ВЕДОМСТВ

Пен А.Ю.
Университет общественной безопасности
Республики Узбекистан, д.ф.т.н. (PhD), доцент

Конечная цель управления безопасностью конкретной системы - объективная оценка оперативной обстановки и принятие адекватного решения по поставленной задаче.

На фоне ускоренной смены проблемных ситуаций, череды террористических актов, природно-климатических кризисов и естественно, участия личного состава силовых структур в оперативных действиях по ликвидации последствий катастроф, представляется актуальным концептуальное рассмотрение вопросов материально-технического обеспечения подразделений силовых ведомств. Решение специальных задач, возложенных на силовые структуры, независимо от их ведомственной принадлежности, наряду с другими, тесно связано с организацией и эффективностью функционирования приданной группы связи [1]. Успешное выполнение упомянутых задач однозначно определяется уровнем и рациональной номенклатурой используемых технических средств связи (ТСС) [2,3]. В работе освещается предложенный подход формирования состава, а также выбора структуры и ТСС, а иначе рациональной её номенклатуры, для группы обеспечения связи силового ведомства.

Подход отличают возможности, представляемые аппаратом матричной алгебры: анализа ТСС с использованием различных функций от матрицы (расстояния, коэффициент корреляции между матрицами и т.д.); учёта всех определяющих характеристик ТСС; нахождения значимости показателей (столбец, строка) ТСС - характеризующих его в некотором определённом отношении.

С введением понятия, характеризующего ТСС матрицей его определяющих характеристик, появилась возможность решения

задачи уменьшения номенклатуры ТСС путём объединения их в классы подобных между собой объектов. Предложен критерий, базирующийся на понятии расстояния между матрицами (как мера близости между ними), по которому устанавливается их подобие.

Решение задачи определения рациональной номенклатуры ТСС сводилось к выявлению представителя из класса эквивалентных средств. В результате получены выражения для нахождения «типичного» ТСС при наличии и отсутствии базисного средства, а также минимальной номенклатуры рассматриваемого класса ТСС.

Предложенный подход был апробирован в задаче определения номенклатуры ТСС, применяемых в задачах обеспечения связи отдельного подразделения правоохранительной структуры Республики.

При ограниченности отечественных ТСС, сравнивались самостоятельно их ряды, производимые в странах дальнего и ближнего зарубежья. Результатами анализа выявлено, что для решения насущных задач силового ведомства группа связи должна оснащаться определенным «ассортиментом» технических средств. Причем, результаты анализа также выявили парадоксальное противоречие - в условиях всемерного расширения использования цифровых систем связи их пожароопасность, учитывая экстремальный характер эксплуатации, существенно выше, чем аналоговых [4].

Использованной литературы:

1. *Мавлянкариев Б.А. и Насыров А.А. Хатамов Б.Б. Пен А.Ю.* Проблемы безопасности при организации связи подразделений правоохранительных структур / Тр. 8-ой межд.НТК «Новое в безопасности жизнедеятельности». - Алматы: 2006. -с.480-484.

2. *Мавлянкариев Б.А. и Насыров А.А. Хатамов Б.Б. Пен А.Ю.*Управление безопасностью объекта: стратегия управления, модель / Тр. 8-ой межд.НТК «Новое в безопасности жизнедеятельности». - Алматы: 2006. -с.485-488

3. *Мавлянкариев Б.А.* Модель управления качества связи с учетом риска помех / Мат.15 межд.НТК «Системы безопасности» СБ-

2006, M.: 2006.- c. 107-111.

4. *Мавлянкариев Б.А.* Многофункциональные датчики длявысоко рисковых пожаро и экологические опасных систем. // Материалы 8-ой международной конференции «Системыбезопасности СБ-99». М.:1999. с.58-59.

QUROLLI KUCHLAR TIZIMIDA SUN'IY INTELLEKT TEXNOLOGIYALARNI QO'LLASHNING ZAMONAVIY YECHIMLARI

Nigmatov Z.Z.

O'zbekiston Respublikasi Harbiy xavfsizlik va mudofaa universitetining Quruqlikdagi qo'shinlar instituti, Istiqbolli harbiy texnologiyalar kafedrasi Sun'iy intellekt va kiberxavfsizlik siklli dotsenti, dotsent, t.f.f.d (PhD)

So'nggi yillarda sun'iy intellekt (SI) texnologiyalari global miqyosda turli sohalarda innovatsion yechim sifatida jadal rivojlanmoqda. Jumladan, mudofaa va xavfsizlik tizimlarida ushbu texnologiyalarni qo'llash dolzarb ahamiyat kasb etmoqda. AQSh, Xitoy, Rossiya kabi yirik davlatlar SI asosidagi yechimlarni harbiy boshqaruv, razvedka, kiberxavfsizlik va jangovar operatsiyalarni qo'llab-quvvatlashda keng qo'llashmoqda. Bu jarayonlar xalqaro xavfsizlik muvozanatiga sezilarli ta'sir ko'rsatmoqda.

Qurolli kuchlar tizimida SI texnologiyalarini tatbiq etishning asosiy sabablari quyidagilardan iborat:

birinchidan, zamonaviy harbiy tahdidlar tobora murakkablashib bormoqda. An'anaviy qurollanish uslublari raqamli xavfsizlik, kiberhujumlar, dronlar va avtonom tizimlar kabi yangi xavflar fonida yetarli bo'lmay qolmoqda.

ikkinchidan, harbiy qarorlar qabul qilish jarayonida tezkorlik va aniqlik talab etiladi. SI algoritmlari katta hajmdagi ma'lumotlarni qisqa vaqt ichida qayta ishlash imkonini berib, qo'mondonlik tizimining samaradorligini oshiradi.

uchinchidan, inson resurslarini tejash va jangovar sharoitlarda xavfsizlikni ta'minlash SI qo'llashining muhim ustunligidir.

Hozirgi davrda sun’iy intellekt asosida ishlab chiqilgan yechimlar quyidagi yo‘nalishlarda qo‘llanilmoqda:

- razvedka va kuzatuv tizimlarida sun’iy yo‘ldoshlar va dronlar orqali to‘plangan ma’lumotlarni tahlil qilish;
- kiberxavfsizlik sohasida tarmoq hujumlarini oldindan aniqlash va neytrallashtirish;
- jangovar boshqaruv tizimlari uchun qaror qabul qilishda yordam beruvchi intellektual dasturlar;
- logistika va ta’minotda harbiy resurslarni samarali taqsimlash hamda transport tizimlarini optimallashtirish.

O‘zbekiston Respublikasi ham ushbu global tendensiyalardan chetda qolmay, Qurolli Kuchlar tizimini zamonaviy axborot-kommunikatsiya texnologiyalari bilan mustahkamlash, SI imkoniyatlaridan keng foydalanishga intilmoqda. Mamlakatimizda raqamli transformatsiya jarayonlari, “Raqamli O‘zbekiston – 2030” strategiyasi doirasida SI texnologiyalarini joriy etish bo‘yicha muhim qadamlar tashlanmoqda. Shu bilan birga, harbiy sohada sun’iy intellektni qo‘llashning ilmiy, tashkiliy va amaliy asoslarini ishlab chiqish dolzarb vazifa sifatida qaralmoqda.

Ushbu maqolada Qurolli Kuchlar tizimida sun’iy intellekt texnologiyalarini qo‘llashning zamonaviy yechimlari ilmiy tahlil qilinadi, xalqaro tajribalar o‘rganilgan holda O‘zbekiston sharoitida qo‘llash istiqbollari yoritiladi. Shu orqali harbiy xavfsizlikni ta’minlashda raqamli innovatsiyalarning tutgan o‘rni va ularni tatbiq etish mexanizmlari bo‘yicha aniq xulosalar ishlab chiqiladi.

Dunyoning ilg‘or mamlakatlari qurolli kuchlari, qurol-yarog‘, harbiy va maxsus texnika (QHMT) rivojlanishining istiqbollari deyarli barcha harbiy mutaxassislar tomonidan birinchi navbatda axborotlashtirish, robotlashtirish, qo‘shinlar va qurollarni boshqarishni avtomatlashtirish bilan bog‘liq.

Qo‘shinlarni boshqarish jarayonlarini avtomatlashtirish va QHMT shuningdek, ushbu maqsadlar uchun sun’iy intellekt tizimlaridan foydalanishni farqlash kerak. Birinchi holda, biz ma’lumotlarni yig‘ish, tasniflash, tuzish algoritmlari to‘plami bilan jihozlangan kompyuterlar

haqida gapiramiz, keyinchalik ular rasmiylashtirilgan usullar yordamida jangovar muammolarni hal qilish uchun dastlabki ma'lumotlar tizimi sifatida ishlatiladi. Avtomatlashtirishga nisbatan intellektualizatsiyaning asosiy farqlari-bu turli xil va to'liq bo'lmagan ma'lumotlarga, tez-tez o'zgarib turadigan vaziyatlarga asoslangan holda, kompyuterning muhim noaniqlik sharoitida qaror qabul qilish qobiliyatini amalga oshirish. SI tizimining o'ziga xos dasturiy ta'minotni mustaqil ravishda takomillashtirish qobiliyati, shu jumladan algoritmik jihatdan ta'minlanmagan vaziyatlarda dasturlashni o'zi amalga oshirish qobiliyati sifatida o'rganish va moslashuvchanlikning o'zi ham katta ahamiyatga ega.

Uning asosiy xususiyati bu murakkab va tez o'zgaruvchi sharoitlarda odamga o'xshash qarorlar qabul qilish qobiliyati. An'anaviy avtomatlashtirilgan boshqaruv tizimlari qat'iy algoritmlar asosida ishlaydi va oldindan belgilangan vazifalar bilan chegaralangan. Shu sababli ular noaniq yoki kutilmagan sharoitlarda samarasiz bo'lishi mumkin. SI esa moslashuvchanlik, o'z-o'zini o'rganish va yangi vaziyatlarga tez moslashish qobiliyati bilan ajralib turadi. Bu uning nafaqat jangovar boshqaruv, balki razvedka, logistik ta'minot, kiberxavfsizlik va strategik tahlil sohalarida ham keng qo'llanilishiga yo'l ochmoqda.

Ushbu maqola tahliliy va taqqoslash metodlariga asoslangan bo'lib, turli davlatlar tajribasi (AQSh, Xitoy, Rossiya) hamda amaliy loyihalar (DARPA, Project Maven, dronlar to'dasi texnologiyalari) misolida SI texnologiyalarining qo'llanilish yo'nalishlari ko'rib chiqiladi. Shuningdek, O'zbekiston va Markaziy Osiyo mintaqasi uchun moslashuvchan yondashuvlar ishlab chiqish imkoniyatlari baholanadi. Tahlil shuni ko'rsatadiki, SI texnologiyalari Qurolli kuchlarda quyidagi asosiy yo'nalishlarda samarali yechimlar berishi mumkin:

1. **Harbiy qurilishni boshqarishda** geosiyosiy vaziyatni tahlil qilish, xavflarni baholash, dushman niyatlarini prognozlash.
2. **Jangovar tayyorgarlik**ni oshirishda real vaqt rejimida simulyatsiyalar va ko'p agentli modellashtirish orqali qo'shinlarni mashq qildirishda keng qo'llash.

3. **Jangovar boshqaruv** tizimida ya’ni razvedka, zarba berish va mudofaa tizimlarida SI asosidagi axborot-qaror qabul qilish tizimlarida keng joriy qilish.

4. **Moddiy-texnik ta’minot** – resurslarni taqsimlash, ta’minot zanjirini optimallashtirish, ehtiyot qismlar va o‘q-dorilar zaxiralarini bashoratlash.

5. **Kiber va axborot urushi** – ijtimoiy tarmoqlarda noto‘g‘ri axborotni aniqlash, targ‘ibot va qarshi targ‘ibotni avtomatlashtirish, shifrlash tizimlarini sinovdan o‘tkazish.

SI texnologiyalarini harbiy sohada keng tatbiq qilish bir qator muammolarni ham yuzaga keltiradi. Birinchidan, algoritmlarning shaffofligi va boshqaruv nazoratini saqlash zarurati mavjud: SI qarorlari inson hayoti bilan bog‘liq bo‘lgani uchun ularning xavfsizligi va ishonchliligi alohida ahamiyatga ega. Ikkinchidan, SI tizimlari keng ma’lumotlar bazasiga tayanganligi sababli axborot xavfsizligini ta’minlash dolzarb masalaga aylanadi. Uchinchidan, sun’iy intellekt asosidagi qurollarni qo‘llash xalqaro huquqiy me’yorlarni qayta ko‘rib chiqishni talab qiladi.

Shu bilan birga, imkoniyatlar ham katta: kvant kompyuterlar SI samaradorligini bir necha bor oshirishi, dronlar to‘dasi esa an’anaviy jangovar tizimlarni falaj qilish darajasiga chiqishi mumkin. Shuningdek, SI tibbiy ta’minotda qo‘llash yaradorlarni davolash, reabilitatsiya qilish va hatto neyroprotezlar orqali ularning hayot sifatini tiklashda ham ulkan imkoniyatlarga ega.

Qurolli Kuchlar tizimida sun’iy intellekt (SI) texnologiyalarini qo‘llash zamonaviy harbiy strategiya va mudofaa salohiyatini mustahkamlashning eng muhim yo‘nalishlaridan biridir. Tahlillar shuni ko‘rsatadiki, SI harbiy faoliyatning barcha bosqichlarida – razvedka va kuzatuv, jangovar boshqaruv, kiberxavfsizlik, logistika, tibbiyot, shuningdek, ta’lim va simulyatsiya jarayonlarida samaradorlikni tubdan oshirishi mumkin.

Biroq, SI texnologiyalarini muvaffaqiyatli tatbiq etish nafaqat texnik imkoniyatlar, balki tashkiliy, huquqiy va axloqiy yondashuvlarni ham talab qiladi. Bu borada bir nechta muhim xulosalar ilgari surish mumkin:

1. **Strategik darajadagi muvofiqlashtirish** orqali SI texnologiyalarini joriy etishda davlat mudofaa strategiyasi, xalqaro tajribalar va milliy xavfsizlik ehtiyojlari birgalikda hisobga olinishi kerak.
2. **Kadrlar tayyorlashda** yangi intellektual texnologiyalarni samarali qo‘llash uchun harbiy mutaxassislarning malakasini oshirish, ilmiy-tadqiqot bazasini mustahkamlash zarur.
3. **Texnik infratuzilma** shakllantirishda SI tizimlari katta hajmdagi ma’lumotlar, yuqori tezlikdagi hisoblash va xavfsiz tarmoqlarni talab qiladi. Shu bois, infratuzilmani modernizatsiya qilish dolzarbdir.
4. **Huquqiy va axloqiy me’yorlar** – avtonom qurollar, qaror qabul qiluvchi algoritmlar va inson ishtirokisiz operatsiyalarni amalga oshirishda xalqaro va milliy huquqiy asoslar ishlab chiqilishi lozim.
5. **Integratsion yondashuv** – SI texnologiyalari alohida emas, balki mavjud harbiy tizimlar bilan integratsiyalangan holda, bosqichma-bosqich joriy etilishi samarali natija beradi.

Umuman olganda, SI texnologiyalarini Qurolli Kuchlar tizimida keng joriy etish davlat mudofaa salohiyatini oshirish, zamonaviy xavfsizlik muammolariga tezkor javob berish va jangovar tayyorgarlikni yuqori darajaga ko‘tarishda strategik yechim sifatida qaralishi lozim. Shu bilan birga, bu jarayon ilmiy asoslangan, kompleks va milliy manfaatlarga mos holda olib borilishi zarur.

Qurolli kuchlarda SI texnologiyalarini joriy etish strategik ustuvorlikka aylanib bormoqda. Bu jarayon nafaqat jangovar imkoniyatlarni kengaytiradi, balki davlat xavfsizligi, iqtisodiy barqarorlik va axborot kurashidagi pozitsiyani ham mustahkamlaydi. O‘zbekiston uchun bu yo‘nalishda xalqaro tajribalarni o‘rganib, milliy mudofaa tizimiga moslashgan SI yechimlarini ishlab chiqish dolzarbdir. Shu asosda harbiy samaradorlikni oshirish, xavflarni erta aniqlash va tezkor qarorlar qabul qilish imkoniyatlari sezilarli darajada kengayadi.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasi Prezidentining 2023-yil 31-maydagi PQ-167-son “O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora tadbirlar to‘g‘risida”gi qarori.

2. O‘zbekiston Respublikasining 2022 yil 15 apreldagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonuni.

3. Muratovich M.R., Rajaboevich I.A. As a continuous process in forming and developing the professional consciousness of military servants//PEDAGOGS journal. – 2023. – T. 36. – №. 1. – C. 32-34.

4. Muratovich M. R. Rajaboyevich IA Harbiy xizmatchilarning kasbiy ongini shakllantirish va rivojlantirishda uzluksiz jarayon sifatida //PEDAGOGS jurnali. – 2023. – T. 36. – №. 1. – C. 32-34.

5. Махмудов Р. М., Хайдаров И.О. Ахборот–психологик хавфсизликнинг шахсга таъсир этувчи восита ва усуллари //PEDAGOGS jurnali. – 2023. – T. 28. – №. 1. – C. 30-33.

6. Махмудов Р. М. “Қуролли Кучлар тизимида мураббий-ҳарбий хизматчи аёлларни касбий фаолиятга тайёрлашдаги методик ишларининг ўзига хослиги” //PEDAGOGS jurnali. – 2023. – T. 30. – №. 1. – C. 119-122.

HARBIY OBYEKTLAR PERIMETRINI MUHOFAZA QILISHDA TOLALI-OPTIK DATCHIKLAR TAHLILI

Yusupov U.A.
Tashmanov Y.B.
O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti kafedra katta o‘qituvchisi.
O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti kafedra boshlig‘i.

Hozirgi davrda harbiy obyektlarning perimetrini ishonchli himoya qilish global xavfsizlik tizimining eng muhim masalalaridan biri hisoblanadi. Strategik ahamiyatga ega obyektlar atrofida ruxsatsiz kirish, terrorchilik xuruji yoki diversiya harakatlarini erta aniqlash va oldini olish

samarali himoya tizimlarini talab etadi. An'anaviy kuzatuv va signalizatsiya vositalari ko'plab sharoitlarda yetarlicha samaradorlik bermasligi sababli, so'nggi yillarda yuqori texnologiyalarga asoslangan innovatsion yechimlarga ehtiyoj ortmoqda.

Shunday zamonaviy texnologiyalardan biri – tolali-optik datchiklar bo'lib, ular yuqori sezgirlik, elektromagnit shovqinlarga barqarorlik va portlash hamda yong'in xavfsizligi kabi afzalliklari bilan ajralib turadi. Optik tola asosidagi bunday datchiklar yordamida harbiy obyektlar perimetri bo'ylab uzluksiz kuzatuv olib borish, turli mexanik ta'sirlarni (tebranish, bosim, kesish, egilish) aniqlash va xavfsizlik tizimiga tezkor signal uzatish mumkin.

Natijada tolali-optik texnologiyalar an'anaviy elektr datchiklariga nisbatan ishonchliligi, ekspluatatsion qulayligi va uzoq muddatli xizmat ko'rsatishi bilan ustunlik qiladi hamda harbiy obyektlarning xavfsizlik darajasini sezilarli ravishda oshirishga xizmat qiladi.

Optik tolalar nafaqat telekommunikatsiya sohasida ma'lumot uzatishda, balki o'lchash sohasida datchiklar yaratishda ham tobora keng qo'llanilmoqda. Optik tolalarning ishlatilishida bir qator afzalliklari mavjud: keng o'tkazuvchanlik qobiliyati, optik signalning kichik so'nishi, yuqori darajadagi shovqinbardoshlilik, ruxsatsiz kirishdan kuchli himoya, kichik og'irlik va hajm, qisqa tutashuv va uchqun hosil bo'lmasligi sababli portlash va yong'inga xavfsizlik, uzoq xizmat muddati.

Tolali-optik datchiklar elektr analoglariga nisbatan quyidagi afzalliklarga ega:

– elektromagnit maydon va shovqinlarga ta'sirchan emas;

– radiatsiyaga chidamli;

– murakkab iqlim sharoitlari va agressiv kimyoviy muhitlarda barqaror ishlaydi;

– yerga ulash va galvanik ajratishga ehtiyoj yo'q;

– yong'in va portlash xavfsizligi yuqori;

– datchik hisoblash qurilmadan o'nlab kilometr uzoqda joylashishi mumkin;

– ko‘plab datchiklarni ketma-ket ulab, yagona tizim yaratish imkoniyati mavjud;

– bir datchikdan bir nechta parametrlarni aniqlash mumkin;

– radio to‘lqin manbai hisoblanmaydi;

– elektr toki urishi xavfi yo‘q;

– korroziyaga uchramaydi;

– yuqori ekologik xavfsizlik darajasiga ega;

– kichik og‘irlik va hajm;

– ixchamlik.

Ushbu afzalliklarning ba’zilari portlash va yong‘inga xavfsizlik (elektr ulanish mavjud bo‘lmagani sababli uchqun chiqish ehtimoli yo‘q), agressiv muhitlarda ishlashdagi barqarorlik optik tola asosidagi datchiklarni xavfli obyektlarda qo‘llash imkonini beradi. Bundan tashqari, yerga ulash konturlari va turli o‘tkazgichlarni ulash joylarida kuchlanish muammolari kuzatilmaydi, shuningdek, qiyin kirish mumkin bo‘lgan hududlarda ham o‘lchash imkoniyati mavjud.

Bugungi kunda tolali-optik o‘lchov va nazorat tizimlari nafaqat ekspluatatsion xususiyatlari, balki tannarxi bo‘yicha ham elektr tizimlariga raqobatchi bo‘lib bormoqda.

Tolali-optik datchiklarga odatda shunday elektron qurilmalar kiradi: ular ko‘rinadigan, infraqizil va ultrabinafsha diapazondagi elektromagnit nurlanish ta’sirida ro‘yxatga olish yoki boshqaruv tizimiga yakka yoki kompleks signal uzata oladi. Signal uzatish datchik elementlari orasida optik tola orqali amalga oshiriladi.

Odatda optik datchik tarkibiga quyidagilar kiradi:

- nurlanish manbai (yarim o‘tkazgich lazeri yoki maxsus diod, signal hosil qiladi);
- optik nurlanish qabul qilgich (fotodiod);
- o‘zgartirgich (optik nurlanish parametrlarini ro‘yxatga olish qurilmasi qabul qila oladigan signallarga aylantiradi).

Tolali-optik datchikning ishlash prinsipi quyidagicha:

– nurlanish manbaidan chiqqan optik nurlanish uzatuvchi optik tola kanali orqali sezgir elementga yetib boradi. Bu element optik tolaning

maxsus tayyorlangan qismi bo‘lib, u o‘lchanayotgan kattalik ta’sirida bo‘ladi;

– fizik ta’sir natijasida sezgir elementning optik xususiyatlari o‘zgaradi, bu esa optik nurlanish parametrlarining o‘zgarishiga olib keladi;

– o‘zgargan optik nurlanish optik kanal orqali ro‘yxatga oluvchi qurilmaga uzatiladi.

Tolali-optik datchiklar bir necha belgilar bo‘yicha tasniflanadi: foydalanish usuliga ko‘ra, o‘lchanayotgan parametrning lokalizatsiyasiga ko‘ra, o‘lchanayotgan kattalikning optik nurlanishga ta’sir joyiga qarab, ishlash prinsipiga ko‘ra.

- Foydalanish usuliga ko‘ra:
  - optik tola faqat uzatish liniyasi sifatida ishlatiladigan datchiklar (ular “gibrid datchiklar” deb ataladi, chunki o‘lchash optik toladan tashqarida amalga oshiriladi);
  - optik tola sezgir element sifatida ishlatiladigan sensor tipidagi datchiklar (ular “sof tolali datchiklar” deyiladi, chunki o‘lchash optik tolaning o‘zida amalga oshiriladi).

Bu yerda optik tolaning elektr maydonga (Kerr effekti), magnit maydonga (Faradey effekti), vibratsiya, harorat, bosim va deformatsiyaga (masalan, egilish) sezgirligi qo‘llaniladi. Odatda bu effektlar aloqa tizimlarida kamchilik sifatida qaraladi, ammo datchiklarda ularni afzallik sifatida foydalanish mumkin.

- O‘lchanayotgan parametr lokalizatsiyasiga ko‘ra:
  - nuqtaviy datchiklar (obyektning muayyan nuqtasida o‘lchash va nazorat qilish imkonini beradi, bunda optik tola sezgir element va signalni uzatish vositasi sifatida ishlatiladi);
  - taqsimlangan yoki ko‘p nuqtali datchiklar (optik tola butun uzunligi bo‘ylab yagona parametrni sezadi);
  - qisman taqsimlangan datchiklar (optik tolada joylashtirilgan datchiklar massividan iborat bo‘lib, optik tola butun massivdan ma’lumot uzatishni ta’minlaydi).
- O‘lchanayotgan kattalikning ta’sir joyiga ko‘ra:

- ichki modulyatsiyali tolali-optik datchiklar (unda optik tola sezgir element sifatida ishlaydi, modulyatsiya mexanik ta’sir, harorat, magnit yoki elektr maydon ta’sirida amalga oshiriladi);
- tashqi modulyatsiyali tolali-optik datchiklar.

Tolali-optik datchiklar yuqori aniqlik, ishonchlilik va xavfsizlik talab etiladigan sohalarda, jumladan, harbiy obyektlar perimetrini muhofaza qilishda samarali qo‘llanilishi mumkin bo‘lgan zamonaviy texnologiyalardan biridir. Ularning elektromagnit shovqinlarga mutlaqo ta’sirchan emasligi, uzoq masofalarda ham uzluksiz ishlashi, portlash va yong‘in xavfsizligi, agressiv muhitlarda barqarorligi ushbu texnologiyani strategik ahamiyatga ega hududlarni kuzatish va himoya qilishda muhim ustunlikka ega qiladi.

Perimetr xavfsizligi tizimlarida tolali-optik datchiklarning qo‘llanilishi hududni 24/7 real vaqt rejimida kuzatish, har qanday noxush harakat yoki tashqi ta’sirni aniqlash, signalizatsiya va avtomatik ogohlantirish tizimlari bilan integratsiyalash imkonini beradi. Ayniqsa, taqsimlangan yoki ko‘p nuqtali datchiklar yordamida katta maydonlarni bir butun tarzda nazorat qilish mumkinligi harbiy obyektlarda hududiy xavfsizlikni ta’minlash uchun katta amaliy ahamiyat kasb etadi.

Bundan tashqari, tolali-optik datchiklarning korroziyaga chidamliligi, elektr toki urishi xavfining yo‘qligi va yerga ulash ehtiyojining mavjud emasligi ularni uzoq muddatli foydalanishga moslashtiradi. Ularning ixchamligi va ko‘p funksionalligi tufayli bunday texnologiyalarni mavjud perimetr muhofaza tizimlariga integratsiya qilish nisbatan oson bo‘lib, xarajatlarni kamaytiradi va samaradorlikni oshiradi.

Shunday qilib, harbiy obyektlarni ishonchli darajada himoyalash, xavfsizlik monitoringini takomillashtirish va tashqi xavf-xatarlarni erta aniqlash jarayonida tolali-optik datchiklar eng istiqbolli va samarali texnologiyalardan biri sifatida alohida ahamiyat kasb etadi. Kelajakda ushbu texnologiyaning yanada rivojlanishi perimetr xavfsizligi tizimlarining ishonchliligi va samaradorligini sezilarli darajada oshirishi kutilmoqda.

Foydalanilgan adabiyotlar:

1. Родина О.В. Волоконно-оптические линии связи. Практическое руководство. – М.: Горячая линия – Телеком, 2020. – 400 с.

2. Листвин А. В., Листвин В. Н., Швырков Д. В. Оптические волокна для линий связи. М.: ЛЕСА Рарт, 2003. 107 с.

3. Кабели оптические. Общие технические условия. ГОСТ Р 52266-2020. – Москва. – Стандартинформ, 2020.

4. Волоконно-оптические датчики. Вводный курс для инженеров и научных работников Под ред. Э. Удда М: Техносфера, 2008. – 520 с.

SUN'IY INTELLEKT TIZIMLARIDA MA'LUMOTLAR VA BILIMLAR BAZASINI TASHKIL ETISH USULLARI TAHLILI

Raximov B.N.
t.f.d., professor
Muxtdinov X.A.
i.f.n., professor
Yusupov B.K.
PhD, professor
Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti

Sun'iy intellekt tizimlari rivojlanishi bilan ma'lumotlar va bilimlar bazasini samarali tashkil etish masalasi yanada dolzarb ahamiyat kasb etmoqda. Har qanday sun'iy intellekt tizimining samaradorligi asosan uning ma'lumotlar va bilimlar bilan qanday ishlashi va ularni qay tarzda saqlashi bilan bog'liq. Ma'lumotlar bazasi ko'pincha tizimning asosiy fakt va raqamlar to'plamini saqlovchi bo'limi hisoblanadi, bilimlar bazasi esa o'sha ma'lumotlar asosida qaror qabul qilish va muammolarni hal qilishga imkon beradigan qoidalardan iborat.

Ma'lumotlar va bilimlar bazasini tashkil etish sun'iy intellekt tizimlari uchun alohida muhim, chunki bu tizimlarning samaradorligi va to'g'ri ishlashi uchun to'g'ri hamda optimallashtirilgan usullardan foydalanish talab etiladi. Odatda, ushbu usullar ma'lumotlar va bilimlar

bazasini samarali boshqarish va ularni ishlatish uchun qo‘llaniladi. Bunga relatsion ma’lumotlar bazalari, ontologik modellar, semantik tarmoqlar va qoidalar asosidagi tizimlar kiradi. Har bir usulning o‘ziga xos afzalliklari va qo‘llanilish sohalari mavjud bo‘lib, ular ma’lum bir sun’iy intellekt tizimining foydalanish maqsadiga qarab tanlanadi [1]. Shu sababli ham sun’iy intellekt tizimlarida ma’lumotlar va bilimlar bazasini tashkil etish usullarini tadqiq qilish dolzarb muammolardan biri hisoblanadi.

Bilim va bilimlar bazasi

Sun’iy intellekt va mashinali o‘qitishda bilim va bilimlar bazasining o‘rni.

Sun’iy intellekt va mashinali o‘qitishda bilim va bilimlar bazasi juda muhim rol o‘ynaydi. Quyida bu ikki sohada bilim va bilimlar bazasining o‘rni va ahamiyatini batafsil tushuntirib o‘taman.

Sun’iy intellektda bilimning o‘rni.

Sun’iy intellekt tizimlari inson bilimlarini taqlid qilib, murakkab masalalarni hal qilishga va qaror qabul qilishga mo‘ljallangan. Bunda bilimlar va bilimlar bazasi asosiy o‘rinni egallaydi.

Sun’iy intellekt tizimlarida foydalaniladigan bilimning turlari:

- Deklarativ bilim: Bu turdagi bilimlar faktlar, qoidalar yoki faktlarni ifodalash usullari sifatida saqlanadi. Masalan, “Toshkent O‘zbekistonning poytaxti” degan fakt deklarativ bilimdir.
- Prosedural bilim: Bu bilimlar qanday qilib biror ishni bajarish kerakligi to‘g‘risida bo‘ladi. Masalan, qanday qilib mashinani boshqarish yoki matematik hisob-kitoblarni bajarish haqida bilimlar procedural bilimdir [2, 3].

Sun’iy intellektda bilimlarni qo‘llanilishi:

- Ekspert tizimlar: Bu turdagi tizimlar odam ekspertlarning bilimlarini qoidalar va faktlar orqali saqlaydi va bu bilimlarga asoslanib qaror qabul qiladi. Masalan, tibbiy ekspert tizimlar kasalliklar diagnostikasini amalga oshirishda doktorlarning bilimlarini o‘zida saqlaydi va ulardan foydalanadi.
- Qaror qabul qilish: Sun’iy intellekt tizimlari bilimlarni analiz qilish va ulardan yangi bilimlar olish orqali muammolarni hal qilishga yordam beradi. Ular bilimlar bazasida mavjud bo‘lgan bilimlardan

foydalanib, yangi vaziyatlarda qanday qarorlar qabul qilish kerakligini o‘rganadi.

Mashinali o‘qitishda bilimning o‘rni.

Mashinali o‘qitish algoritmlari asosan bilim va ma’lumotlarga tayanadi. Bilim va bilimlar bazasi mashinaga ma’lumotlarni to‘g‘ri o‘rgatish va optimal natijalarga erishishda katta ahamiyatga ega.

Mashinali o‘qitishning bilimga tayanishi:

- Ma’lumot va bilimlar: Mashinali o‘qitish algoritmlari bilimlar bazasidan olingan ma’lumotlar ustida ishlaydi. Bu ma’lumotlar yordamida algoritmlar o‘zlarini o‘rgatadi va kelajakdagi prognozlar yoki klassifikatsiyalarni amalga oshiradi.
- Ma’lumotlar bazasi va bilishga asoslangan modellar: Mashinali o‘qitishda algoritmlar ilmiy nazariyalar va bilimlar bazasi asosida modellar yaratadi. Ma’lumotlar bazasi qanchalik to‘liq va aniq bo‘lsa, mashina o‘zini shunchalik samarali o‘rgatadi va yaxshi natijalar beradi.

Mashinali o‘qitishdagi bilimlar bazasining o‘rni:

- Ma’lumotlar yig‘ish va qayta ishlash: Mashinali o‘qitish uchun katta hajmdagi ma’lumotlar kerak bo‘ladi, va ushbu ma’lumotlar bilimlar bazasida saqlanadi. Bilimlar bazasi ma’lumotlar yig‘ilishida va ularni tahlil qilishda foydalaniladi.
- Bilimlar transferi: Mashinali o‘qitish tizimlari bir sohada olingan bilimlarni boshqa sohalarda qo‘llash orqali bilimlarni transfer qilish imkoniyatiga ega. Masalan, o‘rganilgan biror model boshqa sohalarda ishlatilishi mumkin.

Sun’iy intellekt va mashinali o‘qitishda bilimlar bazasidan foydalanishning afzalliklari [3]:

- Samaradorlik: Bilimlar bazasi sun’iy intellekt va mashinali o‘qitish tizimlarini samarali qiladi, chunki tizimlar yangidan yangi bilimlarni izlash va ularga moslashish qobiliyatiga ega bo‘ladi.
- O‘zini-o‘z o‘qitish: Bilimlar bazasidagi ma’lumotlardan foydalanib, tizimlar o‘zini-o‘zi rivojlantirish imkoniyatiga ega bo‘ladi, ya’ni yangi bilimlarni o‘rganadi va yangiliklarga moslashadi.
- Bilimlarni saqlash va qayta ishlash: Sun’iy intellekt tizimlari bilimlar bazasini yaratib, unda saqlangan bilimlarni tahlil qilish va ularni

o‘rganish orqali ilg‘or algoritmlarni ishlab chiqadi.

Bilim va bilimlar bazasi sun’iy intellekt va mashinali o‘qitish tizimlarining asosi hisoblanadi. Bilimlar bazasi sifatida xizmat qiladigan ma’lumotlar ombori yordamida tizimlar yangi bilimlarni o‘zlashtiradi, o‘rganadi va qaror qabul qiladi. Shuning uchun, bilim va bilimlar bazasining to‘g‘ri boshqarilishi ushbu sohalardagi tizimlarning samaradorligini oshirishda katta ahamiyatga kasb etadi.

Ma’lumotlar bazasi va bilimlar bazasining o‘zaro farqi

Sun’iy intellekt tizimlarida ma’lumotlar bazasi va bilimlar bazasidan foydalanish.

Sun’iy intellekt tizimlarida ma’lumotlar bazasi va bilimlar bazasi - bu ikkita asosiy vosita bo‘lib, ular bir-biridan farq qiladigan, ammo bir-birini to‘ldiradigan texnologiyalardir. Ular birgalikda murakkab tizimlarni yaratishda va qaror qabul qilishda ishlatiladi. Quyida har birining ta’rifi, o‘ziga xos xususiyatlari va ularning sun’iy intellekt tizimlarida qanday qo‘llanilishi haqida batafsil ma’lumot beraman.

1. Ma’lumotlar bazasi.

Ma’lumotlar bazasi - bu jadal ravishda ma’lumotlarni yig‘ish, saqlash va qidirish uchun foydalaniladigan texnologiya. Bu sun’iy intellekt tizimlarining katta hajmdagi ma’lumotlarni samarali boshqarishi va ulardan foydalanuvchilarga kerakli axborotni taqdim etish imkonini beradi [4, 5].

a. Ma’lumotlar bazasining xususiyatlari.

- **Ma’lumotlarning tartiblanishi**: Ma’lumotlar bazasi turli formatda, jumladan matnlar, raqamlar, rasm yoki videolar shaklida bo‘lishi mumkin. Ular tuzilgan ma’lumotlar ko‘rinishida (masalan, SQL) yoki yarim tuzilgan (masalan, NoSQL) shakllarda saqlanishi mumkin.
- **Moslashuvchan qidiruv**: Ma’lumotlar bazasi katta hajmdagi ma’lumotlardan qidiruv, saralash va filtrlar orqali kerakli ma’lumotlarni topish imkoniyatini beradi.
- **Real vaqtda ishlash**: Ma’lumotlar bazalari real vaqtda yoki yuqori tezlikda ishlashi mumkin, bu sun’iy intellekt tizimlariga tezkor qarorlar qabul qilish imkonini beradi.

b. Ma’lumotlar bazasining sun’iy intellektda ishlatilishi.

- **Ma’lumotlar yig‘ish va saqlash**: Ma’lumotlar bazasi sun’iy intellekt tizimlarida ma’lumotlarni yig‘ish uchun asosiy vosita hisoblanadi.

Sun'iy intellekt algoritmlari uchun ishlatiladigan ma'lumotlar bu bazalardan olinadi. Misol uchun, chat-botlar foydalanuvchi so'rovlarini tahlil qilish uchun avvalgi dialoglar yoki lug'at ma'lumotlar bazasidan foydalanadi.

- **O'qitish ma'lumotlarini boshqarish**: Mashinani o'qitish (Machine Learning) algoritmlari katta hajmdagi ma'lumotlar to'plamiga (dataset) asoslanadi. Ma'lumotlar bazasi o'qitish uchun zarur bo'lgan ma'lumotlarni samarali boshqaradi va yangilanib turadi.
- **Tahlil qilish va prognozlash**: Ma'lumotlar bazasida saqlangan tarixiy yoki real vaqtdagi ma'lumotlar tahlil qilinib, sun'iy intellekt algoritmlari yordamida prognozlar qilinadi. Masalan, moliyaviy prognoz tizimlarida ma'lumotlar bazasi moliyaviy o'zgarishlarni saqlaydi va kelajakdagi tendensiyalarni tahlil qiladi.

2. Bilimlar bazasi.

Bilimlar bazasi - bu murakkab qoidalar, qonuniyatlar, ma'lumotlar va tushunchalarni o'z ichiga olgan, biror ma'lumot yoki vaziyatga nisbatan qanday javob berish kerakligini belgilaydigan tizimdir. Bilimlar bazasi insonlarning tajribalari va qoidalari asosida yaratiladi va qaror qabul qilish jarayonlarida ishlatiladi.

a. Bilimlar bazasining xususiyatlari.

- **Strukturalangan bilimlar**: Bilimlar bazasi faktlar, qoidalar va qonuniyatlar ko'rinishida bo'ladi. Bu qoidalarga ko'ra, tizim ma'lumotni qanday tahlil qilish va qarorlar qabul qilishini belgilaydi.
- **Qoidalarga asoslangan tizimlar**: Bilimlar bazasida ma'lum bir "agar-shunda" qoidalari mavjud bo'ladi. Masalan, tibbiy tashxis qo'yish tizimida agar bemorda o'ziga xos alomatlar mavjud bo'lsa, u holda aniq tashxis tavsiya qilinishi mumkin.
- **Tushuntirish qobiliyati**: Bilimlar bazasi foydalanuvchi uchun qaror qabul qilish jarayonini tushuntirishi mumkin. Misol uchun, ekspert tizimlarida tizim qanday qarorga kelganligini tushuntiruvchi qism bo'lishi mumkin.

b. Bilimlar bazasining sun'iy intellektda ishlatilishi [5].

- **Ekspert tizimlari**: Bilimlar bazasi ekspert tizimlarida keng qo'llaniladi. Bu tizimlar insonlar kabi murakkab masalalar bo'yicha qaror

qabul qilish uchun ekspert bilimlarini qo‘llaydi. Masalan, tibbiyot, muhandislik, huquqshunoslik va boshqa sohalarda ekspert tizimlar bilimlar bazasiga tayangan holda tavsiyalar beradi.

- **Murakkab masalalarni hal qilish**: Bilimlar bazasi murakkab va noaniq masalalarni hal qilishda yordam beradi. Masalan, kasalliklarni diagnostika qilish tizimlari alomatlar asosida kasallik tashxisini belgilashi mumkin.
- **Qaror qabul qilish**: Bilimlar bazasidan foydalangan holda sun’iy intellekt tizimlari turli qoidalarga asoslangan qarorlar qabul qilishi mumkin. Bunda tizim qoidalardan foydalanib, ma’lumotlarni tahlil qiladi va optimal qaror chiqaradi.

1-jadval

Ma’lumotlar bazasi va bilimlar bazasi o‘rtasidagi 7 ta farq va ularning xususiyatlari

Xususiyat	Ma’lumotlar bazasi	Bilimlar bazasi
Ma’lumotlar turi	Asosan xom ma’lumotlar va faktlar	Murakkab bilimlar, qonuniyatlar va qoidalar
Ma’lumotlarning tabiati	Strukturali va tuzilgan ma’lumotlar	Ma’lumotlar bilan birga ular qanday ishlatilishi haqida ham ma’lumot
Foydalanish usuli	Katta hajmdagi ma’lumotlarni saqlash va qidirish uchun	Qaror qabul qilish va muammolarni hal qilish uchun
Amalga oshirilishi	SQL, NoSQL, ma’lumotlar omborlari	Qoidalarga asoslangan tizimlar, ekspert tizimlari
Misollar	MySQL, MongoDB, Oracle, PostgreSQL	MYCIN, DENDRAL, CLIPS
Xususiyat	Ma’lumotlar bazasi (Database)	Bilimlar bazasi (Knowledge Base)

3. Ma’lumotlar bazasi va bilimlar bazasi o‘rtasidagi farqlar.

Ma’lumotlar bazasi va bilimlar bazasi sun’iy intellekt va axborot tizimlar uchun muhim vositalar bo‘lib, ular o‘zaro bog‘liq bo‘lsa-da, turli funksiyalarga ega. Ularning ta’riflarini va farqlarini ko‘rib chiqamiz. Ma’lumotlar bazasi va bilimlar bazasi o‘rtasidagi asosiy farq va ularning xususiyatlari 1-jadvalda keltirilgan [6, 7].

4. Bilimlar bazasi va ma’lumotlar bazasining integratsiyasi.

Ko‘plab zamonaviy sun’iy intellekt tizimlarida **ma’lumotlar bazasi** va **bilimlar bazasi** birgalikda ishlaydi. Masalan [7, 8]:

- **Tibbiy tashxis tizimlari**: Ma'lumotlar bazasida bemorning tibbiy ma'lumotlari saqlanadi, bilimlar bazasi esa bu ma'lumotlar asosida kasallik tashxisini aniqlash uchun qoidalarga ega bo'ladi.
- **Kiberxavfsizlik**: Bilimlar bazasi hujum turlarini va xavf xabarlarini biladi, ma'lumotlar bazasi esa tarmoqlardagi voqealar va xatti-harakatlar haqidagi ma'lumotlarni saqlaydi.
- **Mashinani o'qitish modellarida**: O'qitish uchun ma'lumotlar bazasi katta hajmdagi ma'lumotlar bilan ishlasa, bilimlar bazasi modellarni tanlash va ularni qanday ishlashini nazorat qilishda qoidalar asosida harakat qiladi.

Bilimlar bazasi va ma'lumotlar bazasi o'rtasidagi o'zaro farqlari tahlili bo'yicha xulosa qiladigan bo'lsak sun'iy intellekt tizimlarida ma'lumotlar bazasi va bilimlar bazasi o'zaro bir-birini to'ldiradi. Ma'lumotlar bazasi tizim uchun ma'lumotlarni saqlash va qidirish uchun ishlatilsa, bilimlar bazasi murakkab bilimlarni qayta ishlash hamda qarorlar qabul qilishga yordam beradi. Tizimlar o'rtasidagi integratsiya ularning muvaffaqiyatli ishlashi uchun zarur bo'lib, ular birgalikda turli sohalarda yuqori samaraga ega sun'iy intellekt yechimlarni taqdim eta oladi.

Foydalanilgan adabiyotlar:

1. Taherdoost, H., & Madanchian, M. (2023). Artificial Intelligence and Knowledge Management: Impacts, Benefits, and Implementation. https://www.mdpi.com/2073-431X/12/4/72
2. Duran, C., & Gutierrez, S. (2021). Artificial Intelligence Methodologies for Data Management. Symmetry. https://doi.org/10.3390/sym13112040
3. Stoykova, S., & Shakev, N. (2023). Artificial Intelligence for Management Information Systems: Opportunities, Challenges, and Future Directions. Algorithms. https://doi.org/10.3390/a16080357
4. Konys, A., & Nowak-Brzezińska, A. (2022). Knowledge Engineering and Data Mining.
5. Dai, W., & Liu, X. (2020). Knowledge Graph Embedding and Completion in AI Systems. Springer. https://link.springer.com/article/10.1007/s11023-020-09509-w
6. Gupta, A., (2021). AI-Based Knowledge Base Management Systems for Industrial Applications. Springer. https://www.springer.com/gp/book/9789811640

TOIFALANGAN OBYEKTLARGA QARATILGAN KIBERHUJUM TURLARI VA ULARDAN HIMOYANI TASHKIL ETISH USULLARI

To‘rayev B.Z.
t.f.d., professor
Rayimov M.SH.
Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti

Hozirgi kunda axborot texnologiyalari va raqamli infratuzilmalar jadal rivojlanib bormoqda, bu esa yangi kiberxavfsizlik tahdidlari va hujum turlarining paydo bo‘lishiga olib kelmoqda. Ayniqsa, toifalangan obyektlar (yoki muhim axborot resurslari) kiberhujumlarga nisbatan sezgir bo‘lib, ularga zarar yetkazish davlatga katta zarar keltirishi mumkin. Toifalangan obyektlarga davlat ma’lumotlari, maxfiy sirlarini saqlovchi serverlar, moliyaviy tashkilotlar tarmoqlari va boshqa himoyalangan axborot tizimlari kiradi.

Kiberhujumlar turlari o‘zgaruvchan va murakkab bo‘lib, hujumchilar yangi texnologiyalarni qo‘llab, turli xil texnikalar yordamida tizimlarga kirishga harakat qilishadi. Toifalangan obyektlarga qaratilgan kiberhujumlar maxfiy ma’lumotlarni o‘g‘irlash, tizimlarni ishdan chiqarish yoki axborotni yo‘q qilishga qaratilgan bo‘lishi mumkin. Bunday hujumlar davlat organlari va boshqa muhim infratuzilma tizimlariga katta xavf tug‘diradi[3].

Texnologiyalar rivojlangan sari kiberhujumlar tobora murakkablashmoqda, shu sababli himoyani tashkil etish usullari ham yangilanib, rivojlanib borishi kerak.Hujumlarni aniqlash, ularning oldini olish va ularni tezkor ravishda bartaraf etish uchun samarali xavfsizlik choralarini amalga oshirish – axborot xavfsizligini ta’minlashning muhim qismlaridan biridir. Ushbu tadqiqotda kiberhujumlar turlarini tahlil qilish, ularning zararli ta’sirini kamaytirish va toifalangan obyektlar xavfsizligini mustahkamlash yo‘llari ko‘rib chiqiladi. Shu sababli ham mazkur toifalangan obyektlarga qaratilgan kiberhujum turlari va ulardan himoyani tashkil etish usullarini ko‘rib chiqish muhim va dolzarb muammolardan biri hisoblanadi.

Toifalangan obyektlarga bo‘ladigan kiberhujumlarni ikkita asosiy turga bo‘lish mumkin taqsimlangan va maqsadli hujumlar[1,3].

Taqsimlangan kiberhujumlar bir vaqtning o‘zida ko‘p sonli foydalanuvchilar va obyekt resurslariga qaratilgan. Odatda, bunday hujumlar obyekt haqida va unda ishlovchi xodimlarning sizib chiqqan ma’lumotlar bazalaridan foydalanadi[2].

Maqsadli hujumlar - bu ma’lum bir toifalangan obyektga qarshi oldindan rejalashtirilgan "hujum". Ushbu hodisalarda tajovuzkor nafaqat ichki resurslarga kirish huquqiga ega bo‘ladi, balki u aniqlanmaguncha obyekt tarmog‘ida qoladi - bu kunlar, oylar va hatto yillar bo‘lishi mumkin. Maqsadli hujumlar yuqori texnik malakaga ega xakerlar tomonidan amalga oshiriladi. Ular avtomatlashtirilgan vositalardan foydalanadilar, hujum vektorlarini mustaqil ravishda aniqlaydilar, zaifliklardan va ba’zi tizim xususiyatlaridan foydalanadilar, o‘z tajribalari asosida.

Maqsadli kiberhujumlar va ularning ishlash tamoyillari bo‘yicha asosiy ma’lumotlar 1-jadvalda keltirilgan.

1-jadval

Maqsadli kiberhujumlar va ularning ishlash tamoyillari

Kiberhujum turi	**Maqsad**	**Ishlash tamoyillari**	**Nishonlar**
Fishing (Phishing)	Maxfiy ma’lumotlarni olish	Soxta elektron pochta yoki xabarlar orqali foydalanuvchini aldab, maxfiy ma’lumotlarni olish.	Foydalanuvchilar, toifalangan obyektlar xodimlari
Ransomware	Ma’lumotlarni shifrlab, to‘lov talab qilish	Maqsadli tizim yoki ma’lumotlarni shifrlab, ularga kirishni cheklash va to‘lov evaziga ochish.	Kompaniyalar, davlat muassasalari
DDoS (Distributed Denial of Service)	Tizimni ishdan chiqarish	Ko‘plab so‘rovlar yuborish orqali server yoki tarmoqni ortiqcha yuklab, uni ishlamay qolishga majbur qilish.	Veb-saytlar, onlayn xizmat ko‘rsatuvchi tizimlar
APT (Advanced Persistent Threat)	Uzoq muddatli ma’lumot o‘g‘irlash	Tizimga kirib, uzoq muddat davomida yashirin holda qolib, ma’lumotlarni	Davlat muassasalari,banklar

Kiberhujum turi	Maqsad	Ishlash tamoyillari	Nishonlar
		muntazam ravishda o‘g‘irlash.	
MITM (Man-in-the-Middle)	Foydalanuvchi va server o‘rtasidagi ma’lumotlarni ushlash	Foydalanuvchi va server o‘rtasidagi ma’lumot almashinuvini ushlab, o‘zgartirish yoki maxfiy ma’lumotlarni o‘g‘irlash.	Banklar, onlayn to‘lov tizimlari
Zero-Day Attack	Yangi aniqlangan tizim zaifliklaridan foydalanish	Tizim yoki dasturdagi yangi aniqlangan zaifliklari orqali tezkorlik bilan hujum qilish va shikast yetkazish.	Har qanday yangi dastur yoki tizim
SQL Injection	Ma’lumotlar bazasiga ruxsatsiz kirish	Veb-saytning kiritish maydonlari orqali zararli SQL buyruqlarini yuborib, ma’lumotlar bazasiga kirishga urinish.	Ma’lumotlar bazasi bilan bog‘liq veb-saytlar,maxfiy ma’lumotlar bazalari
Social Engineering	Foydalanuvchilarni aldab ma’lumot olish	Psixologik aldov usullari yordamida foydalanuvchilarni maxfiy ma’lumotlarini berishga majburlash.	Foydalanuvchilar, toifalangan obyektlar xodimlari
Spear Phishing	Aniq nishonga qaratilgan fishing hujumi	Maxsus maqsadli guruhga yoki shaxsga yo‘naltirilgan soxta xabar yoki elektron pochta orqali ma’lumot olish.	Korporativ rahbarlar, yuqori darajadagi xodimlar
Credential Stuffing	Parollarni sinab ko‘rib kirish	O‘g‘irlangan foydalanuvchi parollarini turli xizmatlarda sinab, tizimga ruxsatsiz kirish.	Har qanday onlayn tizimlar yoki akkauntlar

Fishing. Fishing hujumlari turli kompaniyalarning qonuniy xabarlari sifatida yashirilishi mumkin bo‘lgan elektron pochta xabarlariga tayanadi. Bunday soxta xabarda tajovuzkorlar havolaga amal qilishni, zararlangan faylni yuklab olishni taklif qilishi yoki maxfiy foydalanuvchi

ma’lumotlarini – loginlar, parollar va bank kartasi hisob raqamlarini uzatishni so‘rashi mumkin[4].

DDoS hujumlari. Taqsimlangan kiberhujumlar toifasiga kiradi. Ushbu hujumlar bir nechta kompiyuterlar yordamida ko‘p sonli so‘rovlar bilan tizimlarni to‘sib qo‘yadi, bu esa o‘tkazish qobiliyatining pasayishiga va tizimlarning haddan tashqari yuklanishiga va tizimni ishdan chiqishga olib keladi. Aslida, DDoS hujumi avtomagistralni to‘sib qo‘yadigan kutilmagan tirbandlikka o‘xshaydi[7].

Man-in-the Middle (MITM) hujumi. Ushbu turdagi hujum bilan kiberjinoyatchi tarmoqqa uchinchi ko‘rinmas foydalanuvchi sifatida kiradi va barcha veb-trafikni o‘zi orqali o‘tkazadi. Ayni paytda potensial qurbon hech narsadan bexabar, bu esa tajovuzkorning tizimlar uchun barcha kirish ma’lumotlariga ega bo‘lishiga olib keladi. Keyinchalik olingan ma’lumotlar toifalangan obyektlar faoliyatiga zarar yetkazadigan usulda foydalanish mumkin bo‘ladi[5].

Ushbu jadvalda turli xil maqsadli kiberhujumlar, ularning asosiy maqsadlari va ishlash tamoyillari ko‘rsatilgan. Har bir hujum turi o‘ziga xos texnikalar va vositalardan foydalanib amalga oshiriladi va ularning har biri turli sohalarga zarar yetkazishi mumkin. Shu bois, tizimlar uchun himoyani ta’minlashda har bir hujum turiga qarshi samarali choralar ko‘rilishi muhimdir.

Toifalangan obyektlarga amalga oshiriladigan kiberhujumlardan himoyalanish usullari

Toifalangan obyektlarda kiberhujumlarni tezkor oldini olish va unga nisbatan javob qaytarish bu ma’lumotlar xavfsizligi va saqlanishini uchun juda muhimdir. Toifalangan infrastrukturada axborot xavfsizligini ta’minlash bo‘yicha chora-tadbirlarni uchta asosiy turlari mavjud: texnik vositalar, tashkiliy tadbirlar va xavfsizlik darajasini profilaktik tekshiruvlari. Toifalangan obyektlarga amalga oshiriladigan kiberhujumlardan himoyalanish usullari 2-jadvalda keltirilgan.

2-jadval

Toifalangan obyektlarga amalga oshiriladigan kiberhujumlardan himoyalanish usullari

Kiberhujum turi	Himoyalanish usullari	Izoh
Fishing (Phishing)	Foydalanuvchilarni xabardor qilish va o‘qitish Elektron pochta filtrlash tizimlarini o‘rnatish	Soxta xabarlarni aniqlash uchun kuchli spam filtrlardan foydalanish va xodimlarni o‘qitish
Ransomware	Ma’lumotlarni muntazam zaxiralash Antivirus va antimalware vositalarini yangilab borish	Zaxiralangan ma’lumotlar bilan fayllarni qayta tiklash va ransomwaredan himoyalanish
DDoS (Distributed Denial of Service)	Tarmoqni yukni taqsimlash tizimlari bilan himoyalash DDoS hujumlarni aniqlash vositalari o‘rnatish	Tarmoqdagi ortiqcha yuklamani kamaytirish va hujumlarni oldindan aniqlash
APT (Advanced Persistent Threat)	Tarmoqni muntazam monitoring qilish Kuchli autentifikatsiya va foydalanuvchi ruxsatlarini boshqarish	Uzoq muddatli yashirin hujumlarni aniqlash uchun doimiy tahlil qilish
MITM (Man-in-the-Middle)	End-to-End shifrlashni qo‘llash SSL sertifikatlarni yangilash va tasdiqlash	Foydalanuvchi va server o‘rtasidagi ma’lumotlarni shifrlash orqali hujumlarni oldini olish
Zero-Day Attack	Dasturlarni yangilab borish Zararli dasturlardan himoyalanish vositalarini o‘rnatish	Tizim zaifliklarini tezda tuzatish va xavfsizlik patchlarini muntazam yangilash
SQL Injection	SQL so‘rovlarini himoyalash uchun parametrli so‘rovlar qo‘llash Ma’lumotlar bazasi xavfsizligini kuchaytirish	Ma’lumotlar kiritish joylarida qo‘shimcha xavfsizlik choralarini joriy etish
Social Engineering	Xodimlarni doimiy o‘qitish Maxfiy ma’lumotlarga kirish uchun kuchli autentifikatsiya tizimlarini o‘rnatish	Psixologik hujumlarni oldini olish uchun xavfsizlik protokollarini takomillashtirish
Spear Phishing	Elektron pochta xavfsizligini kuchaytirish Maxsus xavfsizlik choralari va autentifikatsiya usullarini kuchaytirish	Aniq maqsadli hujumlarni oldindan aniqlash va elektron pochta himoyasini kuchaytirish
Credential Stuffing	Kuchli parol siyosatini joriy qilish Ikki faktorli autentifikatsiyani qo‘llash	O‘g‘irlangan ma’lumotlar orqali tizimga kirishni

Kiberhujum turi	Himoyalanish usullari	Izoh
		oldini olish uchun parol va ruxsatlarni boshqarish

Ogohlikni oshirish va zamonaviy apparat va dasturiy qurilmalardan foydalanish. Muntazam ichki vebinarlar va axborot xavfsizligi asoslari bo‘yicha tushuntirishlar olib borish. Bu xodimlarning xabardorligini oshirishga yordam beradi va ular hujumlarni aniqlash va ularga qarshi kurashish uchun zarur bo‘lgan ko‘nikmalarga ega bo‘lishini ta’minlaydi.

Xulosa qilib aytadigan bo‘lsak toifalangan obyektlarga qaratilgan kiberhujumlar davlat organlari, korporatsiyalar va maxfiy ma’lumotlarni saqlovchi boshqa muhim infratuzilmalar uchun katta xavf tug‘diradi. Ushbu hujumlar maxfiy ma’lumotlarni o‘g‘irlash, tizimlarni ishdan chiqarish yoki ularni buzishga qaratilgan bo‘lib, ular phishing, ransomware, DDoS, APT kabi turli shakllarda bo‘lishi mumkin. Har bir hujumning o‘ziga xos texnikasi va maqsadi bor[8]. Himoyalanish usullari esa hujumning har xil turlariga qarshi samarali choralar ko‘rishga qaratilgan. Bularga kuchli autentifikatsiya, shifrlash texnologiyalari, muntazam dasturiy yangilanishlar, ma’lumotlarni zaxiralash va xodimlarni xavfsizlik bo‘yicha doimiy o‘qitish kiradi[6]. Zamonaviy kiberxavfsizlik strategiyalari har bir hujum turiga mos choralarni o‘z ichiga olishi va tizimlarni muntazam kuzatish va monitoring qilish orqali ularni o‘z vaqtida aniqlash va bartaraf etish imkoniyatini berishi zarur. Shunday qilib, kiberhujumlardan himoyalanishda integratsiyalangan xavfsizlik tizimlari va muntazam xavfsizlik choralarini kuchaytirish eng muhim omil hisoblanadi.

Foydalanilgan adabiyotlar:

1. J.Smith & A. Khan, (2023), Cyber Attack Types and Defense Strategies.

2. L.Chen, (2022), Emerging Cyber Threats: A Review.

3. M.Jones, (2023), Protecting Critical Infrastructure.

4. R.Patel, (2023), Phishing Attacks: Techniques and Prevention.

5. A.Gupta, (2024), Ransomware: Understanding the Threat.

6. S.Lopez, (2023), Cybersecurity Frameworks: Best Practices.

7. P.Williams, (2023), Network Security: Current Trends and Challenges.

8. D.Zokirov, (2023), Tarmoq xavfsizligi va yangi tahdidlar.

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СОВРЕМЕННЫХ КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЯХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Базаров А.Б.
Военный институт информационно-коммуникационных технологий и связи Военного университета безопасности и обороны Республики Узбекистан, PhD

Традиционный подход к описанию функционирования современных телекоммуникационных сетей на основе моделей, основанных на математических формулах с некоторыми упрощенными предположениями, не обеспечивает представления сложности происходящих процессов. При этом упрощенные модели не могут эффективно представить практические сценарии, а разработанные сложные модели требуют сложных математических вычислений. Для решения данной проблемы применение методов искусственного интеллекта (ИИ) в секторе телекоммуникаций рассматривается перспективной.

Проектирование, управление и оптимизация телекоммуникационных сетей представляют собой сферы, где наиболее актуальны процессы внедрения ИИ.

Интеллектуальный подход к методам эксплуатации и управления современными сложными телекоммуникационными инфраструктурами позволит снизить затраты и повысить масштабирование.

Методы ИИ в системе связи специального назначения позволяют применить различные способы оптимизации функционирования системы [1].

Необходимость улучшения качества и устойчивости связи при применении различных устройств, приложений и сложных сетей для беспроводных сетей требуют большого количестве информационных ресурсов.

ИИ предоставляет возможность построить систему управления с высокой производительностью при внедрении в телекоммуникационные системы, которые обрабатывают большие объем данные.

Внедрение передовых методов ИИ, таких как машинное обучение (МО) и глубокое обучение (ГО), в мобильной связи обеспечит в управлении огромными данными.

Эффективно адаптироваться к реальным условиям и учиться на опыте позволяют методы машинного обучения. Такая адаптация является решающей при обеспечении высоких требований предоставляемые к телекоммуникационным сетям [2].

Возможности данной технологии позволяют применить ее на различных уровнях функционирования беспроводной сети (рис.1):

на физическом уровне - кодирование и декодирование, формирование луча и определение сигнала;

на уровне управления - распределение ресурсов сети и частот, доступ к каналам;

на сетевом уровне - управление трафиком и сетями.

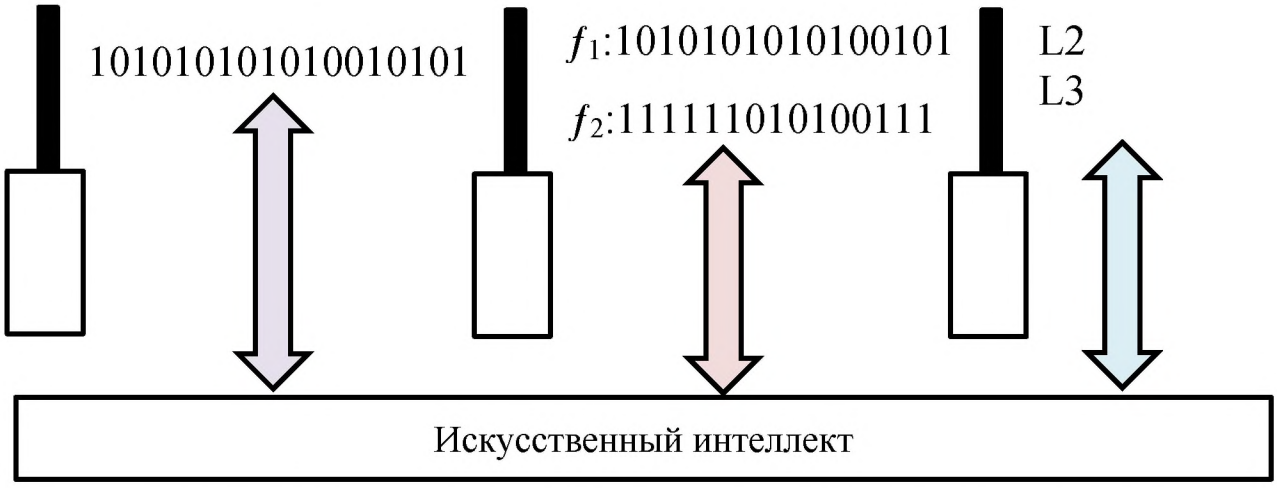


Рис. 1. Применение ИИ в системах беспроводной связи.

В отличие от традиционных подходов, где для оптимизации могут быть применены методы вычислительно невыполнимые или неспособные адаптироваться к изменяющимся условиям, данный факт является определяющим для решения сложных задач телекоммуникационных сетей.

Прогностическое обслуживание оборудования является основным параметром, который обеспечивает непрерывность обслуживания и имеет решающее значение для многих приложений, где применяются методы ИИ.

Выявление и определение путей решения проблем, возникающих в сети в режиме реального времени с применением ИИ, позволяет обеспечивает непрерывное функционирование системы.

Динамическое распределение полосы пропускания и определение приоритета трафика в моменты пиковой нагрузки и обеспечение оптимальной производительности являются проблемами управления сетевым трафиком, для которых применение методов ИИ являются одним из путей решения.

Изменения условий нагрузки и запросов пользователей в режиме реального времени обеспечивается управлением трафиком с применением методов ИИ как более эффективного при сравнении со статическими методами.

Интеллектуальное управление сетевыми ресурсами с применением ИИ обеспечивает необходимую полосу пропускания и низкую задержку, сохраняя при этом приемлемую производительность для менее требовательных услуг.

Анализ противодействия различных средств радиоэлектронной борьбы и тактики действий войск требует пересмотра порядка организации и функционированию радиосвязи.

Учитывая растущую зависимость от данных, необходимо понимать, что сети беспроводной связи при применении их в реальных условиях подвержены влиянию помех, сбоям в работе, частотным и территориальным ограничениям.

Надежная передача информации в системе управления является необходимым условием для эффективного функционирования вооруженных сил и должна считаться важнейшей параметром при реализации систем связи.

Проблемы оптимального распределения частного диапазона, применяемой мощности и скорости передачи данных, изменяемых по

мере противодействия со стороны противника, является актуальной. При этом создание самооптимизирующейся сети (СОС) позволяет обеспечить передачу информации в сложной радиоэлектронной обстановки.

Внедрение методов ИИ и МО в управление сетью позволят оптимизировать распределение ресурсов, улучшить маршрутизацию трафика и обеспечат функционировать СОС.

Объединение информационных ресурсов в единое целое при привлечение различных сил и средств является задачей, требующего тщательного принятия решения. Разработка и создание единой платформы для обеспечения обмена информацией между различными уровня управления повышает ситуационную осведомленность, возможности планирования и взаимодействия.

Обработка большого количества информации с применением методов ИИ и МО позволяют осуществить оптимизацию управления в реальном режиме времени, обеспечив устойчивость передачи информации.

Таким образом решения данных проблем предлагается провести исследования применения технологий ИИ, включающие в себя методы МО и ГО для обеспечения создания СОС.

Основными направлениями исследования определить:

разработку математической основы методов и алгоритмов ИИ для применения в системе СОС;

анализ методов и алгоритмов ИИ для применения в беспроводных системах связи;

разработка модели СОС специального назначения для совершенствования процесса передачи информации в сложной радиоэлектронной обстановке.

Использованной литературы:

1. Мищенко Д.А. //Математические модели и методы динамической адаптации интерактивных телекоммуникационных сетей: автореферат дис. кандидата технических наук: 1.2.2. //

«Саратовский государственный технический университет имени Гагарина Ю.А.». Саратов, 2024. - 23 с.: ил.

2. Generative AI in the Telecom Industry/The Ultimate Guide - https://www.subex.com/blog/generative-ai-in-the-telecom-industry-the-ultimate-guide.

QUROLLI KUCHLAR TUZILMALARIDA KIBERXAVFSIZLIK MUTAXASSISLARINI TAYYORLASH UCHUN KIBERPOLIGON YECHIMI

Qurbonov M.R.
CYBER-BRO LLC va CYBEROIT Inc
Kiberxavfsizlik kompaniyasi asoschi va rahbari.

Cyber Range tushunchasi va mohiyati

Cyber Range - bu virtual laboratoriya va simulyatsiya muhiti bo‘lib, unda kiberhujumlar, himoya choralarini qo‘llash hamda real infratuzilmaga o‘xshash tarmoqlar modellashtiriladi. U “raqamli poligon” vazifasini bajaradi va harbiy kadrlarni real kiber tahdidlarga tayyorlash imkonini beradi.

Cyber Range platformasida:

- Turli xil hujum ssenariylari (APT, DDoS, SCADA tizimlariga hujum va h.k.) sinovdan o‘tkaziladi;
- Kiberxavfsizlik bo‘yicha mutaxassislar xavfsiz muhitda mashq qiladi;
- Qurolli Kuchlarning o‘ziga xos infratuzilmalari modellashtiriladi.

Asosiy vazifalari

Cyber Range platformasi Qurolli Kuchlar tizimida quyidagi asosiy vazifalarni bajaradi:

1. **O‘quv va tayyorlov jarayonlari** - harbiy xizmatchilarni kiberxavfsizlik bo‘yicha amaliy mashg‘ulotlarda ishtirok ettirish.
2. **Test va baholash** - harbiy infratuzilmadagi zaifliklarni aniqlash va ularni bartaraf etish bo‘yicha tavsiyalar ishlab chiqish.
3. **Simulyatsiya** - real kiberhujum sharoitini yaratish va unga

qarshi mudofaa choralarini mashq qilish.

4. **Innovatsiyalarni smash** - yangi dasturiy va texnik vositalami xavfsizlik nuqtai nazaridan tekshirish.

5. **Hamkorlikni rivojlantirish** - turli bo‘linmalar va ittifoqchi davlatlar bilan qo‘shma mashg‘ulotlarni tashkil qilish.

Qurolli Kuchlar tizimidagi ahamiyati

Qurolli Kuchlarda Cyber Range platformasini joriy etish bir nechta strategik vazifalarni hal etishga xizmat qiladi:

- **Kiberhujumlardan himoya qilish** - aloqa, boshqaruv, razvedka va jangovar tizimlarni himoya qilish.
- **Harbiy operatsiyalarni qo‘llab-quvvatlash** - jang maydonida raqamli tizimlarning uzluksizligini ta’minlash.
- **Maxsus kiberbo‘linmalarni tayyorlash** - ofitserlar va mutaxassislar real tajribaga ega bo‘ladi.
- **Milliy xavfsizlikni mustahkamlash** - kiber urush sharoitida strategik ustunlik yaratish.

Ustunliklari

Cyber Range platformasining asosiy ustunliklari quyidagilardan iborat:

- **Xavfsiz muhit** - real tizimlarga zarar yetkazmasdan mashq o‘tkazish.
- **Moslashuvchanlik** - turli hujum va himoya ssenariylarini yaratish imkoniyati.
- **Tejamkorlik** - real infratuzilmada sinov o‘tkazishga nisbatan arzonroq.
- **Tezkor tayyorlash** - qisqa muddatda ko‘plab mutaxassislarni o‘qitish.
- **Xalqaro integratsiya** - hamkor davlatlar bilan qo‘shma mashg‘ulotlarni tashkil etish imkoniyati.

Amaliy qo‘llash yo‘nalishlari

1. Milliy Qurolli Kuchlar tizimi uchun **Kibertrening markazi**ni tashkil etish.
2. Harbiy aloqa, boshqaruv va razvedka tizimlarining zaifliklarini

tekshirish.

3. Mudofaa sohasida ishlab chiqilayotgan milliy dasturiy ta'minotlarni sinovdan o'tkazish.

4. Ittifoqchi davlatlar bilan qo'shma kiberxavfsizlik mashg'ulotlarini o'tkazish.

Xakerlik guruhlari va xalqaro APT guruhlarining O'zbekistondagi izlari

O'zbekistonda mahalliy va xalqaro xakerlik guruhlari faoliyat yuritmoqda. Quyida asosiy guruhlar va ularning faoliyati tahlil qilinadi:

1. **Mahalliy xakerlar**: O'zbekistonda mahalliy xakerlar asosan jiddiy texnik bilimlarga ega bo'lmaganligi sababli, oddiy ammo ko'p uchrovchi ojizliklardan foydalanib turli veb saytlarni deface - bosh sahifaning o'zgartirilishi kabi buzg'unchilik harakatlarini amalga oshirishadi, bundan tashqari fishing, firibgarlik va foydalanuvchilarni aldash bilan shug'ullanish holatlari uchrab turadi. Ularning aksariyati darknet bozorlarida shaxsiy ma'lumotlarni sotishga urinishgan.

2. **Xalqaro APT Guruhlari**: APT41 (Barium) va RedEcho guruhlari O'zbekistonning muhim infratuzilmasiga, xususan, energetika va telekommunikatsiya tarmoqlariga qarshi maqsadli hujumlar uyushtirgan. Evil Corp guruhining 2020 yildagi faoliyati, masalan, Wishbone dasturidagi 40 million foydalanuvchi ma'lumotlarini o'g'irlash bilan bog'liq edi. Bu guruh Rossiya maxsus xizmatlari bilan hamkorlikda ishlaydi degan taxminlar mavjud. 2024-yilda "BladedFeline" hackerlik guruhining izlari aniqlangan, xabar berilishicha guruh O'zbekistondagi telekommunikatsiya provayderi tarmoqlariga muvaffaqiyatli kirib borgan. Aynan qaysi provayder haqida gap ketgani va xujum masshtabi haqida aniq ma'lumot ochiqlanmagan. Guruhning xujum taktikasi va kiber qurollari analiz qilinganda asosan Eronlik guruhlarning TTP izlariga mos kelmoqda. Python, C#/.NET va C++ da yozilgan implantlar va PowerShell, VBScript orqali dastlabki kirish huquqini olishga urinishlar aynan eronlik guruhlarni eslatadi. Xujumning dastlabki izlari 2022-yilning may oylariga to'g'ri kelmoqda.

3. **Hujum Manbalari**: 97% hujumlar xorijiy IP manzillardan,

xususan, AQSh, Indoneziya va Niderlandiyadan keladi. Proksi-serverlar va VPN lar orqali haqiqiy manzillar yashiriladi.

4. **“Cyber Threat Intel”** tizimimiz kiber razvedka natijalariga koʻra, internetda Oʻzbekiston fuqarolariga tegishli boʻlgan 10 milliondan ortiq shaxsiy ma’lumotlar mavjud. Data Leak (ma’lumotlarning sizib chiqishi) - bu shaxsiy, korporativ yoki davlatga tegishli maxfiy ma’lumotlarning noqonuniy ravishda DarkNet yoki boshqa ochiq manbalarda tarqalishi.

5. **Infostealerlardan** ximoyalanish uchun bir nechta texnik choralar va ishlarni amalga oshirish zarur. Birinchi navbatda, tizimni muntazam yangilab turish, barcha xavfsizlik yangilanishlarini oʻrnatish lozim. Shuningdek, antivirus va anti-malware dasturlarini oʻrnatib, ularni muntazam ravishda yangilab borish ham muhim. Foydalanuvchi tomonidan foydalaniladigan barcha parollarni kuchli va murakkab qilish, shuningdek, ikki faktorli autentifikatsiyani (2FA) yoqish xavfsizlikni sezilarli darajada oshiradi. Internetda ishlashda faqat ishonchli va xavfsiz veb- saytlar va ilovalardan foydalanish kerak. Shubhali va noma’lum manbalardan yuklab olingan fayllardan saqlanish lozim. Tizimda administrator huquqlari faqat zarur boʻlganda berilishi kerak, shuningdek, "rootkit" yoki boshqa zararli dasturlarning tizimga kirishiga yoʻl qoʻymaslik uchun tarmoq monitoringi va xavfsizlik devorlari (firewall) oʻrnatish lozim. Xodimlar va foydalanuvchilarni xavfsizlikka oid treninglardan oʻtkazish ham muhimdir, chunki inson faktori koʻpincha zaif nuqta boʻlib xizmat qiladi. Dasturlarning ishlashini monitoring qilish, tarmoqda nojoʻya faoliyatlarni aniqlash va oldini olish uchun tarmoq traffigini tahlil qilish, shuningdek, zarur hollarda tizimga kirish uchun shifrlash texnologiyalarini qoʻllash xavfsizlikni mustahkamlashga yordam beradi.

6. Oʻzbekiston domeni ma’muriyati statistikasiga koʻra, mamlakatimizda **136 mingdan** ortiq domen nomlari mavjud. Bizning kiber razvedka tahlillarimizga koʻra, **10 milliondan** ortiq foydalanuvchilarning maxfiy ma’lumotlari, jumladan login parollar va shaxsiy ma’lumotlari dark webda tarqalganligi aniqlandi. Xakerlar oʻgʻirlagan bu ma’lumotlar

millionlab foydalanuvchilar hamda, **10 mingga** yaqin vebsaytlarni tahdid ostida qoldirmoqda.

Kiberxavfsizlik kompaniyamizning roli

CYBER-BRO O‘zbekiston kiberxavfsizlik sohasida yetakchi kompaniya sifatida muhim rol o‘ynaydi. Kompaniya milliy va xalqaro standartlar (CBEST, TIBER-EU, OWASP, ISO) asosida xizmatlar ko‘rsatadi va quyidagi yo‘nalishlarda faoliyat yuritadi:

1. **360° Xavfsizlik Tekshiruvi**: Tashkilot infratuzilmasini real hujum ssenariylari asosida sinovdan o‘tkazib, zaifliklarni aniqlaydi. SAST va DAST usullari yordamida dasturiy kodlardagi xatolar tahlil qilinadi.
2. **Targeted Attack Simulation (TAS)**: Qizil va ko‘k jamoalar yordamida APT guruhlarining hujumlarini simulyatsiya qiladi, bu tashkilotlarning real tahdidlarga tayyorgarligini, bardoshliligini oshiradi va baholaydi.
3. **Kiber Akademiya**: Tashkilot xodimlari uchun offlayn va on onlayn shaklida kiberxavfsizlik bo‘yicha maxsus kurslar tashkil qiladi. Bu xodimlarning malakasini oshirishga xizmat qiladi.
4. **Malware Analysis va Reverse Engineering**: Zararli dasturlarni tahlil qilib, ularning tarqalishini oldini oladi va himoya mexanizmlarini ishlab chiqadi.
5. **Konsulting xizmatlari**: Tashkilotlarga kiberxavfsizlik strategiyasini ishlab chiqishda yordam beradi va xalqaro sertifikatlarga ega mutaxassislar jalb qilinadi.

CYBER-BRO O‘zbekiston kibersarhadlarini himoya qilishda vatanparvar kadrlar yetishtirishga e’tibor qaratadi. Kompaniya kiberhujumlarni monitoring qilish, aniqlash va ulardan himoyalanish bo‘yicha davlat organlari va xususiy sektor bilan hamkorlik qiladi. Shu orqali O‘zbekistonning raqamli infratuzilmasini xavfsiz va barqaror saqlashga hissa qo‘shadi.

O‘zbekistonning raqamli transformatsiya jarayoni kiberxavfsizlik sohasida jiddiy muammolarni keltirib chiqarmoqda. Zamonaviy kibertahdidlar, xususan, phishing, malware, DDoS va APT hujumlari muhim infratuzilma uchun xavf tug‘diradi. Statistik ma’lumotlar

kiberhujumlar sonining keskin oshganini ko‘rsatmoqda, bu esa malakali kadrlar va zamonaviy texnologiyalarga bo‘lgan ehtiyojni oshiradi. CYBER-BRO kabi kompaniyalar kiberxavfsizlikni ta’minlashda muhim rol o‘ynab, tashkilotlarni himoya qilish va kiber gigiyenani oshirishda faol ishtirok etmoqda. Kelajakda kiberxavfsizlikni mustahkamlash uchun davlat, xususiy sektor va ta’lim muassasalari o‘rtasidagi hamkorlikni kuchaytirish zarur. Bu orqali O‘zbekiston raqamli makonda xavfsiz va barqaror muhitni ta’minlay oladi.

Cyber Range - bu Qurolli Kuchlar uchun raqamli davrda zarur bo‘lgan yangi avlod o‘quv poligoni hisoblanadi. U nafaqat kiberhujumlarga qarshi samarali mudofaa choralarini ishlab chiqishga, balki yangi strategiyalarni sinovdan o‘tkazishga, xalqaro hamkorlikni rivojlantirishga va milliy kiberxavfsizlikni mustahkamlashga xizmat qiladi.

Shunday ekan, Qurolli Kuchlar tizimida Cyber Range platformasini joriy etish - mamlakatimiz mudofaa salohiyatini oshirish, milliy xavfsizlikni ta’minlash va kelajakdagi kiber urush sharoitida raqobatbardosh bo‘lishning eng muhim omillaridan biridir.

Foydalanilgan adabiyotlar:

1. Microsoft Threat Intelligence (https://www.microsoft.com/en-us/security/blog/topic/threat-intelligence/)
2. Cyber-Bro.uz Blogi - kibertahdidlar hisobotlari (https://cyber-bro.uz/cbro-kiber- razvedka-tizimi/)
3. Nation-State Cyber Actors - (https://www.cisa.gov/topics/cyber-threats-and- advisories/nation-state-cyber-actors)
4. Hiylaqush kiberoperatsiyasi - (https://cyber-bro.uz/opcreeper/)

TELEKOMMUNIKATSIYA SOHASIDA MUTAXASSISLIK FANINI MASOFAVIY O‘QITISHNING METODLARI VA USULLARI

Abdulxayev N.M.
Musayev A.I.
“University of Management and Future Technologies” universiteti,
“Kammunikatsiya va raqamli texnologiyalari” kafedrasi dotsenti
“University of Management and Future Technologies” universiteti,
“Kammunikatsiya va raqamli texnologiyalari” kafedrasi dotsenti

Keyingi yillarda mutaxassislik fanlarini masofadan o‘qitish jarayonini jahon standartlari asosida tashkil etish maqsadida zamonaviy o‘qitish metodlaridan foydalanishga e’tibor qaratilmoqda. Zamonaviy metodlarni masofaviy o‘qitish sharoitida asinxron va sinxron o‘qitish rejimlarida mos holda qo‘llashni takomillashtirish umumiy ta’lim samaradorligining oshishiga xizmat qiladi. Xalqaro tajribalardan ko‘rish mumkinki, telekommunikatsiya sohasida mutaxassislik fanlarini masofadan o‘qitish jarayonida borgan sari keng rivojlanib bormoqda.

Mutaxassislik fanlarini masofaviy o‘qitish jarayonida o‘qitish vositalari o‘quv mazmunini taqdim etish, ta’lim oluvchilarning o‘quv faoliyatini nazorat qilish va boshqarishga xizmat qiladi.

Masofadan o‘qitishning modellari asosida zamonaviy o‘qitish metodlarini qo‘llash natijasida ta’lim oluvchi talabalar mustaqil fikrlash, tahlil qilish, xulosalar chiqarish, o‘z fikrini bayon qilish, uni asoslagan holda himoya qila bilish, munozara, bahs olib borish ko‘nikmalarini rivojlantirishga ta’lim oluvchilarning bilimlarni o‘zlashtirish faolligini oshirishga xizmat qiladi. Odatda an’anaviy ta’lim jarayonida qo‘llaniladigan bir qator zamonaviy metodlar masofaviy o‘qitish jarayonida ham qo‘llaniladi. Lekin masofaviy o‘qitish shaklining o‘ziga xos xususiyati va mazmunidan kelib chiqqan holda ta’lim berish usullari boshqacha tarzda tashkil etiladi.

Telekommunikatsiya sohasida masofaviy o‘qitish texnologiyalari zamonaviy ta’lim imkoniyatlarini kengaytiradi. Ularga quyidagilarni taqdim qilish qilishimiz mumkin:

a) o‘quv materialini (elektron kutubxonalarda, video formatida, kvestlar ko‘rinishida va boshqalar);

b) har xil turdagi topshiriqlarni (test yoki matn shaklida, kvestlar, keyslar, o‘rganish uchun maqolalar to‘plami ko‘rinishida va boshqalar);

v) ta’lim oluvchilar va ta’lim beruvchilarning turli formatdagi savollari va javoblarini (forum, chat, internet-konferensiya, shaxsiy xabarlar tizimi, videomurojaat va boshqalar);

g) ta’lim natijalarini (shaxsiy kabinet, ta’lim jarayoni ishtirokchilari uchun ularga ma’lum loginlar va parollar bo‘yicha ko‘rish uchun ochiq kundalik) va boshqalar.



1-rasm. Ta’lim jarayonining tashkil etilishini ketma-ketligining eski va zamonaviy ko‘rinishing umumiy ko‘rinishi.

Bu yerda ta’lim jarayonining tashkil etilishini ketma-ketligining eski va zamonaviy ko‘rinishi ko‘rsatilib o‘tildi.

Masofadan o‘qitish vositalari va kommunikatsiya shakllarini tanlash orqali o‘quv axborotni tasavvur qilishning uch turini ko‘rsatish mumkin.

1. "Birlik media" — qandayda bir o'qitish vositasi va axborot yetkazib berish kanalidan foydalanishni nazarda tutadi. Masalan, o'zaro xat yozishuv, o'quv radiosi yoki teleko'rsatuv orqali o'qitish. Bunday o'qitish modelida ustunlikka ega o'qitish vositasi grafik va chop etilgan materiallari bo'ladi. Ikki tomonlama kommunikatsiya amalga oshirilmaydi, shuning uchun bu masofaviy o'qitish metodini an'anaviy o'qitishga yaqin deb qarash mumkin.

2. "Multimedia" o'qitishning har xil vositalaridan foydalanishni nazarda tutadi: chop etilgan o'quv qo'llanmalari, kompyuter o'qitish tizimida har xil audio va videoyozuv tashuvchilari. Bunda axborotni "bir tomonga" yetkazish cheklangan, ikki tomonlama kommunikatsiyada ustunlikka ega. Kunduzgi o'qitishning elementlaridan foydalanish lozim: ta'lim oluvchi va tyutorning shaxsiy uchrashuvi, yakunlovchi o'quv seminarlari yoki konsultatsiyalar o'tkaziladi, imtihon qabul qilish yuzma-yuz bo'ladi va boshqalar.

3. "Gipermedia" — masofaviy o'qitish modelining uchinchi avlodi, kompyuter telekommunikatsiyalari ustunlik qiladigan zamonaviy axborot texnologiyalardan foydalaniladi. Bunda oddiy shakl sifatida elektron pochta, telefon va videokonferensiyalar hamda audio o'qitish qo'llaniladi.

Xulosa sifatida shuni ta'kidlash lozimki mutaxassislik fanlarini masofaviy o'qitishda bilim oluvchilar tomonidan quyidagi afzalliklarga erishish mumkin:

- Ta'lim oluvchi o'quv materiallarni mustaqil ravishda xotirjam o'qishi, ko'rishi, tinglashi, istalgancha takrorlashi mumkin.
- Darsda bo'lmagan ta'lim oluvchilar o'quv materiallarni mustaqil o'qish, ko'rish, tinglashi asosida o'zlashtirishlari mumkin.
- Ta'lim oluvchilar o'zlari uchun qulay bo'lgan vaqtda, istalgan joyda va har qanday vositadan (smartfon, planshet, noutbuk) foydalangan holda o'qishi mumkin.
- Darsdagi vaqt avval o'rganilgan materialni chuqurroq tushunish va izohlashni o'z ichiga olgan vazifalarga sarflanadi.
- Tyutor har bir ta'lim oluvchi bilan alohida muloqot o'rnatishi uning bilim darajasiga vazifalarni moslashtirishga yordam beradi.

- Tyutorning diqqati ta’lim oluvchining muayyan ishiga qaratilgan bo‘ladi (yakka ta’lim).

Foydalanilgan adabiyotlar:

1. Abduqodirov A.A., Pardaev A.X. Masofali o‘qitish nazariyasi va amaliyoti. – Toshkent: Fan, 2015 . – 145 b.

2. Вайндорф-Сысоева, М.Е. Методика дистанционного обучения: учеб. пособие для вузов // М.Е.Вайндорф-Сысоева, Т.С.Грязнова, В.А.Шитова; под общ. Ред М.Е.Вайндорф-Сысоевой. – М.: Издателство Юрайт, 2018. – 194 с. – Церийа: образовательный процесс.

3. Ибрагимов И.М. Информационные технологии и средства Фойдаланилган адабиётлар рўйхати 108 дистанционного обучения. – М: Академия, 2008. – 329 с.

4. Ibraymov A. Masofaviy o‘qitish tizimini tashkil etish va o‘quv kurslari mazmunini ishlab chiqishning o‘ziga xos xususiyatlari // O‘zMU xabarlari. – Toshkent, 2016. – №1/5 – B. 110 – 113.

5. Никуличева Н.В. Внедрение дистанционного обучения в учебный процесс образовательной организатсии: практ. пособие / Н.В. Никуличева. – М.: Федералный институт развития образования, 2016– 72с

ВНЕДРЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ В ВООРУЖЕННЫЕ СИЛЫ УЗБЕКИСТАНА

Абдуллаева С.М.
Дехконов О.Р.
ТАТУ

В последние десятилетия искусственный интеллект и автоматизированные системы управления начали активно использоваться в военной сфере. Они изменили традиционные подходы к стратегическому планированию, командованию и управлению боевыми действиями. Применение таких технологий позволяет ускорить процесс принятия решений, снизить количество

человеческих ошибок, повысить точность и оперативность действий, а также оптимизировать использование ресурсов. В связи с этим возникает вопрос о внедрении ИИ и АСУ в систему Вооруженных Сил Узбекистана, что может значительно повысить эффективность работы армии и обеспечить ее конкурентоспособность на международной арене.

Роль искусственного интеллекта и автоматизированных систем управления.

Искусственный интеллект обладает значительным потенциалом для использования в оборонной сфере, поскольку он способен обрабатывать большие объемы данных и прогнозировать возможные сценарии развития событий на поле боя. Применение ИИ позволяет эффективно анализировать данные разведки, определять оптимальные тактики и стратегии ведения боевых действий, а также прогнозировать поведение противника. Пример успешного применения ИИ в армиях других стран, таких как США, Китай и Россия, показывает, что эти технологии способны значительно улучшить эффективность военных операций, повысить точность принятия решений и минимизировать риски, связанные с человеческим фактором [2].

Автоматизированные системы управления (АСУ) также играют ключевую роль в управлении военными подразделениями. АСУ позволяют централизовать и ускорить передачу информации, оптимизировать логистику, а также улучшить координацию действий различных частей армии. Эти системы могут быть использованы для автоматизации планирования операций, мониторинга боевых действий, а также для обеспечения быстрой и точной обратной связи между командованием и подразделениями [3].

Преимущества внедрения ИИ и АСУ в Вооруженные Силы Узбекистана

Внедрение ИИ и АСУ в систему Вооруженных Сил Узбекистана принесет множество преимуществ. Во-первых, это позволит значительно ускорить процесс принятия решений, что особенно

важно в условиях боевых действий. Во-вторых, ИИ и АСУ помогут уменьшить влияние человеческого фактора, что повысит точность и надежность принятия решений. В-третьих, применение таких технологий позволит оптимизировать использование ресурсов, что приведет к более эффективному распределению материалов, техники и личного состава [6].

Также стоит отметить, что использование ИИ и АСУ существенно повысит уровень безопасности и защиты данных. Современные системы безопасности способны защищать информацию, связанную с операциями, от кибератак и утечек, что крайне важно для обеспечения секретности и безопасности военных данных [4].

Проблемы внедрения ИИ и АСУ

Несмотря на очевидные преимущества, внедрение ИИ и АСУ в Вооруженные Силы Узбекистана сопряжено с рядом проблем. Одной из основных является техническая сложность интеграции новых систем в существующие военные структуры. Многие из них требуют обновления инфраструктуры, а также совместимости с уже существующими программными и аппаратными решениями. Важно также обеспечить бесперебойную работу новых технологий в условиях ограниченных ресурсов и нестабильных условий, таких как полевые операции.

Еще одной проблемой является необходимость подготовки специалистов для работы с новыми технологиями. Для этого нужно разработать новые образовательные программы и тренировки, которые будут охватывать не только теоретические аспекты работы с ИИ и АСУ, но и практические навыки работы с этими системами в реальных условиях.

Технические и кадровые аспекты внедрения ИИ и АСУ

Для успешной интеграции ИИ и АСУ в Вооруженные Силы Узбекистана необходимо создать соответствующую инфраструктуру, которая будет включать в себя серверные мощности, системы хранения данных и надежные сети связи. Важной частью этого

процесса является создание и поддержание соответствующих программных продуктов, которые смогут эффективно взаимодействовать с существующими военными системами.

Не менее важным аспектом является кадровая подготовка. Специалисты, которые будут работать с ИИ и АСУ, должны иметь не только технические знания, но и практический опыт работы с военными системами. Это потребует пересмотра существующих образовательных программ и создания новых курсов, направленных на подготовку специалистов, способных эффективно работать с высокотехнологичными системами.

Проблемы безопасности и конфиденциальности данных

Внедрение ИИ и АСУ также связано с рисками, связанными с безопасностью данных. Кибератаки могут повлиять на функционирование этих систем, что приведет к утечке информации и потере контроля над военными действиями. Для защиты данных необходимо разработать системы кибербезопасности, которые будут предотвращать атаки и защищать информацию от несанкционированного доступа.

Особое внимание должно быть уделено защите персональных данных, связанных с личной информацией солдат и офицеров. Это включает в себя как данные, связанные с боевыми действиями, так и информацию о личной жизни военнослужащих, которую необходимо защищать в соответствии с международными стандартами и правами человека.

Перспективы внедрения ИИ и АСУ в Вооруженные Силы Узбекистана

Внедрение ИИ и АСУ в Вооруженные Силы Узбекистана имеет долгосрочные перспективы, которые позволят значительно повысить боеспособность армии, улучшить координацию действий, оптимизировать ресурсы и повысить безопасность. Узбекистан имеет потенциал для разработки и внедрения высокотехнологичных решений в оборонной сфере, что поможет стране стать более конкурентоспособной на международной арене [11].

С успешной интеграцией этих технологий армия Узбекистана сможет оперативно реагировать на угрозы, эффективно распределять ресурсы и обеспечивать безопасность не только на уровне страны, но и в рамках глобальных операций. Внедрение ИИ и АСУ в Вооруженные Силы Узбекистана является важным шагом на пути к созданию современного и высокотехнологичного оборонного сектора.

Внедрение искусственного интеллекта и автоматизированных систем управления в Вооруженные Силы Узбекистана представляет собой важный шаг к повышению их боеспособности и эффективности. Применение этих технологий в управлении боевыми действиями, анализе данных и прогнозировании обеспечит существенное улучшение процессов планирования и принятия решений, сделает армию Узбекистана более конкурентоспособной и эффективной в современных условиях.

Использованной литературы:

1. *Sparrow, R.* (2019). *Artificial Intelligence and the Future of Warfare*. Journal of Military Ethics, 18(3), 245-264.

2. *Binns, T.* (2020). *Automation in Military Systems: Opportunities and Challenges*. International Journal of Defence Technology, 15(4), 321-340.

3. *Родионов, А. Н.* (2020). *Использование искусственного интеллекта в военных операциях*. Журнал оборонных технологий, 9(2), 47-52.

4. *Кузнецов, С. П.* (2019). *Автоматизированные системы управления в современной армии*. Оборонная промышленность, 12(6), 233-245.

5. *Васильев, М. А.* (2018). *Инновационные технологии в военной сфере и их влияние на безопасность*. Современные технологии обороны, 8(4), 56-70.

6. *Sushko, M. & Kurbanov, S.* (2021). *Cybersecurity and Artificial Intelligence: Protecting Military Systems*. International Journal of Military Cybersecurity, 4(1), 67-80.

7. *Урманов, И. Б.* (2017). *Применение искусственного интеллекта в Вооруженных Силах России*. Журнал "Войсковые технологии", 13(1), 58-62.

8. *Liu, Z. & Zhang, J.* (2020). *Smart Defense Systems: Integrating AI and Automation into Military Forces*. Defence Innovation Review, 7(3), 143-160.

9. *Жуков, М. С.* (2021). *Автоматизация военных систем и ее влияние на эффективность вооруженных сил*. Оборонный вестник, 6(4), 101-109.

10. *Miller, L.* (2020). *The Role of Artificial Intelligence in Modern Warfare: A Strategic Perspective*. Journal of Defence Studies, 19(2), 50-65.

11. *Semenov, A. Y. & Tkachenko, V. P.* (2021). *The Impact of Artificial Intelligence on the Future of Warfare*. Russian Defence Journal, 5(1), 78-90.

12. *Goryacheva, O. V.* (2019). *Automation in the Military: A New Era of Combat*. International Review of Military Technology, 9(2), 35-49.

13. *Wang, Y. & Li, L.* (2020). *Military AI Integration: Challenges and Prospects*. Journal of Defence Technology, 22(1), 110-125.

14. *Davis, M.* (2021). *AI in Combat: How Military Forces Are Using Artificial Intelligence to Improve Combat Operations*. Military Technology, 18(3), 189-205.

15. *Золотухин, В. И.* (2018). *Развитие искусственного интеллекта в армейских операциях: перспективы и проблемы*. Вестник военной науки, 7(3), 90-104.

RAQAMLI TEXNOLOGIYALARNI QO‘LLASH ORQALI HARBIY EKZOSKELET YARATISH

Xurramov A.I.
O‘zbekiston Respublikasi Harbiy xavfsizlik va Mudofaa universiteti
Quruqlikdagi qo‘shinlar instituti “Ilmiy ishlar va innovatsion faoliyatni tashkil etish” bo‘limi katta ofitseri t.f.d. (DSc), dotsent, kapitan

Harbiy sohada inson salohiyatini oshirish eng muhim strategik vazifalardan biridir. Zamonaviy jangovar sharoitda askarlarning yuqori tezlikda harakatlanishi, og‘ir yuklarni ko‘tarishi va uzoq muddat davomida bardoshli bo‘lishi zarur. Shu bois dunyo davlatlari ekzoskelet texnologiyalarini ishlab chiqishga katta e’tibor qaratmoqda.

Raqamli texnologiyalar bu jarayonda muhim rol o‘ynaydi: ular yordamida ekzoskeletlar nafaqat mexanik konstruksiya sifatida, balki aqlli boshqaruv tizimiga ega bo‘lgan integrallashgan qurilma sifatida shakllanmoqda.

Raqamli texnologiyalarning harbiy ekzoskelet yaratishda o‘rni

Raqamli modellashtirish – mexanik qismlarning 3D modeli yaratiladi va yuklama, kuchlanish, chidamlilik bo‘yicha kompyuter simulyatsiyalari o‘tkaziladi. Bu fizik prototiplar sonini kamaytiradi.

Raqamli egizak (digital twin) – ekzoskeletning virtual nusxasi real vaqt rejimida askar harakati bilan uyg‘unlashtirilib, ishlash samaradorligi va texnik xizmat ko‘rsatish jarayoni oldindan nazorat qilinadi [1-3].

Sensor tizimlari – askar muskullaridagi kuchlanish, bo‘g‘imlarning harakati, yurak urishi va kislorod darajasini nazorat qiluvchi biosensorlar ekzoskeletga integratsiya qilinadi (1- rasm).

Sun’iy intellekt va mashina o‘rganish – ekzoskelet foydalanuvchi harakatlarini oldindan bashorat qilib, qo‘shimcha kuchni sinxron tarzda taqsimlaydi.

Og‘ir qurollar va jihozlarni (50–80 kg gacha) uzoq masofaga olib yurish.

Harbiy xizmatchilarning tezkor harakatini oshirish (yugurish tezligini 20–30% ga ko‘paytirish).



1- rasm. Harbiy ekzoskelet.

Charchoqqa chidamlilikni oshirish, jarohatlar ehtimolini kamaytirish.

Maxsus sharoitlarda (tog‘li hududlar, radioaktiv yoki kimyoviy zonalar) barqarorlikni ta’minlash.

Texnik topshiriq – jangovar sharoit talablari asosida parametrlash.

Raqamli dizayn – CAD/CAM tizimlarida modellashtirish.

Virtual sinovlar – kuchlanish, energiya sarfi, ergonomika bo‘yicha simulyatsiyalar.

Prototiplash – 3D bosma va CNC uskunalarida sinov nusxalari tayyorlash.

Raqamli egizak integratsiyasi – sinov natijalarini real vaqt kuzatuvi bilan moslashtirish [4-6].

Energiya manbalari (akkumulyatorlarning og‘irligi va ishlash muddati).

Sensor va boshqaruv tizimlari ishonchliligi (2- rasm)..



2- rasm. Harbiy ekzoskelet.

Harbiy sharoitlarda shovqin, magnit va elektromagnit halaqitlarga qarshilik.

Ekzoskelet texnologiyasini parashyut bilan uyg‘unlashtirish askarlar uchun yangi imkoniyatlarni ochadi. An’anaviy desant operatsiyalarida askar havodan tushgach og‘ir jihozlari bilan tez harakatlana olmaydi. Ekzoskelet esa:

Parashyutdan xavfsiz foydalanish – qo‘nish vaqtida zarbani so‘ndiruvchi gidravlik yoki elastik tizimlar askarning oyoq bo‘g‘imlarini jarohatdan himoya qiladi.

Jihozlarni xavfsiz olib tushish – 50–80 kg gacha bo‘lgan yuklarni parashyut bilan qo‘ndirishda ekzoskelet yuk taqsimotini tenglashtirib, orqa va bel muskullarini himoya qiladi.

Qo‘nishdan so‘ng tezkor harakat – askar zudlik bilan jangovar pozitsiyani egallashi va og‘ir qurol bilan ham yuqori tezlikda yurishi mumkin.

Desant tezkorligi – havodan tushgan bo‘linmalar qisqa vaqt ichida jangovar holatga keladi.

Jarohatlarning kamayishi – tizzalar, tovon va umurtqa pog‘onasi zarbadan himoyalanadi.

Og‘ir qurollarni tezkor joylashtirish – minomyot, pulemyot yoki portlovchi moddalarni tashish uchun qo‘shimcha texnika talab qilinmaydi.

Sur’atli hujum imkoniyati – raqamli boshqaruv orqali ekzoskelet askarning yugurish va sakrash qobiliyatini oshiradi, bu esa jangda raqib ustidan taktika jihatidan afzallik beradi [7, 8].

Xulosa qilib aytganda, raqamli texnologiyalarni qo‘llash orqali harbiy ekzoskeletlarni yaratish nafaqat askarlarning jismoniy imkoniyatlarini kengaytiradi, balki zamonaviy urush sharoitida ularga ustunlik beradi. “Raqamli egizak”, sun’iy intellekt va sensor tarmoqlarini joriy etish ekzoskeletlarning samaradorligi, ishonchliligi va moslashuvchanligini ta’minlaydi. Shu bois mazkur sohada O‘zbekiston Qurolli Kuchlari uchun ham ilmiy-tadqiqot ishlarini yo‘lga qo‘yish dolzarb hisoblanadi.

Foydalanilgan adabiyotlar:

1. Bogue, R. *Exoskeletons and robotic prosthetics: A review of recent developments*. Industrial Robot: An International Journal, 2015, 42(5), 422–427.

2. Dollar, A.M., Herr, H. *Lower Extremity Exoskeletons and Active Orthoses: Challenges and State-of-the-Art*. IEEE Transactions on Robotics, 2008, 24(1), 144–158.

3. Yang, X., Chen, X., & Chen, W. *Digital Twin for Smart Manufacturing and Maintenance in Military Applications*. Journal of Intelligent Manufacturing, 2021, 32(6), 1523–1538.

4. Kazerooni, H. *Human–Robot Interaction via the Transfer of Power and Information Signals*. IEEE Transactions on Systems, Man, and Cybernetics, 2005, 35(2), 198–208.

5. Panichsakul, S., et al. *Development of Powered Exoskeletons for Load Carrying in Military Operations*. Defense Technology, 2020, 16(4), 1053–1064.

6. Zuehlke, D. *SmartFactory – Towards a Factory-of-Things*. Annual Reviews in Control, 2010, 34(1), 129–138.

7. Умаров, А., Раҳмонов, Ш. *Рақамли технологиялар ва уларнинг ҳарбий соҳада қўлланилиши*. Тошкент: Fan va texnologiya нашриёти, 2022.

8. Ўзбекистон Республикаси Мудофаа вазирлиги. *Ҳарбий инновация ва рақамли трансформация стратегияси*. Тошкент, 2023.

TASVIRLARDAN YO‘L BELGILARINI TANIB OLUVCHI DASTURIY VOSITANING INTERFEYSI

M.A.Umarov
Bozorboyeva Z.Q.
XudoyberdiyevSh.B.
Giyasova G.A.
Samarov Sh.X.
UMFT universiteti dotsenti, muhriddin.umarov.1992@gmail.com
UMFT universiteti magistri

Ushbu dasturiy vositalardan yo‘l belgilarini tanib olish tizimlarida grafik protsessorlar yordamida avtomatik tanib olish uchun qo‘llash mumkin. Ushbu dasturiy vositalarni ishlab chiqishda zamonaviy sun’iy intellekt texnologiyalaridan, turli usullar, chuqur o‘qitishga asoslangan algoritmlar va yondashuvlardan keng foydalanildi. Yo‘l belgilarini dinamik tasvirlardan tanib oluvchi dasturiy majmuaning funksional tuzilishi quyidagi bosqichlarda amalga oshiriladi (1-rasm).

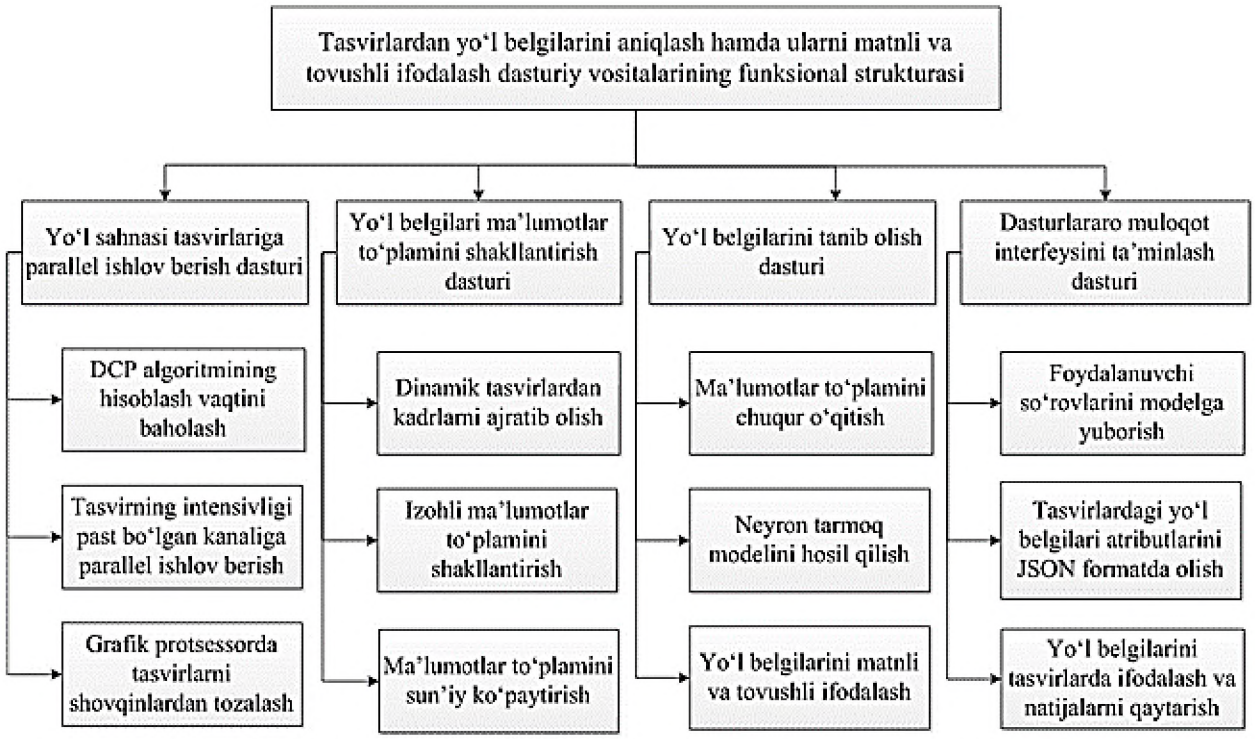
Yuqorida keltirilgan grafik protsessorlarda dinamik tasvirlardan yo‘l belgilarini aniqlovchi va sinflashtiruvchi dasturiy majmua vazifalarni bajarish jihatdan 4 ta asosiy qismdan iborat:

- Yo‘l sahnasi tasvirlariga parallel ishlov berish;
- Yo‘l belgilari ma’lumotlar to‘plamini shakllantirish;
- Yo‘l belgilarini tanib olish;
- Dasturlararo o‘zaro muloqotni ta’minlash.

Yo‘l sahnasi tasvirlariga parallel ishlov berish bosqichida DCP algoritmining hisoblash vaqtini baholash, Tasvirning intensivligi past bo‘lgan kanaliga parallel ishlov berish, grafik protsessorda tasvirlarni shovqinlardan tozalash jarayonlari amalga oshiriladi. Ushbu vazifalar keyingi bosqichlardagi yo‘l belgilari ma’lumotlar to‘plamini ishlab chiqish hamda yo‘l belgilarini dinamik tasvirlardan aniqlash darajasini oshirish uchun xizmat qiladi.

Yo‘l belgilari ma’lumotlar to‘plamini shakllantirish bosqichida dinamik tasvirlardan kadrlarni ajratib olish, izohli yo‘l belgilari ma’lumotlar to‘plamini shakllantirish, yo‘l belgilari ma’lumotlar

to‘plamini sun’iy ko‘paytirish jarayonlari amalga oshiriladi. Keyin bosqichda sun’iy intellekt texnologiyalarida yo‘l belgilari ma’lumotlar to‘plamidan foydalanish muhimdir.



1-rasm. Tasvirlardan yo‘l belgilarini aniqlash hamda ularni matnli va tovushli ifodalash dasturiy vositalarining funksional strukturasi

Yo‘l belgilarini tanib olish bosqichida ma’lumotlar to‘plamini chuqur o‘qitish, yo‘l belgilarini dinamik tasvirlardan tanib olish, aniqlangan ma’lumotlarni foydalanuvchiga vizual va tovushli ifodalash kabi muhim vazifalar bajariladi. Yo‘l belgilarining 56 ta sinfi ushbu tadqiqotda foydalanilgan bo‘lib, aniqlangan yo‘l belgilarini tasvirdagi joylashgan o‘rni koordinatalari, yo‘l belgisining nomi, tovushli hamda yo‘l belgining vizual tasviri ifodalanishi bilan jarayon yakunlanadi.

Dasturlararo o‘zaro muloqotni ta’minlash bosqichida foydalanuvchi so‘rovlarini modelga yuborish, tasvirlardagi yo‘l belgilari atributlarini JSON formatda olish, yo‘l belgilarini tasvirlarda ifodalash va olingan natijalarni veb ilovada tasvirlash amallarni bajaradi. Ishlab chiqilgan dasturiy majmuaning foydalanuvchi interfeysini ishlab chiqish, barcha sohalarga kirib borgan veb texnologiyalar bilan modelni integratsiyasini amalga oshirish vazifalari bajarilgan.

Yuqorida keltirilgan dasturiy vositalarni ishlab chiqishda, tadqiqot natijalarini olishda foydalanilgan texnik va dasturiy ta'minotlarning nomlari, parametrlari hamda talablari quyida berilgan:

- Kompyuter xarakteristikasi: CPU: AMDA Ryzen 7 U-5800, x64, 8x3.2 GHz; GPU: Nvidia Geforce 3050 RTX 4Gb, Tezkor xotira: 16 Gb, Doimiy xotira: 512 SSD va 1 Tb HDD.
- Operatsion tizim: Ubuntu 20.04; Windows 10 Pro, 64 razryadli.
- Dasturlash tillari: Python 3.8; C++.
- Texnologiyalar: OpenCV, CUDA, Tensorflow, Flask.

Yo'l sahnasi tasvirlariga parallel ishlov berish. Tasvirlarga dastlabki ishlov berish kompyuterli ko'rish masalalarida muhim qadam hisoblanib, turli yondashuvlarga ega. Yo'l sahnasi tasvirlaridan obyektlarni aniqlash masalasida turli ob-havo sharoitlarida tasvir yorqinligining pastligi yo'l belgilarini tanib olishni qiyinlashtiradi [1]. Ushbu tadqiqot ishida tasvirlarga parallel ishlov berish algoritmlarining samaradorligini baholash uchun CPU va GPU platformalarida turli tasvir o'lchamlari uchun ishlash vaqti solishtirildi (2-rasm).



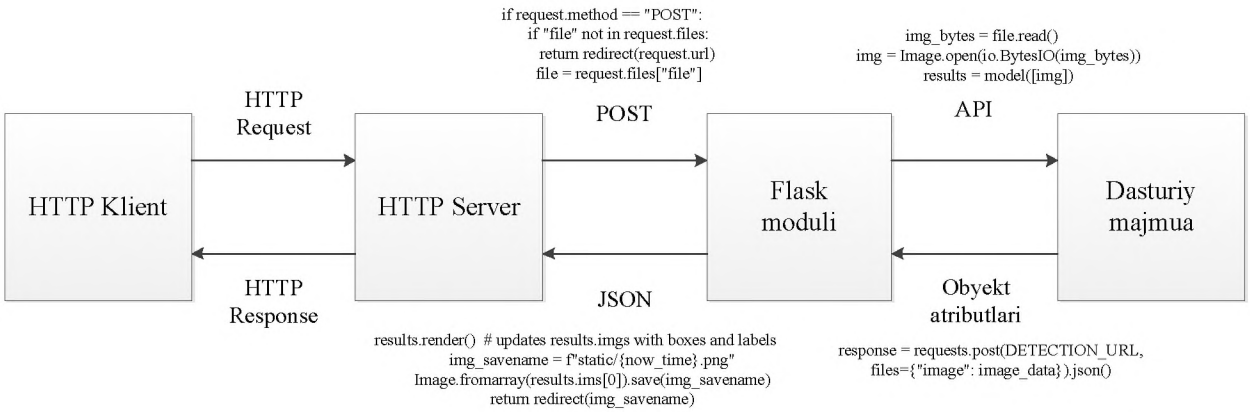
(a) (b)

2-rasm. Tasvirlarni shovqinlardan tozalash: (a) tumanli tasvir, (b) tumansiz tasviri

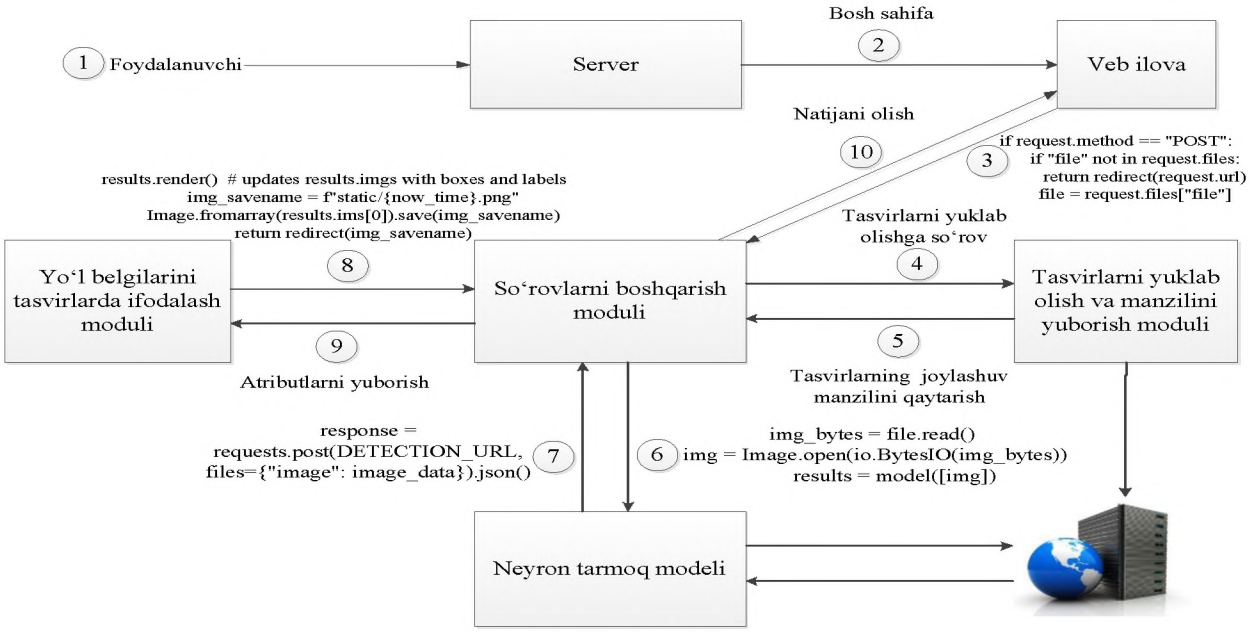
Haydovchilarga ma'lumotlarni matnli, ovozli va vizual yetkazish uchun har bir sinfga tegishli yo'l belgilarining nomlari keltirilgan matnli fayl, ushbu nomlarning ovozli fayllari (56 ta *.mp3 formatdagi fayllar, vaqti 1-4 soniya oralig'ida) va ularning vizual tasviri (56 ta *.jpg formatdagi rasmlar, o'lchami 50x50) oldindan ishlab chiqilgan. Dinamik tasviridan tanib olingan yo'l belgining matni videoning yuqori qismiga yoziladi, uning ovozli fayli yangi oqim yaratish orqali video oqim bilan bir vaqtda ovozli ma'lumotlar oqimi ham yaratiladi va haydovchiga xabar

beriladi. Yo‘l belgisining vizual tasviri tasvirlarni birlashtirish orqali dinamik tasvirning yuqori qismiga ifoda etiladi.

Dasturlararo o‘zaro muloqotni ta’minlash. Ishlab chiqilgan modellardan va dasturiy vositalardan keng foydalanish uchun veb ilova hamda foydalanuvchi interfeysi ishlab chiqildi. Foydalanuvchilardan kelgan so‘rovlarni qabul qilish hamda model bilan integratsiyani amalga oshirish, aniqlangan ma’lumotlarni qayta veb ilovaga yuborish jarayonlarini tashkil etuvchi dasturlararo muloqot interfeysi ishlab chiqildi. Ushbu veb ilova ma’lumotlar to‘plami hajmini ko‘paytirish uchun ham xizmat qiladi. Ma’lumotlarni uzatish va qabul qilish jarayoni quyida ko‘rsatilgan (3-rasm va 4-rasm).



3-rasm. Ma’lumotlarni uzatish va qabul qilishning umumiy sxemasi



4-rasm. Dasturlararo muloqot interfeysi

Tadqiqotlarni natijalarini baholash uchun turli metrikalardan foydalanildi. Chuqur o‘qitishga asoslangan algoritmlarda eng ko‘p qo‘llaniladigan usul bu Precision va Recall metrikalari hisoblanadi. Bunda to‘rtta asosiy ko‘rsatkichlar mavjud: TN (True Negative), FN (false Negative), TP (True Pozitive) va FP (False Pozitive) [2].

$$Precision = \frac{TP}{TP+FP} \quad (1)$$

$$Recall = \frac{TP}{TP+FN} \quad (2)$$

1-jadval.

Yo‘l belgilarini tanib olish bo‘yicha o‘tkazilgan tadqiqotlarda qo‘llanilgan modellar

Yo‘l belgilarini tanib olish bo‘yicha o‘tkazilgan tadqiqotlarda qo‘llanilgan modellar	Precision (aniqlik)
YOLOv5 + ShuffleNet-v2 + BIFPN + CA + EIOU (Haohao Zou)	92.5 %
Yolov5l + GSconv + PDCM + SCAM (Jie Hu)	89.2 %
Faster R-CNN + FPN + ROI Align + DCN (Xiang Gao)	86.5 %
YOLOv5+SK+TDI+C3 (Taklif etilgan)	**95.1 %**

Yuqoridagi natijalarni olishda foydalanilgan dasturiy va apparat vositalari ham muhim ahamiyatga ega, bunda ishlash vaqtini qisqartirishda hisoblash qurilmasining unumdorligiga bog‘liq. Dinamik tasvirlardan yo‘l belgilarini tanib olish tasvirning o‘lchami va sifatiga bevosita bog‘liqdir. Dasturiy majmuani ishlab chiqishda va tadqiqotni sinovdan o‘tkazishda quyidagi parametrli hisoblash qurilmasi, texnologiyalari foydalanildi (2-jadval).

2-jadval.

Tadqiqotni sinovdan o‘tkazishda foydalanilgan apparat va dasturiy vositalar

CPU: AMD Ryzen 7-5800H	OS: Ubuntu 20.04
GPU: NVIDIA Geforce RTX 3050Ti	PyTorch: 1.9
Memory: 16G	CUDA: 10.1
Python: 3.9	CUDNN: 7.4
Torch-vision: 0.9	YOLO: YOLOv5s
Compiler: Anaconda, Pycharm	Numpy: 1.18

Chuqur o‘qitish natijasida model 2 ta *.pt* kengaytmali vazn faylini saqlaydi. last.pt fayli oxirgi davrdagi vazn fayli va best.pt fayli eng yuqori aniqlikka erishgan davrdagi vazn faylidir [3, 4]. Ikkala fayl ham hajmi bir xil bo‘lib, 14 MB xotiradan joy oladi. Ishlab chiqilgan yo‘l belgilari ma’lumotlar to‘plami (UTSD) va neyron tarmoq arxitekturasi yordamida chuqur o‘qitish natijalari quyidagi 5-rasmlarda ko‘rsatilgan.



5-rasm. Chuqur o‘qitish natijalari

Tuman konsentratsiyasi yuqori tasvirlardagi kichik yo‘l belgilarini ham tanib olish orqali algoritmning ishonchligini ko‘rish mumkin. Ishlab chiqilgan Model CPU, GPU, CUDA, CUDNN, OpenCV, OpenMP va ularning kombinatsiyalaridan foydalangan holda tarmoqni kompilyatsiya qilish va ishga tushirish imkoniyatini beradi.

Ushbu ish yo‘l harakati xavfsizligida eng muhim inson omiliga qaratilgan bo‘lib, yo‘l harakati hodisalarini kamaytirish uchun xizmat qiladi. Ijtimoiy samaradorlik sifatida haydovchilarni tayyorlash maktablariga joriy qilish, iqtisodiy samara olish uchun yo‘l-transport hodisalarini oldini olish nazarda tutilgan.

Haydovchilarga 3 xil ko‘rinishda ma’lumotlar yetkaziladi:

- Yo‘l belgisining vizual tasvirini.
- Yo‘l belgisining matnli izohini.
- Yo‘l belgisining tovushli signalini.

Ishlab chiqilgan dasturiy majmua amaliy masalalarga tadbiq etish uchun joriy qilingan va quyidagi samaradorlikka erishilgan.

Ushbu ish bo‘yicha olib borilgan tadqiqotlar va ilmiy izlanishlar natijasi ma’lumotlar to‘plamlari, modellar, usullar, algoritmlar va ilmiy yondashuvlar o‘rganib chiqildi. Shuningdek, tadqiqot vazifalari va masalalarini bajarish jarayonida tegishli ilmiy yechimlar, model va algoritmlar ishlab chiqildi hamda mavjud usullar takomillashtirildi. Ushbu ilmiy yechimlar asosida grafik protsessorlarda tasvirlarga parallel ishlov berish, yo‘l belgilari ma’lumotlar to‘plamini ishlab chiqish, sun’iy intellekt texnologiyalaridan foydalanib yo‘l belgilarini tanib olish bo‘yicha bir nechta dasturiy vositalar yaratilib, dasturiy majmua ishlab chiqildi.

Foydalanilgan adabiyotlar:

1. Vittorio Mazzia, Aleem Khaliq, Francesco Salvetti, Marcello Chiaberge. Real-Time Apple Detection System using Embedded Systems with Hardware Accelerators: an Edge AI Application // Digital Object Identifier 10.1109/ACCESS.2017.doi. Volume 4, 2016.

2. Mukhiddinov M.N., Akmuradov B.U., Djuraev O.N. Robust Text Recognition for Uzbek Language in Natural Scene Images. International Conference on Information Science and Communications Technologies (ICISCT 2019). IEEE, 4-6 November 2019, Tashkent Uzbekistan.

3. Umarov M.A., Ramatov I.I. Yo‘l belgilarini aniqlash uchun qo‘shimcha konvolyutsion neyron tarmog‘iga ega YOLOv5 algoritmi // “Raqamli texnologiyalar: sohalarda amaliy joriy etishning yechimlari va

muammolari” Xalqaro ilmiy-texnik anjumani ma’ruzalar to‘plami. Toshkent-2022. -B. 126-129.

4. Vaibhavi Golgire. Traffic Sign Recognition using Machine Learning: A Review // International Journal of Engineering Research and Technology (IJERT), ISSN: 2278-0181, Vol. 10 Issue 05, May-2021.

OMMAVIY TARTIBSIZLIKLAR JARAYONIDA TOIFALANGAN OBYEKTLARNI HIMOYALASHNING ZAMONAVIY TEXNIK YECHIMLARI

Jalolov A.A.
Achilov F.B.
O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti
Axborot texnologiyalari kafedrasi o‘qituvchisi
O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti
O‘quv boshqarma boshlig‘i polkovnik,
t.f.f.d (PhD), dotsent.

Jahonda shiddat bilan o‘zgarayotgan notinch va murakkab vaziyat, turli mojarolar jonajon Vatanimiz xavfsizligini, el-yurtimizning osoyishta hayotini ta’minlash hamda mavjud tahdid va xatarlarga munosib javob berishga doim tayyor turishimizni taqozo etmoqda.

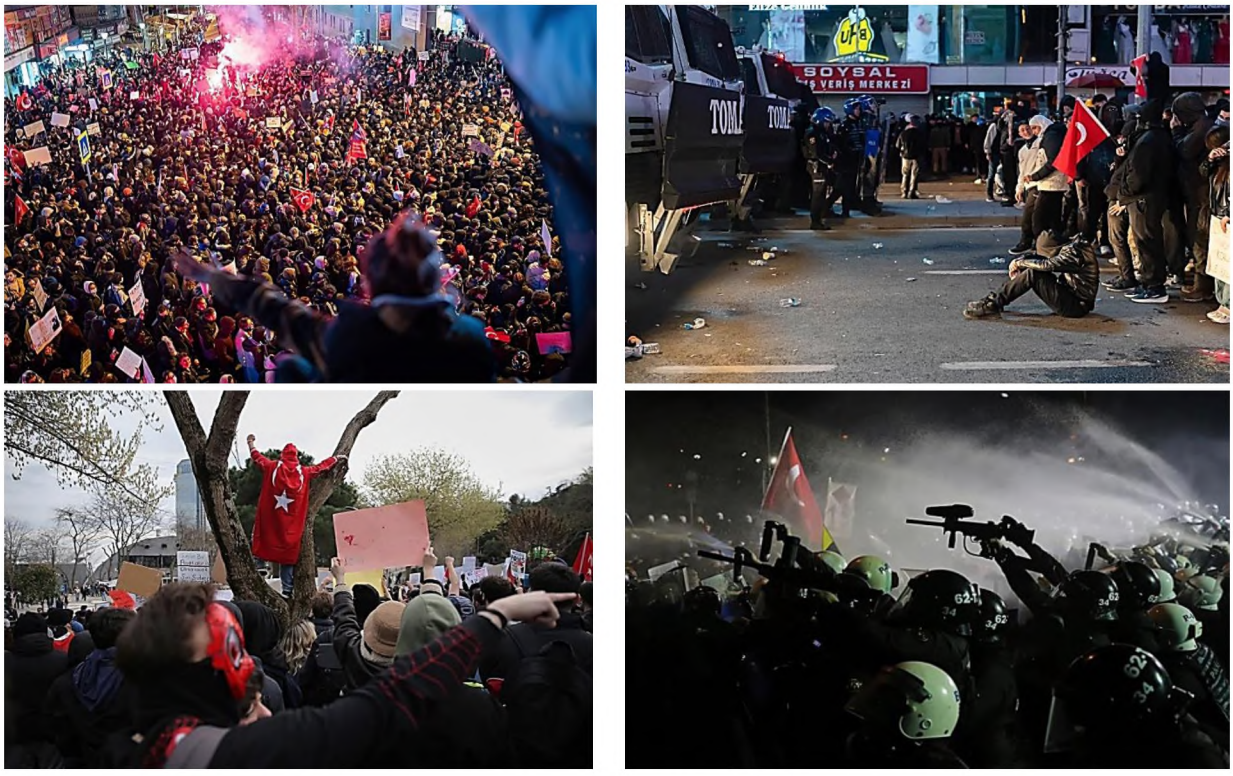
So‘ngi vaqtlarda dunyo miqyosida ommaviy tartibsizliklar, fuqarolarga nisbatan zo‘ravonlik va davlat obyektlariga keng ko‘lamda zarar yetkazish kabi hodisalar kuchayib bormoqda, xususan sodir bolayotgan ommaviy tartibsizliklar oqibatida fuqarolar va tadbirkorlarning mol-mulklari, davlat va ijtimoiy infratuzilmaga juda katta miqdorda zararlar yetkazilmoqda [3].

Bunday vaziyatda davlat ahamiyatiga ega obyektlarini, o‘ta muhim va toifalangan hamda boshqa obyektlarni, jismoniy va yuridik shaxslarning mol-mulkini qo‘riqlash va himoya qilish Milliy gvardiyaning eng asosiy vazifalaridan biri bo‘lib qolmoqda [1].

2025 yil 19 mart kuni Istanbul meri va Turkiyaning amaldagi prezidenti Rajab Toyyib Erdo‘g‘anning asosiy muxolifatchisi Akrom Imomo‘g‘li qo‘lga olingach, mamlakat bo‘ylab keng ko‘lamli norozilik

namoyishlari boshlanib ketdi. Imomo‘g‘lining qo‘lga olinishi Jumhuriyat xalq partiyasi qurultoyi arafasida ro‘y berdi, bu yig‘ilishda u partiyaning 2028 yilgi prezidentlik saylovlaridagi nomzodi sifatida ilgari surilishi kutilayotgandi. U bilan birga korrupsiyada gumonlarni o‘nlab safdoshlari ham ushlangan. Shundan buyon o‘n minglab turkiyaliklar o‘z noroziligini ifoda etish uchun ko‘chalarga chiqqan. Shu kunlarda Turkiyaning asosiy shaharlari ko‘chalari qanday ko‘rinishda ekanini aks ettiruvchi suratlar keltiriladi. Turkiyada so‘nggi yillardagi eng yirik namoyishlar - fotosuratlar

Qo‘lga olinganlar soni ikki mingga yaqinlashgan. Quyida Akrom Imomo‘g‘li hibsga olingach, Istanbul va Anqara ko‘chalari qanday ko‘rinishda ekanini aks ettiruvchi suratlar.



1 rasm. Turkiya ommaviy namoyishlar fotolavhalar

Nepal – Janubiy Osiyoda joylashgan, aholisi 30 millionga yaqin kichik davlat bo‘lib, Himolay tog‘ tizmalari bag‘rida joylashgan. Mamlakat iqtisodiyoti asosan qishloq xo‘jaligi, turizm va chet elda ishlayotgan fuqarolarning pul o‘tkazmalariga tayanadi, rivojlanishi sekin kechmoqda. Mamlakat ish o‘rinlari yetishmovchiligi, Hindiston va Xitoyga savdoda qaramlik kabi muammolarga duch kelmoqda.

Nepal hukumati joriy yilning 4 sentabr kuni ayrim messenjerlar va ijtimoiy tarmoqlar faoliyatiga cheklov joriy qilgan edi. 8 sentabr kuni Katmandu va boshqa yirik shaharlarda minglab namoyishchilar hukumat choralariga qarshi ommaviy norozilik namoyishlariga chiqdi. 9 sentabr kuni noroziliklar fonida hukumat ijtimoiy tarmoqlar faoliyatiga qo‘yilgan taqiqni olib tashladi.

Axborot agentliklariga ko‘ra, minglab namoyishchilar yetakchi partiyalar ofislari va ayrim siyosatchilarning uylarini buzib kirib, o‘t qo‘ygan. Namoyishchilar Nepal Kongressi partiyasi idorasi va bir qancha politsiya bo‘limlariga o‘t qo‘ydi.

Nepaldagi ommaviy norozilik namoyishlari “Z avlodi namoyishlari” deb nomlanadi. Politsiya bilan to‘qnashuvlarda kamida 51 kishi halok bo‘lgan, 1300 dan ortiq kishi jarohatlangan.



2 rasm. Nepal ommaviy namoyishlar

Mavjud ma’lumotlar tahliliga ko‘ra, davlat ahamiyatiga ega, o‘ta muhim va toifalangan obyektlarni, jismoniy, yuridik shaxslarni va ularning

mol-mulkini hamda davlat boshqaruvi organlari binolarini talofatlardan saqlash va himoya qilish mukammal emasligi salbiy ta'sir ko'rsatmoqda.

Shu bilan birga, qo'riqlash faoliyatiga zamonaviy qo'riqlash texnologiyalarini keng joriy etish orqali qo'riqlash xizmatining qamrovini yanada kengaytirish, xodimlarning kasbiy mahorati, bilim va ko'nikmalarini oshirish, shuningdek, sohada boshqaruv faoliyati samaradorligini ta'minlash bilan bog'liq tizimli muammolar saqlanib qolmoqda [2].

Dunyoning turli mintaqalarida sodir etilgan ommaviy tartibsizliklarni tahlil qilar ekanmiz [4], shunday xulosa chiqarish mumkinki davlat boshqaruvi organlarining ma'muriy binolari xavfsizligini ta'minlashning yagona standartlarini, ularning muhandislik-texnik himoya tizimini ishlab chiqish zarur.

Yuqoridagilarga asoslangan holda, toifalangan obyektlarda xavfsizlik tizimlarini tashkil qilishda Arduino platformasini va uning modullari imkoniyatlaridan foydalanish afzal ko'rinadi.

Xorijiy tajribalar, masalan, avtomatlashtirilgan xavfsizlik tizimlari, zirhli panjaralar, harakat va ovoz datchiklari yordamida himoya qilishni samarali yo'l sifatida ko'rsatmoqda. Fikrimizcha, Arduino platformasi asosida ishlab chiqilgan avtomatlashtirilgan tizimlar ushbu himoya vositalarini yanada takomillashtiradi.

Himoya tizimidagi tahdidlarni baholash va afzalliklarni tanlashda aniq turdagi obyektga, banklar, korxonalar, katta hajmli ofislar va boshqalarga nisbatan qo'riqlash faoliyatini tashkillashtirish bo'yicha xalqaro tajribalarni hisobga olish ahamiyatli hisoblanadi. Bu tajriba himoyaning zamonaviy texnik yechimlarni va normativ hujjatlarni tayyorlashda ham asos bo'lib xizmat qiladi.

Fikrimizcha, Arduino platformasi va uning modullari asosida quriladigan, ommaviy tartibsizliklarda tartibbuzarlarning g'ayriqonuniy harakatlari natijasida toifalangan obyektlarga yetkazilishi mumkin bo'lgan tajovuzlarni to'sib qoluvchi **avtomatlashtirilgan zirhli jalyuzini tezkor harakatga keltiruvchi qurilma**ni ishlab chiqish zarur.

Arduino Nano mikrokontrolleri va unga ulangan sensorlar, harakat, ovoz, vibratsiya va boshqa datchiklar yordamida obyektlarning xavfsizligini avtomatik tarzda monitoring qilish imkoniyatini beradi. Arduino platformasining afzalliklaridan biri - uning arzonligi va oson dasturlash imkoniyatidir. Ushbu platforma yordamida qurilgan tizimlar ma'lumotlarni qayta ishlash, uzatish va saqlash imkonini beradi, bu esa xavfsizlikni ta'minlashda muhim omil hisoblanadi. Ishlab chiqilgan qurilma Arduino platformasi bazasiga qurilgan bo'lib, uning dasturiy ta'minoti C++ dasturlash tilida yozilgan. Taklif etilayotgan qurilma o'zi va unga ulangan qurilmalari bilan ma'lumotlar almashadi, qurilmalardan kelayotgan ma'lumotlarni qayta ishlaydi, namoyon etadi, vaziyat bo'yicha holatni markaziy boshqaruv qismiga uzatadi va saqlab boradi.

Qurilma quyidagi elementlardan tashkil topgan:

1. Arduino NANO.
2. Harakat datchigi HC-SR501.
3. Ovoz datchigi lm393.
4. Vibratsiya datchigi.
5. LED RGB.
6. Ovozli indicator.
7. Rele.
8. Batareya.
9. LCD display I2C modulli.

Arduino Nano - bu ATmega328 (Arduino Nano 3.x) yoki Atmega168 (Arduino Nano 2.x) mikrokontrolleri atrofida qurilgan kichik, to'liq xususiyatli, u Arduino Duemilanove bilan bir xil funksionallikka ega, ammo kichikroq. Bu faqat quvvat ulagichi yo'qligida farq qiladi va mini-USB orqali ishlaydi. Arduino Nano Gravitech tomonidan ishlab chiqilgan (3-rasm). Asosiy vazifasi avtomatlashtirish va boshqarishda, turli modul va platalar bilan birikkan holda integrallashgan qurilmalarni ishlab chiqarish.



3-rasm. ATmega 168 Arduino Nano

Avtomatlashtirilgan zirhli jalyuzini tezkor harakatga keltiruvchi qurilmadan kelayotgan ma'lumotlarni qayta ishlash, namoyon etish, vaziyat bo'yicha holatni markaziy boshqaruv qismiga uzatish va saqlash imkonini beruvchi **birlashtiruvchi dasturni** ham yaratish maqsadga muvofiq deb hisoblaymiz. Bunda tartibbuzarning harakatini aniqlash tamoyili asosida qurilmaning ishga tushish vaqtini minimallashtirishga erishildi.

Zirhli jalyuzilar yuqori darajadagi himoyani ta'minlaydigan tizimlar bo'lib, ular uylar, ofislar, tijorat binolari va boshqa toifalangan obyektlar uchun samarali yechim bo'lishi mumkin. Ushbu qurilmalar orqali tashqi hujumlarga qarshi chidamlilikni oshirish mumkin. Zirhli jalyuzilar nafaqat jismoniy hujumlardan himoya qiladi, balki tezkor javob tizimlari orqali xavfsizlikni ta'minlaydi.

Zirhli jalyuzilar yuqori darajada himoyalangan rolikli panjaralardir. Ushbu rolikli jalyuzilar uylar, ofislar va tijorat binolarini himoya qilish uchun ishlatilishi mumkin (4-rasm).



4-rasm. Zirhli (o'q o'tkazmaydigan) jalyuzilar

Ilmiy jihatdan mazkur qurilmalardan foydalanish bir necha omillarga asoslanishi mumkin:

Tahdidni baholash: Bino va uning aholisi bilan bog‘liq xavf darajasini aniqlash uchun tahdidni baholash o‘tkazilishi mumkin. Baholash natijalariga ko‘ra, zirhli avtomatlashtirilgan qurilmalarni o‘rnatishni o‘z ichiga olgan xavfsizlik choralarini amalga oshirish mumkin.

Jinoiy statistika: Jinoiy faoliyat, shu jumladan buzish va vandalizm statistikasi zirhli avtomatlashtirilgan qurilmalarga bo‘lgan ehtiyojni tasdiqlovchi ilmiy dalillarni taqdim etishi mumkin. Misol uchun, agar statistik ma’lumotlar hududda buzilish holatlarining yuqoriligini ko‘rsatsa, ushbu qurilmalardan foydalanish zaruriy xavfsizlik chorasi sifatida oqlanishi mumkin.

Sinov va baholash: Zirhli avtomatlashtirilgan qurilmalar turli xil hujumlardan himoyalanish samaradorligini aniqlash uchun sinovdan o‘tkazilishi va baholanishi mumkin. Bu qurilmalarni bolg‘a, tirgak va o‘qotar qurollar kabi hujumlarda ishlatiladigan turli xil asboblar va qurollarga qarshi sinovdan o‘tkazishni o‘z ichiga olishi mumkin.

Qiyosiy tahlil: Muayyan bino yoki vaziyat uchun eng mos chora-tadbirlarni aniqlash uchun turli xil xavfsizlik choralarining samaradorligini qiyosiy tahlil qilish mumkin. Tahlil xarajatlar, samaradorlik va amalga oshirish qulayligi kabi omillarni hisobga olishi mumkin.

Ekspert xulosasi: Zirhli avtomatlashtirilgan qurilmalardan foydalanishni ilmiy asoslash uchun xavfsizlik mutaxassislari, muhandislar va boshqa mutaxassislardan ekspert xulosasini olish mumkin. Ushbu mutaxassislar bino bilan bog‘liq xavf va zaifliklar haqida ma’lumot berishi va tegishli xavfsizlik choralarini, jumladan, ushbu qurilmalardan foydalanishni tavsiya qilishi mumkin.

Umuman olganda, toifalangan obyektlarning deraza qismlarida zirxli avtomatlashtirilgan qurilmalardan foydalanishning ilmiy asoslanishi tahdidlarni baholash, jinoiy statistika, sinov va baholash, qiyosiy tahlil va ekspert xulosasi kombinatsiyasiga asoslanadi. Ushbu qurilmalardan foydalanish bino va uning aholisini turli xil hujumlardan himoya qilish uchun zarur xavfsizlik chorasi sifatida oqlanishi mumkin.

Toifalangan obyektlarni himoya qilishda zamonaviy texnik yechimlarni, xususan, Arduino platformasi asosida quriladigan avtomatlashtirilgan tizimlarni joriy etish, xavfsizlikni yuqori darajada ta'minlash imkonini beradi. Xavf-xatarlarni baholash, jinoiy statistikalar va ekspert xulosalariga asoslangan holda, ushbu texnologiyalarni qo'llash obyektlar xavfsizligini samarali tarzda oshiradi. Xorijiy tajriba, shuningdek, O'zbekiston uchun zamonaviy xavfsizlik tizimlarini joriy etish zaruratini ta'kidlaydi. Bu tizimlar nafaqat jinoiy faoliyatning oldini olish, balki xalqaro bozorda raqobatbardosh mahsulotlarni taqdim etish imkonini beradi.

Foydalangan adabiyotlar:

1. O'zbekiston Respublikasining 2020-yil 18-noyabrdagi "O'zbekiston Respublikasi Milliy gvardiyasi to'g'risida"gi O'RQ-647-son Qonuni. Qonun hujjatlari ma'lumotlari milliy bazasi, 19.11.2020 y., 03/20/647/1569-son; Qonunchilik ma'lumotlari milliy bazasi, 18.05.2022 y., 03/22/770/0424-son; 07.06.2022 y., 03/22/775/0477-son.

2. O'zbekiston Respublikasi Prezidentining 2021-yil 20-fevraldagi "O'zbekiston Respublikasi Milliy gvardiyasi Qo'riqlash bosh boshqarmasining faoliyatini sifat jihatidan yangi bosqichga ko'tarish chora-tadbirlari to'g'risida"gi PQ-4997-son qarori. Qonun hujjatlari ma'lumotlari milliy bazasi, 20.02.2021 y., 07/21/4997/0131-son; Qonunchilik ma'lumotlari milliy bazasi, 28.08.2021 y., 07/21/5235/0840-son.

3. O'zbekiston Respublikasi Prezidenti Sh.M. Mirziyoevning 2018-yil 11-yanvardagi Xavfsizlik kengashining kengaytirilgan tarkibdagi majlisidagi nutqi.

4. Achilov F.B., Jalolov A.A. Davlat boshqaruvi organlarining ma'muriy binolariga sodir etilgan tajovuzlarning tahlili va ularni oldini olish yo'llari // "Obyektlarni muhandis-texnik qo'riqlash vositalari bilan jihozlanishidagi muammolar va ularning yechimlari" mavzusidagi respublika ilmiy konferensiyasi materiallari to'plami. O'R Qurolli Kuchlari Akademiyasi. T.: 2022 yil. 36-39 b.

AVTOMATLASHTIRILGAN ALOQA TIZIMLARI VA ULARNING KIBERHUJUMLARGA BARQARORLIGI

Telmonov J.J.
Xatamov B.B.
O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti,
373-o‘quv guruhi kursanti
O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti, kafedra
boshlig‘ining o‘rinbosari, t.f.f.d. (PhD)

Avtomatlashtirilgan aloqa tizimlari (AAT) harbiy infratuzilmada muhim o‘rin egallaydi hamda qo‘shinlarni boshqarishning turli darajalari o‘rtasida ishonchli axborot almashinuvini ta’minlaydi. Ular qo‘shinlarni boshqarishda, jangovar harakatlarni muvofiqlashtirishda va real vaqt rejimida axborot almashinuvida asosiy rol o‘ynaydi. Raqamli texnologiyalarning rivojlanishi va jangovar harakatlarning tarmoq markaziga asoslangan konsepsiyalariga o‘tish AAT orqali uzatilayotgan ma’lumotlar hajmini sezilarli darajada oshirdi, bu esa ularni zamonaviy qo‘mondonlikning asosiy elementi qilib qo‘ymoqda [1]. Biroq yuqori darajadagi raqamlashtirish kiberhujumlar xavfi bilan birga kechadi, ular boshqaruv tizimlarining faoliyatini izdan chiqarishi mumkin.

Bundan tashqari, bugungi kunda AATning faoliyati jiddiy muammo – qasddan yoki tasodifiy paydo bo‘ladigan halaqitlar ta’siri bilan to‘qnash kelmoqda. An’anaviy himoya usullari (signalni filtrlash, adaptiv modulyatsiya, chastotani o‘zgartirish) asta-sekin talab qilinadigan barqarorlik darajasini ta’minlay olmayapti.

So‘nggi vaqtlarda yuqoridagi tahdidlarga qarshi kurashishda sun’iy intellekt va mashinali o‘qitish usullari tobora ko‘proq qo‘llanilmoqda, ular tizim ishini buzilishidan avvalroq hujumlarni aniqlash va ularga javob qaytarish imkonini beradi.

AAT ovozli ma’lumotlar, videotasvirlar va ma’lumotlarning himoyalangan uzatilishini, turli aloqa turlari (radio, sun’iy yo‘ldosh, optik tolali) integratsiyasini, qo‘mondon va shtablar uchun yagona axborot makonini shakllantirishni, qo‘shinlarni boshqarish tizimlari, razvedka va logistika platformalari bilan o‘zaro hamkorlikni ta’minlaydi [2].

Ushbu xususiyatlar AATni nafaqat tanqidiy muhim, balki axborot infratuzilmasining eng zaif bo‘g‘ini ham qilib qo‘yadi.

AAT uchun kiberxavflar haqida gapirganda, quyidagi turlarini qayd etish mumkin:

1. **Ruxsatsiz kirish.** Aloqa tugunlarining buzilishi dushmanga uzatilayotgan operativ ma’lumotlarni qo‘lga kiritish yoki ularni o‘zgartirish imkonini beradi;

2. **«Xizmat ko‘rsatishni rad etish» (DoS/DDoS) hujumlari.** Sun’iy trafik orqali aloqa kanallarining ortiqcha yuklanishi qo‘shinlar ustidan boshqaruvning yo‘qolishiga olib keladi;

3. **Zararli dasturiy ta’minot.** Viruslar va «trojan» dasturlarining kiritilishi tarmoqning asosiy tugunlarini ishdan chiqarishi mumkin;

4. **Ma’lumotlar bilan manipulyatsiya.** Xabarlarni almashtirish yoki ma’lumotlarni buzib ko‘rsatish qo‘mondonlik tomonidan noto‘g‘ri qarorlar qabul qilinishiga sabab bo‘lishi mumkin;

5. **Ta’minot zanjiri orqali hujumlar.** Qurilma va dasturiy ta’minot ishlab chiqarish bosqichida joylashtirilgan zaifliklar butun tizim xavfsizligiga tahdid soladi [3].

AATning kiberhujumlarga qarshi barqarorligini oshirish bo‘yicha standart tashkiliy-texnik usullar quyidagilardan iborat:

- **kriptografik himoya,** ya’ni hujumlarga chidamli shifrlash algoritmlaridan foydalanish, ko‘p bosqichli autentifikatsiyani qo‘llash, ma’lumotlarni aloqa kanallarida va saqlashda shifrlash;
- **tarmoqlarni segmentlash va zaxiralash,** ya’ni tanqidiy va yordamchi tizimlarni ajratish, zaxira aloqa kanallarini yaratish, foydalanuvchilar uchun «minimal imtiyozlar» prinsipini qo‘llash;
- **aloqa tarmoqlarini monitoring qilish,** ya’ni buzilishlarni aniqlash va oldini olish tizimlarini (masalan, Intrusion Detection/Prevention Systems) joriy etish, aloqa trafikidagi anomaliyalarni tahlil qilish, tarmoq faoliyatini 24/7 monitoring qilish;
- **tashkiliy choralar,** ya’ni kiberxavfsizlik sohasida mutaxassislar tayyorlash, kiberhujumlarni qaytarish bo‘yicha mashg‘ulotlar o‘tkazish, shuningdek, maxsus kiberbo‘linmalarni tashkil etish [4].

Sun’iy intellekt va mashinali o‘qitishdan foydalanish AATning kiberhujumlarga barqarorligini ta’minlashda katta ahamiyat kasb etadi. Bu yondashuv katta ma’lumotlarni tahlil qilish asosida hujumlarni prognozlash, yangi zararli patterlarni avtomatik aniqlash, o‘z-o‘zidan moslasha oladigan adaptiv himoya tizimlarini yaratishga imkon beradi.

Masalan, AQShda **DARPA Cyber Grand Challenge** dasturi doirasida aloqa tarmoqlarining barqarorligini oshirish uchun sun’iy intellektdan foydalanish faol tadqiq qilinmoqda. NATO mamlakatlarida DoS-hujumlarni aniqlash maqsadida avtomatlashtirilgan aloqa tizimlariga integratsiya qilinadigan intellektual monitoring tizimlari qo‘llaniladi. Rossiyada esa radioelektron bostirishga qarshi kurashish uchun radiochastota spektrini tahlil qilish vositalari o‘rnatilgan himoyalangan **SDR-radiostansiyalar**ni sun’iy intellekt asosida ishlab chiqish ishlari olib borilmoqda.

Sun’iy intellekt va mashinali o‘qitish AATda quyidagi maqsadlarda qo‘llaniladi:

- **anomaliyalarni aniqlash** – mashinali o‘qitish algoritmlari tarmoq trafigini tahlil qilib, normal xatti-harakatdan og‘ishlarni aniqlaydi (masalan, DDoS-hujum paytidagi faollikning keskin ortishi);
- **hujumlarni bashorat qilish** – modellar avvalgi hodisalar asosida potensial tahdidlarni oldindan prognoz qiladi;
- **trafikni adaptiv filtrlash** – intellektual tizimlar shubhali ulanishlarni dinamik tarzda bloklaydi;
- **javob choralarini avtomatlashtirish** – sun’iy intellekt yordamida «aniqlash – qaror – harakat» sikli qisqaradi;
- **kriptografik himoyani mustahkamlash** – neyrotarmoqlardan barqaror kalitlarni yaratishda va shifrlashdagi zaifliklarni tahlil qilishda foydalaniladi.

AATning barqarorligini ta’minlashda mashinali o‘qitishning asosiy usullariga quyidagilar kiradi:

1. **Hujumlarni klassifikatsiya qilish** – SVM, qaror daraxtlari va neyron tarmoqlar algoritmlaridan hujum turlarini aniqlash uchun foydalanish;

2. **Trafikni klasterizatsiya qilish** – shubhali paketlar guruhlarini ajratib olish (masalan, K-Means, DBSCAN);

3. **Chuqur o‘qitish (DL)** – katta hajmdagi tarmoq ma’lumot oqimlarini tahlil qilish uchun rekurrent va konvolyutsion neyron tarmoqlardan foydalanish;

4. **Onlayn-o‘qitish (online learning)** – modellarning real vaqt rejimida yangi tahdidlarga moslashuvi;

5. **Ansambl metodlari (Random Forest, Gradient Boosting)** – bir nechta modellarni birlashtirish orqali hujumlarni aniqlash aniqligini oshirish.

Bundan tashqari, zamonaviy mojarolarda AATning **shovqinga bardoshliligi** alohida ahamiyat kasb etmoqda.

Shovqinga bardoshlilik – bu AATning turli xil shovqinlar ta’sirida (tabiiy – atmosfera razryadlari, quyosh faolligi; sun’iy – radioelektron bostirish, kiberhujumlar, elektromagnit impulslari) ham ma’lumot uzatishni maqbul xatolik darajasida ta’minlash qobiliyatidir.

Shovqinga bardoshlilikni oshirishning asosiy usullari:

- **apparat usullari** – elektromagnit nurlanishlardan himoyalovchi filtrlardan va ekranlashdan foydalanish, yo‘naltirilgan nurlanishli antennalardan foydalanish (signal bostirilishi ehtimolini kamaytiradi), aloqa kanallarini zaxiralash;
- **dasturiy-algoritmik usullar** – xatoliklarni tuzatish (masalan, Xemming, Rid–Solomon kodlari, turbo-kodlar, LDPC), ishchi chastotalarni qayta sozlash (FHSS – *Frequency Hopping Spread Spectrum*), keng polosali modulyatsiya (DSSS – *Direct Sequence Spread Spectrum*);
- **tashkiliy-texnik choralar** – zaxira kanallarga avtomatik o‘tuvchi tarmoqlarni qurish, qayta uzatish mexanizmlariga ega tarmoq protokollaridan foydalanish (ARQ), yuklamani bir nechta tarmoq tugunlari orasida taqsimlash.

Sun’iy intellekt va mashinali o‘qitishdan foydalanish statik shovqinlarga qarshi kurash usullaridan **adaptiv himoya tizimlariga** o‘tishga imkon beradi. Bunday tizimlar ish parametrlarini mavjud

sharoitga qarab mustaqil ravishda o‘zgartira oladi. Ularning asosiy yo‘nalishlari quyidagilardan iborat:

- **adaptiv signal filtrlash** – shovqin fonida foydali signalni ajratib olish uchun neyrotarmoq algoritmlaridan foydalanish;
- **chastota spektrini intellektual boshqarish** – ishchi chastotalarni dinamik qayta sozlash va shovqin ehtimolini oldindan bashorat qilish;
- **shovqin manbalarini avtomatik aniqlash** – mashinali o‘qitish usullari yordamida nurlanish manbalarini klassifikatsiya qilish va joylashuvini aniqlash;
- **tarmoqlarda marshrutizatsiyani optimallashtirish** – eng kam shovqin darajasiga ega aloqa kanallarini intellektual tanlash;
- **shovqinli muhitni bashorat qilish** – aloqa parametrlarini oldindan o‘zgartirish uchun prognozlash modellari qo‘llanilishi.

Qurolli Kuchlar uchun **AATning shovqinga bardoshliligi** nihoyatda muhimdir, chunki u qo‘shinlarni boshqarishni faol radioelektron qarshilik sharoitida ham ta’minlaydi, boshqaruv tizimining yashovchanligini oshiradi, ma’lumotlarning yo‘qolishi va buzilish xavfini kamaytiradi, tarmoqmarkaziy urushlar sharoitida ishonchlilikni kafolatlaydi.

Xulosa. Avtomatlashtirilgan aloqa tizimlari harbiy infratuzilma va qo‘shinlarni boshqarishning tanqidiy muhim elementi hisoblanadi. Ularning kiberhujumlarga nisbatan zaifligi barqarorlikni ta’minlashda texnologik hamda tashkiliy choralarni o‘z ichiga olgan kompleks yondashuvni talab etadi. Kriptografiya, IDS/IPS, sun’iy intellekt va zaxira aloqa kanallaridan foydalanish AAT ishonchliligini sezilarli darajada oshirish imkonini beradi. Zamonaviy sharoitda ishonchli kiberxavfsizlik avtomatlashtirilgan aloqa tizimlarining ajralmas komponenti sifatida qaralishi lozim.

Sun’iy intellekt va mashinali o‘qitish avtomatlashtirilgan aloqa tizimlarining kiberhujumlarga barqarorligini ta’minlashda eng muhim vositalardan biriga aylanmoqda. Ular nafaqat tahdidlarni tezkor aniqlash, balki yangi hujum vektorlarini bashorat qilish, javob berish jarayonlarini avtomatlashtirish va harbiy tarmoqlarning ishonchliligini oshirish imkonini beradi. Kelajakdagi tarmoqmarkaziy urushlar sharoitida aynan

intellektual himoya tizimlari avtomatlashtirilgan aloqa tizimlarining yashovchanligi va samaradorligini belgilovchi omilga aylanadi.

Sun'iy intellekt va mashinali o'qitish AATning shovqinga bardoshliligini oshirish uchun yangi imkoniyatlarni ochadi. Ularning qo'llanilishi hisobiga shovqinli va imitatsion signallarni samarali bostirish, aloqa kanallarini adaptiv qayta sozlash, shovqinli vaziyatni avtomatik bashorat qilish, dushman ta'siriga javob berish vaqtini qisqartirishga erishiladi. Kelajakdagi tarmoqmarkaziy urushlar sharoitida aynan shovqinlarga qarshi intellektual algoritmlar harbiy aloqa tizimlarining ishonchliligini ta'minlashning asosiy omiliga aylanadi.

Foydalanilgan adabiyotlar:

1. Alberts D. S., Garstka J. J., Stein F. Network Centric Warfare: Developing and Leveraging Information Superiority. CCRP, 1999.

2. Коваленко В. И. Автоматизированные системы связи: современное состояние и перспективы развития // Вестник связи. – 2020. – №4. – С. 15–22.

3. Кулагин А. А. Киберугрозы военным системам связи и методы их предотвращения // Информационная безопасность. – 2021. – №2. – С. 45–53.

4. NATO Cooperative Cyber Defence Centre of Excellence. Cyber Defence in Military Communications. Tallinn, 2019.

5. DARPA. Cyber Grand Challenge. https://www.darpa.mil.

PORTLOVCHI QURILMALARNI ZARARSIZLANTIRISHDA MASOFADAN BOSHQARILADIGAN YER USTI TRANSPORT VOSITALARIDAN VIDEOOQIMLARNI UZATISH TAHLILI

Tashmanov Y.B

O'R IIV akademiyasi katta o'qituvchisi, t.f.d. (DSc), dotsent

Zamonaviy xavfsizlik tizimlarida portlovchi qurilmalarni aniqlash va ularni zararsizlantirish masalasi jamiyat xavfsizligi uchun eng dolzarb yo'nalishlardan biri hisoblanadi. Terrorizm, harbiy nizolar va noqonuniy harakatlar natijasida yuzaga keladigan portlovchi qurilmalar odamlar hayoti va infratuzilma barqarorligi uchun jiddiy tahdid tug'diradi. Shu bois,

inson hayoti uchun yuqori xavf tug‘diradigan vazifalarda masofadan boshqariladigan yer usti transport vositalari keng qo‘llanilmoqda.

Masofadan boshqariladigan yer usti transport vositalari xavfli hududlarda insonning bevosita ishtirokini minimal darajaga tushirish, masofadan turib aniq manipulyatsiyalar bajarish va portlovchi qurilmalarni zararsizlantirish imkoniyatini yaratadi. Bunday vositalarning samaradorligi ko‘p jihatdan ularga o‘rnatilgan videokuzatuv tizimlariga bog‘liq bo‘lib, videoma’lumotlar orqali operator real vaqtda vaziyatni baholash, obyektlarni aniqlash va tegishli qarorlar qabul qilish imkoniyatiga ega bo‘ladi.

Videokuzatuv tizimlari nafaqat ko‘rish qobiliyatini oshiradi, balki xavfli obyektlarni avtomatik ravishda aniqlash va tahlil qilish imkonini ham beradi. Masalan, kameralar yuqori aniqlikdagi tasvir uzatish orqali portlovchi qurilmaning tashqi ko‘rinishi, uning atrofidagi muhit va ehtimoliy xavf omillarini tezkor baholashga yordam beradi.

Videoma’lumotlarni uzatishda zamonaviy axborot-kommunikatsiya texnologiyalari, jumladan Wi-Fi tarmoqlari va mobil aloqa (3G/4G/5G) kanallaridan foydalanish muhim ahamiyatga ega. Bu yechim videotasvirlarni uzluksiz ravishda, real vaqtda operator pultiga yetkazish imkonini berib, xavfli hududdagi vaziyatni tezkor baholashga xizmat qiladi. Shu bilan birga, kanal sig‘imi va aloqa barqarorligi videotasvir sifatini belgilovchi asosiy omillardan biri hisoblanadi.

Portlovchi qurilmalarni zararsizlantirish jarayonida masofadan boshqariluvchi transport vositalarida videoma’lumotlarni uzatish kanali asosiy ahamiyatga ega. Chunki operatorning vaziyatni baholashi, tezkor qaror qabul qilishi va xavfsizlik darajasini ta’minlashi videotasvir sifati hamda uzatishdagi barqarorlikka bog‘liqdir. Bunda asosan Wi-Fi texnologiyasi va mobil aloqa (3G/4G/5G) tarmoqlari qo‘llaniladi. Ularning afzallik va cheklovlarini qiyosiy tahlil qilish muhimdir.

Wi-Fi orqali uzatish

Afzalliklari:

- Yuqori ma’lumot uzatish tezligi (teoriyada 300 Mbit/s va undan yuqori).

qisqa masofada (100–300 metrgacha) barqaror va yuqori sifatli videotasvir;

Internet tarmog‘idan mustaqil ishlashi mumkin (lokal aloqa) qurilmalarda arzon va keng tarqalgan texnologiya.

Cheklovlari:

masofa cheklangan bo‘lib, yopiq muhitlarda signal kuchsizlanishi yoki yo‘qolishi mumkin;

elektromagnit to‘siqlar ta’sirida uzilish ehtimoli yuqori;

himoya darajasi yetarli ta’minlanmasa, noqonuniy to‘sqinlikka uchrashi mumkin;

mobil aloqa orqali uzatish (3G/4G/5G).

Afzalliklari:

masofa cheklanmagan (operator qamrovi bo‘yicha);

zamonaviy 4G va ayniqsa 5G tarmoqlarida yuqori tezlik (1 Gbit/s gacha) va past kechikish (10 ms atrofida);

harakatlanuvchi obyektlar uchun qulay – signal qamrovi doirasida videotasvir uzatish barqaror;

qo‘shimcha xizmatlar bilan integratsiya qilish imkoniyati (bulutli serverda saqlash, masofaviy monitoring markaziga uzatish).

Cheklovlari:

tarmoq operatorining qamrov hududi va infratuzilmasiga bog‘liq;

harbiy yoki favqulodda holatlarda mobil tarmoq ish faoliyati cheklanishi mumkin;

qo‘shimcha ekspluatatsiya xarajatlari (SIM-karta, tarif rejalari);

kiberxavfsizlik nuqtai nazaridan Wi-Figa nisbatan ko‘proq tahdidlarga ochiq (masalan, tarmoq trafikini to‘sib olish).

Xulosa o‘rnida shuni aytish mumkinki, qisqa masofada va lokal hududlarda (masalan, yopiq binolar yoki maxsus poligonlar) Wi-Fi tarmog‘i samarali va arzon yechim hisoblanadi.

Uzak masofada, harakatchan obyektlar bilan ishlashda va markaziy serverga uzatish zarur bo‘lganda mobil aloqa tarmoqlari (ayniqsa 5G) samaradorligi yuqori.

Amaliy sharoitlarda ko‘p hollarda gibrid yechim qo‘llaniladi, ya’ni Wi-Fi lokal tarmoqda, mobil aloqa esa zaxira kanali sifatida xizmat qiladi.

Foydalanilgan adabiyotlar:

1. Гонсалес Р., Вудс Р. Цифровая обработка изображений. – М.: Техносфера, 2005. – 1072 с.

2. Дворкович А.В., Дворкович В.П. Цифровые видеоинформационные системы (теория и практика). – М.: Техносфера, 2012.

3. Fette, I., Melnikov, A. The WebSocket Protocol. RFC 6455, IETF, 2011.

4.Iqbal, M., Nadeem, M. Real-time video surveillance using WebSocket protocol. International Journal of Computer Applications, 2020.

5.Zhang, H., Wang, L. Intelligent Traffic Monitoring Based on Video Profiling and WebSocket Communication. IEEE Access, 2021.

RAQAMLI TEXNOLOGIYALAR ASOSIDA PROFESSOR-O‘QITUVCHILARNING SAMARADORLIGINI SMART REYTING TIZIMI ORQALI BAHOLASH

Abdiraximov A.A.
IIV Malaka oshirish instituti, Axborot texnologiyalari sikli o‘qituvchisi, katta leytenant

So‘nggi yillarda ta’lim tizimida zamonaviy texnologiyalar rivojlanishi natijasida raqamli transformatsiya jarayonlari tobora jadallashib bormoqda. Raqamli texnologiyalarining keng qo‘llanilishi, masofaviy ta’lim shakllarining rivojlanishi va onlayn platformalarning joriy etilishi professor-o‘qituvchidan yangi turdagi kompetensiyalarni talab qilmoqda.

Xususan, professor-o‘qituvchilarining raqamli ko‘nikmalari nafaqat dars unumdorligiga, balki ta’lim sifatiga ham bevosita ta’sir ko‘rsatadi. Shu bois ta’lim jarayonida professor-o‘qituvchilarining kasbiy faoliyatini aniq mezonlar asosida baholash dolzarb masalaga aylanmoqda. An’anaviy baholash shakllari professor-o‘qituvchilarining faoliyatini to‘liq qamrab

ololmaydi, chunki ular ko‘proq statistik ko‘rsatkichlar va formal yondashuvlarga tayangan holda amalga oshiriladi.

Bunday holatda professor-o‘qituvchilarining raqamli vositalardan foydalanish darajasi, innovatsion metodlarni qo‘llash qobiliyati va pedagogik yondashuvligi e’tibordan chetda qolishi mumkin. Shuning uchun zamonaviy baholash mexanizmlaridan biri sifatida Ichki ishlar vazirligi Malaka oshirish instituti professor-o‘qituvchilarining smart reyting avtomatlashtirilgan elektron reyting axborot tizimi amaliy sinov tariqasida joriy etildi.

Professor-o‘qituvchilar – fakultet va kafedra (sikl) boshliqlari, o‘rinbosarlari, professor, dotsent, katta o‘qituvchi, o‘qituvchi, o‘qituvchi-murabbiy lavozimida ishlayotgan xodimlardir.

Smart reyting tizimi – bu professor-o‘qituvchilarining kasbiy faoliyatini raqamli texnologiyalar asosida, aniq ko‘rsatkichlar (KPI) orqali baholash imkonini beradigan avtomatlashtirilgan dasturiy ta’minot mexanizmi hisoblanadi. Ushbu tizim yordamida professor-o‘qituvchilar faoliyatining turli jihatlari dars jarayonida raqamli texnologiyalardan foydalanish, tinglovchilar bilan interaktiv ishlash samaradorligi, ilmiy-uslubiy faoliyatdagi faolligi va doimiy professional rivojlanishga intilishi kompleks tarzda tahlil qilinadi.

Ushbu tizim quyidagi jihatlarni baholash imkonini beradi:

– Raqamli vositalardan foydalanish samaradorligi;
– Pedagogik innovatsiya va interaktiv yondashuv qobiliyati;
– Kasbiy rivojlanishdagi faollik.

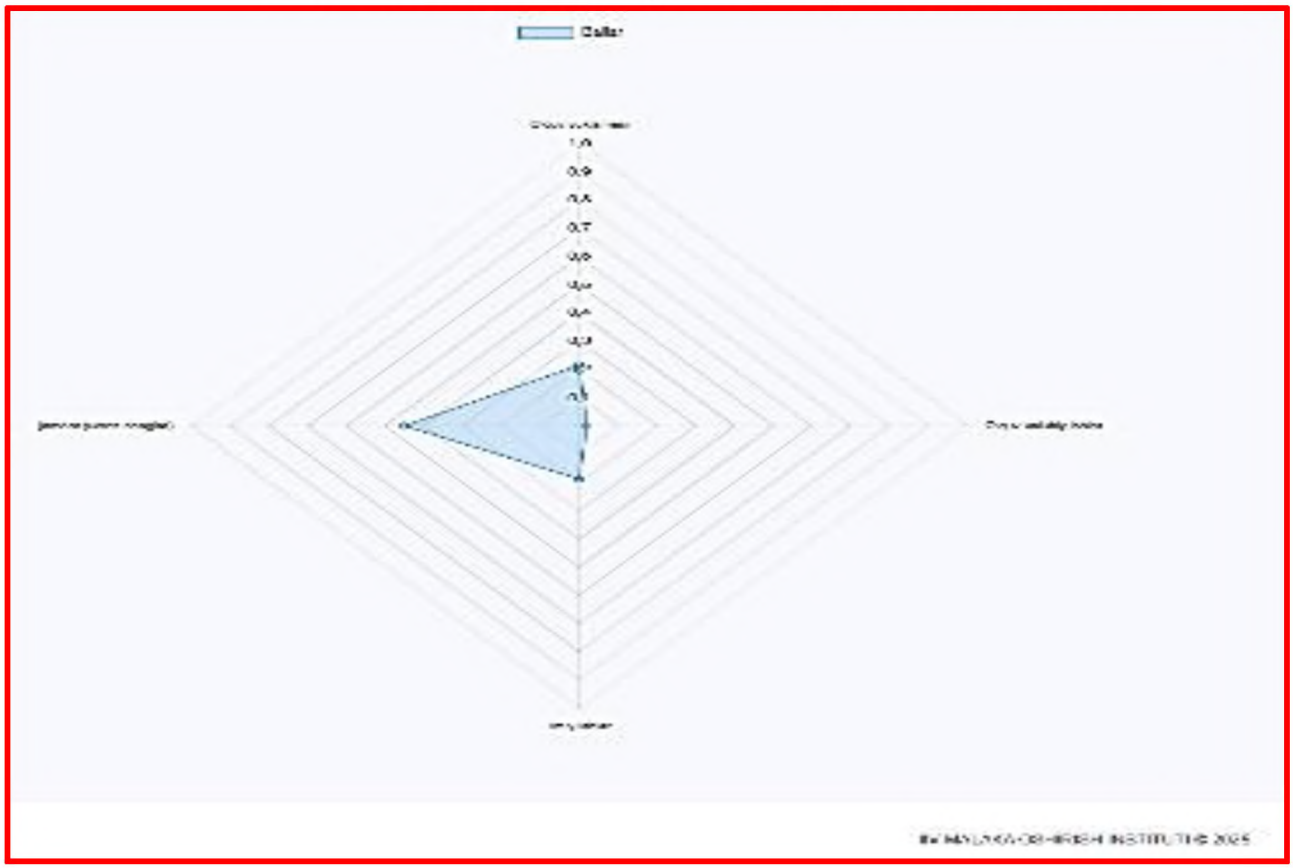
Chet el tajribasida, xususan, Yevropa Ittifoqining DigCompEdu modeli, OECD ko‘rsatkichlari hamda xalqaro reyting tizimlari professor-o‘qituvchilar raqamli kompetensiyasini aniqlashda keng qo‘llanilmoqda. Ushbu tajribalar shuni ko‘rsatadiki, smart reyting tizimi ta’lim sifatini oshirish, ularning ilmiy-pedagogik faoliyatini rag‘batlantirish, professor-o‘qituvchilar o‘rtasida sog‘lom raqobat muhitini shakllantirish, ichki ishlar organlari uchun yuqori malakali mutaxassis kadrlarni tayyorlashga zamin yaratish hamda raqamli ko‘nikmalarni rivojlantirishda samarali vosita hisoblanadi. Yaqinda chop etilgan ilmiy tadqiqotlar shuni tasdiqlaydiki,

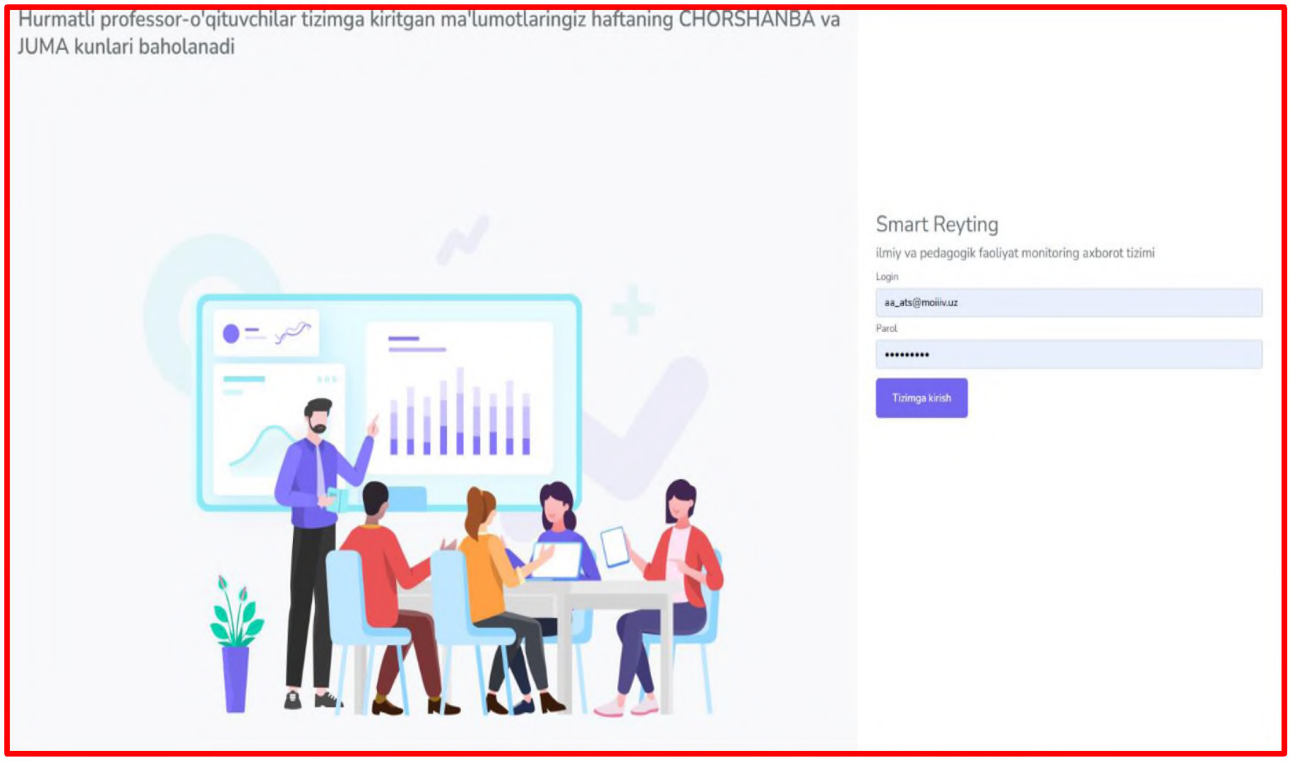
smart reyting tizimi ta’lim sifatini oshirish, shaffoflikni ta’minlash va o‘qituvchilar o‘rtasida sog‘lom raqobat muhitini shakllantirishda samarali vosita bo‘lishi mumkin.

Bu tizim o‘qituvchining nafaqat texnologiyadan foydalanish qobiliyatini, balki uni ta’lim jarayoniga qanchalik samarali integratsiya qila olish darajasini ham ko‘rsatib beradi. AQSh va Finlyandiya tajribasida esa “professional development portfolio” hamda “digital teaching effectiveness index” kabi reyting tizimlari tatbiq etilib, o‘qituvchilarning innovatsion pedagogik yondashuvlari muntazam ravishda raqamli ko‘rsatkichlar orqali baholanadi.

Ushbu raqamli texnologiyalar milliy amaliyot bilan solishtirilganda, bizning ta’lim tizimimizda ham shunga o‘xshash kompleks baholash metodologiyalarini shakllantirish zarurati yaqqol namoyon bo‘ladi. Professor-o‘qituvchilarning reyting tizimi orqali ro‘yxatdan o‘tishi hamda reytingni aniqlashga oid ma’lumotlarni kiritilishi uchun fakultet va kafedra (sikl) boshliqlari mas’ul hisoblanadi.

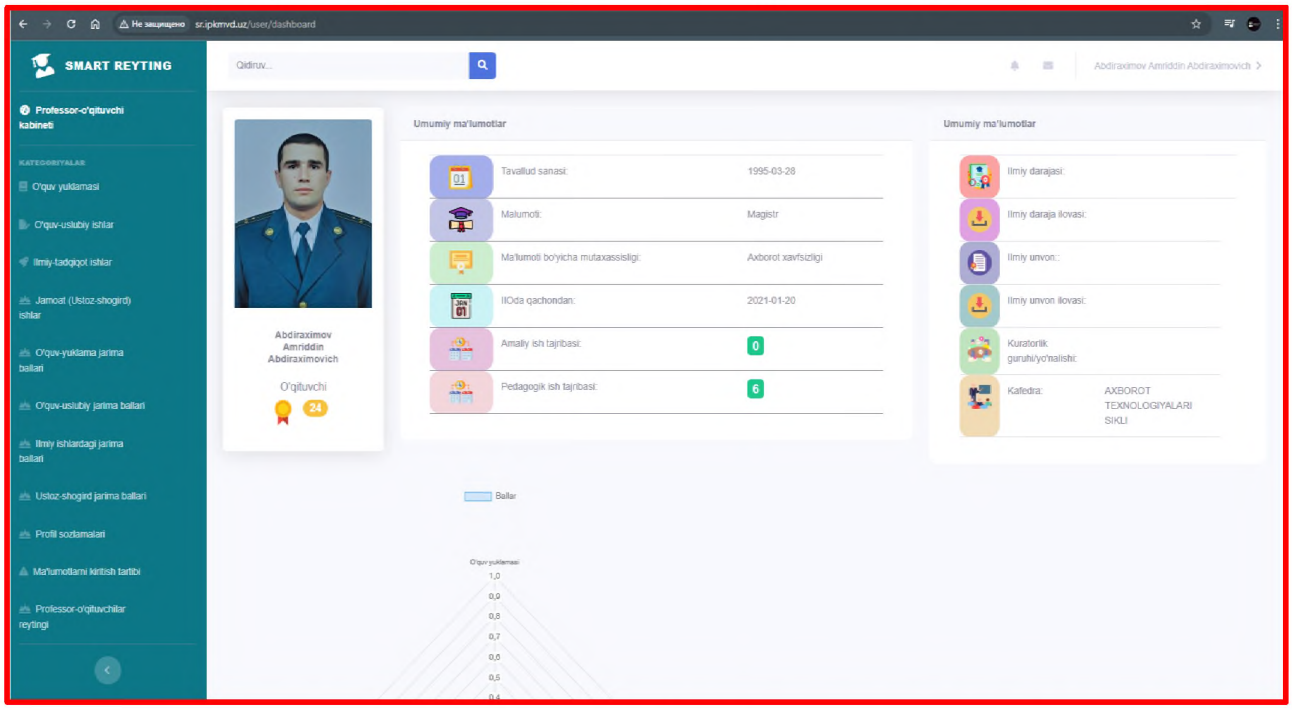
1-rasm. Smart reyting tizimidagi Radar Chart





2-rasm. Smart reyting tizimi ko‘rinishi

Radar Chart – ko‘p o‘lchovli ma’lumotlarni (o‘rgimchak, yulduz) radar diagramma ko‘rinishida grafik ko‘rsatish usuli. Bu o‘rinda, professor-o‘qituvchilar faoliyati ko‘rsatkichlarining (o‘rgimchak, yulduz) radar diagramma ko‘rinishidagi grafik tahlili.

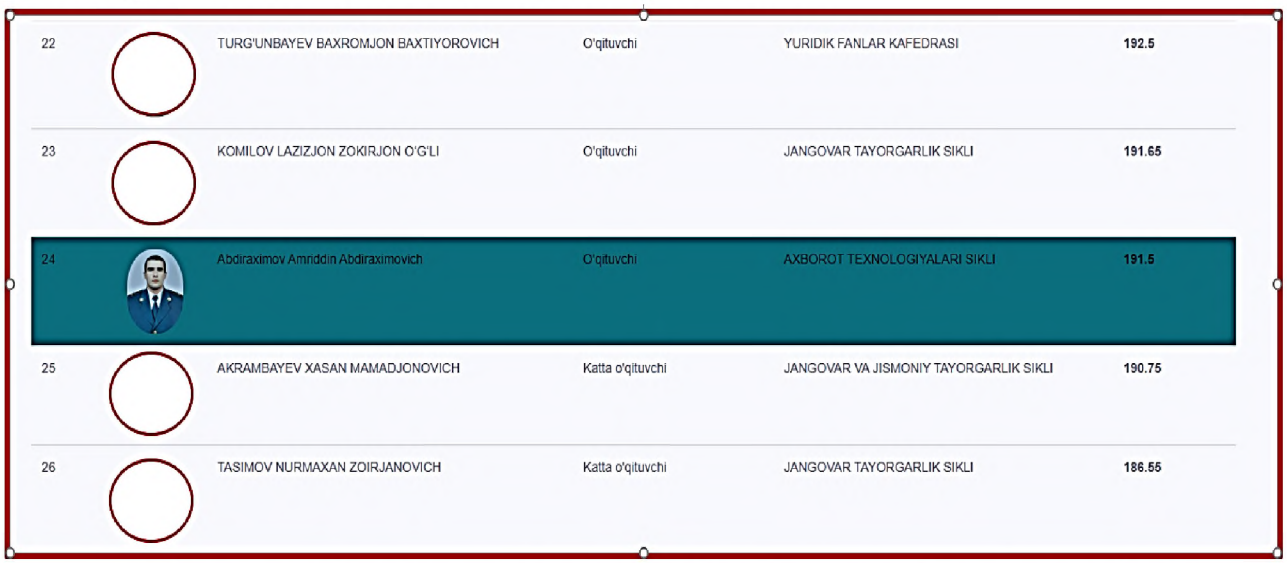


3-rasm. Professor-o‘qituvchilarning umumiy ma’lumotlari

Smart reyting tizimining afzalliklari va muammolari

Smart reyting tizimi klassik baholash yondashuvlaridan farqli ravishda bir qator afzalliklarga ega. Eng avvalo, u ochiqlik va obyektivlikni ta’minlaydi, chunki ko‘rsatkichlar raqamli vositalar orqali avtomatlashtirilgan tarzda qayd etiladi. Ikkinchidan, tizim o‘qituvchining raqamli savodxonlik darajasi, innovatsion metodlarni qo‘llash qobiliyati va kasbiy rivojlanishdagi faolligini kompleks baholash imkonini beradi. Uchinchidan, smart reyting tizimi orqali hosil bo‘lgan natijalar real vaqt rejimida monitoring qilinib, qaror qabul qiluvchi rahbarlar uchun tezkor axborot bazasini yaratadi.

Shu bilan birga, mazkur tizimning ayrim cheklovlari ham mavjud. Jumladan, o‘qituvchilarning barchasi bir xil raqamli imkoniyatlarga ega emasligi, ayrim hududlarda infratuzilma va internet tarmog‘i yetarli darajada rivojlanmaganligi tizim samaradorligiga to‘sqinlik qilishi mumkin. Bundan tashqari, faqat texnik ko‘nikmalarni baholash bilan cheklanib qolish ham yetarli emas, chunki ta’lim sifatiga o‘qituvchining shaxsiy pedagogik mahorati, kommunikativ qobiliyatlari va ijtimoiy-psixologik omillar ham sezilarli ta’sir ko‘rsatadi.



22		TURG'UNBAYEV BAXROMJON BAXTIYOROVICH	O'qituvchi	YURIDIK FANLAR KAFEDRASI	192.5
23		KOMILOV LAZIZJON ZOKIRJON O'G'LI	O'qituvchi	JANGOVAR TAYORGARLIK SIKLI	191.65
24		Abdiraximov Amriddin Abdiraximovich	O'qituvchi	AXBOROT TEXNOLOGIYALARI SIKLI	191.5
25		AKRAMBAYEV XASAN MAMADJONOVICH	Katta o'qituvchi	JANGOVAR VA JISMONIY TAYORGARLIK SIKLI	190.75
26		TASIMOV NURMAXAN ZOIRJANOVICH	Katta o'qituvchi	JANGOVAR TAYORGARLIK SIKLI	186.55

4-rasm. Professor-o‘qituvchilarning monitoring natijasi

Xulosa o‘rnida, raqamli texnologiyalarining joriy etilishi Ichki ishlar organlari tizimida ta’lim effektivligi salmoqli darajada sifatga qarab intilmoqda. Smart reyting tizimi ta’lim sifatini boshqarishda ilg‘or tajriba bo‘lib, u professor-o‘qituvchilar faoliyatini raqamli ko‘rsatkichlar asosida baholash orqali ta’lim sohasining raqamli transformatsiyasini

jadallashtiradi va xalqaro tajribaga mos ravishda milliy ta’lim tizimining samaradorligini oshiradi.

Foydalanilgan adabiyotlar:

1. Mirziyoyev Sh.M. “Axborot xavfsizligi va raqamli taraqqiyot: Yangi strategiyalar”, 2024.
2. O‘zbekiston Respublikasi Prezidentining “Ichki ishlar organlarini xalqchil professional tuzilmaga aylantirish va aholi bilan yanada yaqin hamkorlikda ishlashga yo‘naltirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi PQ-10-son Qarori.T. 2023-yil 20 yanvar.
3. Абдусаломов А. Raqamli texnologiyalar va ta’lim tizimida ularning qo‘llanilishi. – Toshkent: Fan va texnologiya nashriyoti, 2021.
4. Anderson, T., & Rivera, J. *Digital Competence in Higher Education: Frameworks and Applications*. – London: Routledge, 2021.
5. Андреев А.А. *Информационные технологии в образовании*. – Москва: Академия, 2018.
6. European Commission. Digital Education Action Plan (2021–2027): Resetting Education and Training for the Digital Age. – Brussels: EC Publishing, 2021.
7. Xasanov B., Qodirova D. Ta’limda innovatsion texnologiyalar. – Toshkent: O‘zbekiston Milliy universiteti nashriyoti, 2020.

OPTIK TOLALI ALOQA KABELLARI ORQALI BOSHQARILADIGAN DRONLARNING MUDOFAA VA XAVFSIZLIK SOHASIDA QO‘LLANISHI: IMKONIYATLAR VA CHEKLOVLAR

Fayzullayev A.X.
Sindarov Sh.O‘.
O‘zbekiston Respublikasi Harbiy Xavfsizlik va Mudofaa universitetining Axborot-kommunikatsiya texnologiyalari va harbiy aloqa instituti

Uchuvchisiz uchish apparatlarining parvoziga halaqit beruvchi eng asosiy xatarlardan biri elektromagnit bosim berish hisoblanadi. Ushbu turdagi tahdidlarga qarshi kurashish uchun zamonaviy yechim sifatida optik tolali aloqa kabellariga ega UUAlar ishlab chiqarilmoqda. Bu optik

tolali dronlar uchuvchisiz uchish apparati (UUA) texnologiyasidagi yutuq bo‘lib, operatorlarga zaif radio aloqalari o‘rniga optik tolali simli kabel orqali dronlarni boshqarish imkonini beradi [1]. Natijada, amalda to‘sqinlik qilib bo‘lmaydigan, xavfsiz ulanish yuzaga keladi va bu zamonaviy urush qiyofasini o‘zgartirmoqda. Harbiy tahlilchilar optik tolali dronlarni “Ukrainadagi urushni o‘zgartirayotgan dahshatli yangi qurol” deb atagan, yerda turgan qo‘mondonlar esa bu dronlar havoga ko‘tarilgach, ularni faqat yomon ob-havo yoki to‘g‘ridan-to‘g‘ri zarba to‘xtata olishini bildirmoqda. Biroq optik tolali dronlarning ta’siri front chizig‘idan ancha uzoqqa boradi. Yuqori xavfli harbiy operatsiyalardan tortib fuqarolik infratuzilmasini tekshirish va telekommunikatsiyagacha — bu texnologiya dronlardan foydalanish uchun yangi ufqlarni ochmoqda [2].

Optik tolali dronlar — operator bilan aloqa uchun simsiz radio yoki sun’iy yo‘ldosh aloqalariga tayanish o‘rniga fizik **optik tolali kabel**dan foydalanadigan uchuvchisiz uchish apparatlaridir. Amalda bu tipdagi UUAlar ikki ko‘rinishda bo‘ladi: dron yengil optik tolali kabel orqali yerusti boshqaruv stansiyasiga bevosita ulangan bo‘ladi (1-a-rasm) **yoki** dron uchayotganda yechilib boradigan tolali **g‘altak**ni o‘zi bilan olib yuradi
(1-b-rasm) [3].

a)  b) 

1-rasm. Optik tolali dronlar turlari

Tolali liniya kodlangan boshqaruv buyruqlari va jonli video oqimini yorug‘lik impulslari shaklida tashiydi, natijada uchuvchi bilan dron o‘rtasida **yuqori o‘tkazuvchanlik** va **past kechikish**li aloqa ta’minlanadi. Havoga radio signal tarqatadigan odatiy dronlardan farqli ravishda, optik tolali dronning butun aloqasi kabel ichidan o‘tadi va **radiochastota izi**

qoldirmaydi [4]. Ana shu muhim farq bir nechta asosiy ustunliklarni beradi:

- **Radioelektron hujum usullariga qarshi immunitet.** Radioelektron kurash bo‘linmalari **radiochastotali aloqa** signaliga aralashib, radio orqali boshqariladigan dronlarni ishdan chiqarishi yoki boshqaruvni qo‘lga olishi mumkin. Optik tolali dronlar esa “hech qanday radiosignal chiqarmaydi… va ularning signalini to‘sib bo‘lmaydi” [5]. Kabel orqali ulanish tabiatan xavfsiz va elektromagnit shovqindan himoyalangan bo‘lib, bunday dronlarni an’anaviy **radioelektron** halaqitlar va signalni tutib olishdan himoya qiladi. Bugungi jang maydonlarida radio to‘sqinliklar hammayoqda uchrayotgan sharoitda, bu — inqilobiy ustunlik.
- **Yashirin aloqa.** To‘liq radio sukunatida ishlagani sababli, optik tolaga ulangan dronlar radar skanerlari yoki aloqa nurlanishini “eshitadigan” radar tizimlari uchun amalda “ko‘rinmas” bo‘ladi. Albatta, dronning o‘zi jismoniy obyekt sifatida oddiy radarlarida ko‘rinishi mumkin, biroq radio signalning yo‘qligi erta ogohlantirish va kuzatishni ancha qiyinlashtiradi.
- **Yuqori ma’lumot o‘tkazish qobiliyati.** Optik tolali liniyalar nihoyatda katta hajmdagi ma’lumotni yorug‘lik tezligida tashiy oladi. Hatto juda ingichka (inson sochi qalinligidek) tolali ip ham deyarli **nol kechikish** bilan yuqori aniqlikdagi videoni uzata oladi. Operatorlar “maqsadning o‘ziga yetguncha mukammal video oqimi”ni olishini aytadi — bu, ayniqsa, hal qiluvchi onlarda uzilib qolishi yoki “shovqin”ga aylanishi mumkin bo‘lgan analog radio FPV ulanishlaridan keskin farq qiladi [6]. Bunday kristalldek tiniq tasvir murakkab muhitda ham aniq qo‘lda boshqarishni ta’minlaydi.
- **Juda past kechikish.** Tola ichidagi yorug‘likka asoslangan signallar minimal kechikishga ega, ya’ni dron boshqaruv buyruqlariga deyarli zudlik bilan javob beradi va kamera tasviri real vaqtning o‘zida yangilanadi. Bu sun’iy yo‘ldosh orqali boshqariladigan dronlar va ko‘plab radio tizimlaridan farq qiladi. Bunday sezgir boshqaruv dronni tor shahar ko‘chalari yoki zich o‘rmon relyefi orasidan aniqlik bilan olib o‘tishda juda muhim.

- **Radiochastotali aloqaga noqulay muhitlarda ishlash.** Optik tolali boshqaruv radio aloqa odatda ishlamaydigan joylarda — masalan, temir-beton inshootlar ichkarisida, yer osti tunnellarida yoki zich o‘rmonlarda drondan foydalanish imkonini beradi. **Kabel uzilmaguncha** aloqa uzilmaydi. Endilikda yopiq binolardagi yashirinish joylari ham panoh bo‘la olmaydi: orqasidan tola sudrab uchayotgan dron eshik yoki derazadan kirib, bino ichida zarba berish uchun boshqaruvni saqlab qoladi [7].

Shu bilan birga, optik tolali ulanishlar o‘ziga xos muammolar va cheklovlarni ham keltiradi. Eng asosiy cheklov — **fizik kabelning o‘zi**. Dron faqat tolaning uzunligi yetguncha ucha oladi — odatiy g‘altaklar 5 km dan 20–30 km gacha bo‘lishi mumkin. Relelar yoki sun’iy yo‘ldosh orqali nazariy jihatdan cheksiz boshqarilishi mumkin bo‘lgan simsiz dronlardan farqli ravishda tolali dronning masofasi kabel uzunligi bilan qat’iy cheklanadi. Kabel, shuningdek, **tortilish (drag)** va **ilinib qolish** (shox-shabba, elektr simlari yoki binolarga ilinib qolish) xatarlarini keltiradi. Uchuvchilar tolani “bukib yubormaslik” yoki tugunlab qo‘ymaslik uchun ehtiyotkor parvoz qilishi kerak — keskin buralish yoki uzilish signalni darhol uzadi va vazifa yakunlanadi. Manyovrlilik ham erkin uchadigan kvadrokopterlarga qaraganda biroz pastroq — keskin burilishlar kabelning tortishi tufayli qiyinlashadi. G‘altak va kattaroq batareya (dron va kabelni birga ko‘tarish uchun) qo‘shimcha vazn qo‘shadi, shu bois tolali dronlar ko‘pincha radio boshqaruvdagilariga qaraganda **og‘irroq va sekinroq** bo‘ladi. Masalan, odatiy FPV poyga droni 150 km/soatdan oshishi mumkin bo‘lsa, tolali variantlar odatda **taxminan 60–70 km/soat** atrofida tezlikka ega. Bu ularni ko‘rinsa, mayda o‘qotar qurollar uchun nishonga aylantirishi mumkin [8].

Bundan tashqari, **ekspluatatsion xarajatlar** ham bor: har bir vazifadan so‘ng jang maydonida kilometrlab tola sochilib qoladi va odatda jang sharoitida uni qaytarib olishning iloji bo‘lmaydi. Ushbu sarflanadigan kabel (ko‘pincha polimer tolalardan) xarajatni oshiradi — bir ukrainalik qo‘mondonning baholashicha, tolali dron oddiy modeldan qariyb ikki baravar qimmat tushadi (masalan, 10 km diapazonli qurilma uchun

taxminan $1 000–1 200) [9]. Shunga qaramay, operatorlar orasidagi umumiy fikr shuki, **foydalar noqulayliklardan ustun**: Dron hech bir muammosiz, to‘g‘ri nishonga kirib borganida, bu murakkabliklar o‘zini oqlaydi.

Quyidagi 1-jadvalda optik tolali dronlardan foydalanishning afzalliklari va kamchiliklari haqida so‘z boradi.

1-jadval.

Optik tolali dronlardan foydalanishning afzalliklari kamchiliklari

Afzalliklari	**Kamchiliklari**
Radioelektron hujum va halaqitlarga to‘liq immunitet	Masofa kabel uzunligi bilan cheklangan (5–30 km)
Radiochastotali nurlanish yo‘qligi sababli yashirin aloqa	Kabel shox-shabba, sim yoki inshootlarga ilinib qolishi mumkin
Yuqori o‘tkazuvchanlik va past kechikishli aloqa	Manyovrlilik erkin uchadigan dronlarga qaraganda pastroq
Kristalldek tiniq real vaqt video oqimi	Kabel va batareya qo‘shimcha og‘irlik beradi, tezlik sekinroq (60–70 km/soat)
Radioaloqa ishlamaydigan joylarda (bunker, tunnel, beton inshootlar) ishlash imkoniyati	Sekinligi sababli mayda o‘qotar qurollar uchun nishonga aylanishi osonroq
Signalni tutib olish yoki bostirish mumkin emas	Kabel sarflanadi, qaytarib olinmaydi, ekspluatatsion xarajat yuqori
Operator uchun xavfsiz, barqaror boshqaruv	Oddiy FPV dronlariga qaraganda ikki baravar qimmatroq

Xulosa o‘rnida shuni keltirib o‘tish mumkinki, Optik tolali uchuvchisiz uchish apparatlari zamonaviy harbiy va fuqarolik sohalarida qo‘llanilayotgan innovatsion texnologiya sifatida muhim ahamiyatga ega. Ularning asosiy ustunliklari radioelektron halaqitlarga to‘liq immunitet, yashirin va xavfsiz aloqa, yuqori sifatli va past kechikishli ma’lumot uzatish imkoniyatlari bilan belgilanadi. Bu xususiyatlar dronlarni murakkab sharoitlarda ham samarali boshqarish imkonini beradi. Shu bilan

birga, kabel uzunligining chegaralanganligi, tortilish va ilinib qolish xavfi, og‘irlik hamda iqtisodiy xarajatlarning yuqoriligi ularning asosiy kamchiliklari sifatida ko‘riladi. Shunga qaramay, afzalliklar kamchiliklardan ustun bo‘lib, optik tolali dronlarning kelgusida qo‘llanish sohasi kengayishi va strategik ahamiyatining ortishi tabiiy jarayon sifatida baholanadi.

Foydalanilgan adabiyotlar:

1. V. Rodriguez va boshqalar, *An Experimental Tethered UAV-Based Communication System*, **Future Internet (MDPI)**, 2025.
2. Y. N. Shindo va boshq., *Optically Powered and Controlled Drones Using Optical Fibers*, **Photonics (MDPI)**, 2022.
3. F. Fattori va boshq., *Tethered Drones: A Comprehensive Review of Technologies*, **Drones (MDPI)**, 2025.
4. *Fiber-Optic Drones: Posing a Significant C-UAS Challenge*, **U.S. Army Publication**, 2025.
5. D. Hambling, *Jam-Proof Fiber Optic Drone Testing In Ukraine*, **Forbes**, 2024.
6. *Fiber optic drone*, **Wikipedia**, 2025.
7. *A Ukrainian weapons maker is building a new unjammable drone...*, **Business Insider**, avgust 2025.
8. *Ukraine scrambles to overcome Russia’s edge in fiber-optic drones*, **The Washington Post**, may 2025.
9. *Tethered Unmanned Aerial Vehicles—A Systematic Review*, **ResearchGate** (Systematik sharh), 2023.

HARBIY OBYEKTLARNI MUHOFAZA QILISHDA FAZALI TOLALI-OPTIK DATCHIKLAR TAHLILI

Anvarov F.I.
Yusupov U.A.
Tashmanov Y.B.
O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti kursanti.
O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti
kafedra katta o‘qituvchisi.

O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti kafedra
boshlig‘i.

Hozirgi davrda harbiy xavfsizlik sohasida yuqori aniqlikdagi monitoring va erta ogohlantirish tizimlariga bo‘lgan ehtiyoj keskin ortib bormoqda. Xususan, strategik obyektlar, chegaraviy hududlar va maxsus harbiy inshootlar atrofini doimiy nazorat qilish, tashqi xavf-xatarlarni tezkor aniqlash va oldini olish dolzarb vazifalardan hisoblanadi. Shu nuqtai nazardan tolali-optik texnologiyalar, jumladan, fazali datchiklarning qo‘llanilishi alohida ahamiyat kasb etmoqda.

Fazali datchiklarning asosiy afzalligi ularning yuqori sezgirligida namoyon bo‘ladi. Optik interferometriya texnologiyasi yordamida ular tashqi omillar ta’sirida yuzaga keladigan eng kichik fazaviy o‘zgarishlarni ham qayd etishga qodir. Ushbu xususiyat harbiy obyektlar perimetrini himoya qilishda eng kichik tashqi ta’sirlarni ham qayd eta oladi. Masalan, harbiy obyektlarning perimetri bo‘ylab o‘rnatilgan bunday datchiklar tuproq tebranishi, mexanik bosim yoki hatto yaqinlashayotgan transport vositalarining ta’sirini aniqlash orqali erta ogohlantirish tizimlarida samarali qo‘llaniladi.

Ularning taqsimlangan (butun uzunligi bo‘ylab sezgir) ishlash xususiyati katta hududlarni, xususan, harbiy bazalar, chegara chiziqlari va maxfiy obyektlar atrofini kuzatishda qo‘l keladi. Shu orqali patrullash kuchlarini kamaytirish, xavfsizlik monitoringini doimiy ravishda olib borish va inson resurslarini tejash imkoniyati yaratiladi.

Biroq, ishlab chiqarish murakkabligi va yuqori narxi sababli bunday datchiklar odatda strategik obyektlar uchun mo‘ljallangan bo‘ladi.

Kogorent detektorlardan foydalanish talab etilishi esa ularning texnik xizmat koʻrsatish jarayonini ham murakkablashtiradi. Shunga qaramay, yuqori sezgirlik va keng koʻlamli qoʻllanish imkoniyatlari fazali optik datchiklarni harbiy xavfsizlik tizimlarida istiqbolli texnologiyaga aylantirmoqda.

Fazali datchiklarda tashqi omil ta'sirida sezgir element (sensor) chiqishida optik toʻlqinning fazasi oʻzgaradi va bu oʻzgarish interferometrik usulda – oʻlchovchi va nazorat kanallari signallarining ustma-ust tushishi orqali qayd etiladi.

Ushbu datchiklarning afzalligi shundaki, ular eng sezgir hisoblanadi. Oʻlchovlar tashqi omilning kanal materialiga ta'siri orqali amalga oshiriladi va interferometrik usul yordamida qayd etiladi. Optik interferometriya texnologiyasi faza tebranishining 10^{-8} rad gacha boʻlgan oʻzgarishini aniqlash imkonini beradi.

Fazali datchiklar boshqa tolali-optik datchiklarga qaraganda unchalik ixcham emas, chunki optik tolani diametri 3–6 sm dan kichik boʻlgan gʻaltaklarga oʻrash mumkin emas. Ularda atrof-muhit xususiyatlari detektor orqali oʻtayotgan nurlanish spektrining faza siljishiga ta'sir koʻrsatadi. Bunday datchik elementlarining sezgirligi optik tola uzunligiga kuchli darajada bogʻliq: tola uzunligi qancha katta boʻlsa, tashqi ta'sirlarga sezgirlik shuncha yuqori boʻladi. Shu sababli fazali datchiklar ixcham qurilmalardan koʻra taqsimlangan (ya'ni sezgir elementi butun uzunligi boʻylab tolani oʻz ichiga oluvchi) tizimlarni yaratishga koʻproq mos keladi.

Fazali datchiklar uchun, odatda, bir modali tola ishlatiladi, ya'ni yadro qismi ancha ingichka boʻlgan tola. Bu ularning ishlab chiqarilishini ancha murakkablashtiradi va narxini oshiradi. Signalni aniqlash uchun kogorent usullar – gomo- va geterodin detektorlardan foydalanish talab qilinadi.

Yuqori sezgirlik koʻrsatkichlariga qaramay, fazali tolali-optik datchiklarning bir qator kamchiliklari mavjud:

- yetarlicha katta oʻlcham;
- ishlab chiqarish murakkabligi;
- maxsus oʻzgartirgichlarga ehtiyoj;

- yuqori narx.

Fazali tolali-optik datchiklar yuqori sezgirligi sababli harbiy sohada keng qo‘llash imkoniyatiga ega. Bu xususiyatlar quyidagi yo‘nalishlarda qo‘llanilmoqda:

Perimetr xavfsizligi va chegara hududlarini nazorat qilish.

Fazali datchiklar taqsimlangan monitoring tizimlarida samarali ishlaydi, chunki butun optik tola sezgir element vazifasini bajaradi. Masalan, harbiy obyektlar yoki strategik inshootlar atrofida joylashtirilgan tola orqali hatto eng kichik tebranish yoki harakat aniqlanadi. Bu esa dushman harakatini erta aniqlashga xizmat qiladi.

Yer osti harakatlarini kuzatish.

Fazali tolali-optik tizimlar tuproq tebranishlariga juda sezgir bo‘lgani uchun yer osti tunnel qazish ishlarini aniqlashda samarali vosita hisoblanadi. Bu texnologiya chegaralarni noqonuniy kesib o‘tish holatlariga qarshi qo‘llaniladi.

Transport va texnika monitoring

Harbiy texnika harakati paytida hosil bo‘ladigan mikro tebranishlarni qayd etish orqali qo‘shinlarning joylashuvi va texnikaning harakatini nazorat qilish mumkin. Fazali datchiklarning faza siljishlarni aniq qayd etishi texnikaning turi va masofasini ham aniqlash imkonini beradi.

Portlovchi modda va zarba to‘lqinlarini aniqlash

Ulkan sezgirlik fazali datchiklarga portlash yoki zarba to‘lqinlarining minimal ta’sirini ham qayd etishga imkon beradi. Bu ularni jangovar sharoitlarda signalizatsiya va erta ogohlantirish tizimida muhim vosita sifatida qo‘llash imkonini beradi.

Shu bilan birga, fazali datchiklarning murakkab va qimmat ishlab chiqarilishi, hamda ixchamlik darajasining pastligi ularni harbiy amaliyotda keng miqyosda tatbiq qilishni cheklaydi. Biroq yuqori sezgirlik va taqsimlangan monitoring imkoniyatlari sababli ular zamonaviy harbiy xavfsizlik tizimlarining ajralmas qismi sifatida qaralmoqda.

Foydalanilgan adabiyotlar:

1. Родина О.В. Волоконно-оптические линии связи. Практическое руководство. – М.: Горячая линия – Телеком, 2020. – 400 с.

2. Листвин А. В., Листвин В. Н., Швырков Д. В. Оптические волокна для линий связи. М.: ЛЕСА Рарт, 2003. 107 с.

3. Кабели оптические. Общие технические условия. ГОСТ Р 52266-2020. – Москва. – Стандартинформ, 2020.

4. Волоконно-оптические датчики. Вводный курс для инженеров и научных работников Под ред. Э. Удда М: Техносфера, 2008. – 520 с.

OMMAVIY TARTIBSIZLIKLARDA ODAM SANASH MODELLARI TUZILISHINING TAHLILI

Tashmanov Y.B

O‘R IIV Malaka oshirish instituti katta o‘qituvchisi t.f.f.d. (PhD), dotsent

Ommaviy tartibsizliklar sharoitida odamlarni aniq hisoblash masalasi xavfsizlik tizimlari uchun eng dolzarb vazifalardan biri hisoblanadi. Bunday vaziyatlarda odatiy hisoblash usullari samarasiz bo‘lib qoladi, chunki odamlar soni juda ko‘p, harakat jadal va tez o‘zgaruvchan, shuningdek, shaxslarning o‘zaro to‘siq va yaqinligi yuqori darajada namoyon bo‘ladi. Shu bois ommaviy yig‘ilishlar va tartibsizliklarda qo‘llaniladigan odam sanash modellari an’anaviy kompyuter ko‘rishi yondoshuvlaridan farq qiladi.

Odam sanash modellarining tuzilishi, avvalo, real vaqtda katta hajmdagi videoma’lumotlarni qayta ishlashga, shaxslarni aniq segmentatsiya qilishga hamda turli nurlanish, yorug‘lik va harakat sharoitlariga moslashishga qaratilgan bo‘lishi kerak. Shu bilan birga, tartibsizlik holatlarida odamlar harakat trayektoriyasini kuzatish, ularning zichligi va oqim yo‘nalishini tahlil qilish orqali xavf darajasini baholash imkoniyati ham ta’minlanishi zarur.

Shu nuqtai nazardan, ommaviy tartibsizliklarda odam sanash modelining tuzilishi konvolyusion neyron tarmoqlar, ko‘pmasshtabli

xususiyatlarni birlashtirish usullari, obyektlarni segmentatsiya qilish va treking algoritmlari asosida ishlab chiqiladi. Bunday modellar nafaqat odam sonini aniq hisoblaydi, balki odamlar oqimi to‘g‘risidagi statistik va dinamik ma’lumotlarni ham taqdim etib, xavfsizlik xizmatlariga favqulodda choralar ko‘rish imkoniyatini yaratadi.

Chuqur o‘rganish rivojlanishi bilan odam sanashda turli model tuzilish usullari paydo bo‘ldi. Ushbu usullar ko‘p-masshtabli birlashtirish strategiyalarini joriy etish, e’tibor mexanizmlarini integratsiya qilish va transformerlardan foydalanishni o‘z ichiga oladi. Ko‘p-masshtabli xususiyatlarni birlashtirish usullari odamlar ko‘lamining katta farqlari muammosini turli darajadagi xususiyatlarni integratsiya qilish orqali hal qilishga harakat qiladi. Zhang va boshqalar [1] ko‘p ustunli CNN arxitekturasini qo‘llagan, unda har bir CNN ustuni turli qabul qilish maydonlariga ega filtrlardan foydalangan. Jiang va boshqalar [2] kodlovchi-dekodlovchi tuzilishdan foydalanib, qatlamlar orasidagi o‘tishlar orqali ko‘p darajali xususiyatlarni birlashtirgan, bu esa past darajadagi fazoviy tafsilotlar va yuqori darajadagi semantik ma’lumotlarni quyidan yuqoriga yig‘ish imkonini bergan. Bu butun tasvirdan yuqori aniqlikdagi zichlik xaritalarini prognoz qilish imkonini yaratgan. Liu va boshqalar [3] fazoviy piramida pullingidan foydalanuvchi yangi arxitektura taklif qilib, turli masshtablarda kontekst ma’lumotlarni ajratgan va ular asosida so‘nggi zichlik xaritasini hisoblagan. Ma va boshqalar [4] kodlovchidagi turli qatlamlar bergan ma’lumotdan foydalanib, turli qabul qilish maydonlariga ega xususiyat xaritalarini hosil qiladigan ko‘p-masshtabli mexanizm joriy etgan. Zhang va boshqalar [5] SaCNN deb nomlangan masshtabga moslashuvchan CNN ishlab chiqishgan, u ko‘p darajali xususiyatlarni birlashtirib, modelni turli masshtab va nuqtai nazar farqlariga moslashtirgan. Han va boshqalar [6] esa xususiyat tanlash va meros o‘rganish usulini qo‘llab, niqob tanlash va meros yo‘qotish orqali ko‘p-masshtabli birlashtirishni amalga oshirishgan.

E’tibor mexanizmlari ham samarali usul hisoblanadi. Cao va boshqalar [7] SANet modelini taklif etishgan, u ko‘p-masshtabli konvolyusiyalar va moslashuvchan global e’tibor mexanizmidan

foydalanib, turli zichlik va o‘lchamdagi tasvirlar bilan ishlagan. Jiang va boshqalar [8] ikki shoxli tuzilishni qo‘llab, bir shox ortiqcha moslashtirilgan oraliq zichlik xaritalarini va masshtab omillarini hosil qilgan, so‘ng esa uni ikkinchi shoxda yaratilgan e’tibor niqoblari bilan birlashtirib, aniqroq natijalar olgan. Lin va boshqalar [9] o‘rganiladigan global e’tibor moduli va mahalliy bo‘limli e’tibor modullarini qo‘llab, aniqlikni oshirishgan.

Tabiiy tilni qayta ishlash (NLP) sohasida transformer tarmoqlari muvaffaqiyatidan keyin tadqiqotchilar ularni odam sanashda ham qo‘llashni boshlashdi. Sun va boshqalar [10] transformer modellaridan foydalanib, tasvir bloklarini biriktirish va kontekstual tokenlar qo‘shish orqali xususiyat ajratish va ma’lumot almashishni amalga oshirgan. Qian va boshqalar [11] “U-shaklli” ko‘p-masshtabli transformer tarmog‘ini taklif qilib, yangi yo‘qotish funksiyasini joriy etgan va aniqlikni sezilarli darajada oshirgan.

Zamonaviy odam sanash modellari konvolyusion neyron tarmoqlar, ko‘p-masshtabli xususiyatlarni birlashtirish usullari, segmentatsiya va treking algoritmlari asosida ishlab chiqilib, nafaqat sonini aniq hisoblash, balki zichlik va oqim yo‘nalishini tahlil qilish imkonini ham yaratadi.

Tadqiqot natijalari ko‘rsatadiki, ko‘p-masshtabli birlashtirish strategiyalari, e’tibor mexanizmlari va transformer arxitekturalari qo‘llanilishi hisoblash aniqligini sezilarli darajada oshiradi. Xususan, kodlovchi-dekodlovchi tuzilishlar, fazoviy piramida pulling, masshtabga moslashuvchan CNN va e’tibor moduli integratsiya qilingan modellar yuqori aniqlikda zichlik xaritalarini prognoz qilish imkoniyatini bermoqda.

Shu tariqa, ommaviy tartibsizliklarda odam sanashning samarali modellari xavfsizlik xizmatlariga tezkor qaror qabul qilish va favqulodda choralar ko‘rishda ishonchli vosita sifatida xizmat qilishi mumkin. Kelgusida ushbu yo‘nalishda real vaqtda ishlaydigan, hisoblash samaradorligi yuqori va turli tashqi omillarga barqaror modellarni yaratish ilmiy va amaliy jihatdan ustuvor vazifa hisoblanadi.

Foydalanilgan adabiyotlar:

1. Y. Zhang, D. Zhou, S. Chen, S. Gao, Y. Ma, Single-image crowd counting via multi-column convolutional neural network, in: Proceedings of the IEEE conference on computer vision and pattern recognition, 2016, pp. 589–597.

2. X. Jiang, Z. Xiao, B. Zhang, X. Zhen, X. Cao, D. Doermann, L. Shao, Crowd counting and density estimation by trellis encoder-decoder networks, in: Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, 2019, pp. 6133–6142.

3. W. Liu, M. Salzmann, P. Fua, Context-aware crowd counting, in: Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, 2019, pp. 5099–5108.

4. Y. Ma, V. Sanchez, T. Guha, Fusioncount: Efficient crowd counting via multiscale feature fusion, in: 2022 IEEE International Conference on Image Processing (ICIP), IEEE, 2022, pp. 3256–3260.

5. L. Zhang, M. Shi, Q. Chen, Crowd counting via scale-adaptive convolutional neural network, in: 2018 IEEE winter conference on applications of computer vision (WACV), IEEE, 2018, pp. 1113–1121.

6. T. Han, L. Bai, L. Liu, W. Ouyang, Steerer: Resolving scale variations for counting and localization via selective inheritance learning, in: Proceedings of the IEEE/CVF International Conference on Computer Vision, 2023, pp. 21848–21859.

7. X. Cao, Z. Wang, Y. Zhao, F. Su, Scale aggregation network for accurate and efficient crowd counting, in: Proceedings of the European conference on computer vision (ECCV), 2018, pp. 734–750.

8. X. Jiang, L. Zhang, M. Xu, T. Zhang, P. Lv, B. Zhou, X. Yang, Y. Pang, Attention scaling for crowd counting, in: Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, 2020, pp. 4706– 4715.

9. H. Lin, Z. Ma, R. Ji, Y. Wang, X. Hong, Boosting crowd counting via multifaceted attention, in: Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, 2022, pp. 19628–19637.

10. G. Sun, Y. Liu, T. Probst, D. P. Paudel, N. Popovic, L. Van Gool, Boosting crowd counting with transformers, arXiv preprint arXiv:2105.10926 3 (2021) 3.

11. Y. Qian, L. Zhang, X. Hong, C. Donovan, O. Arandjelovic, U. Fife, P. Harbin, Segmentation assisted u-shaped multi-scale transformer for crowd counting., in: BMVC, 2022, p. 397.

РЕСУРСНАЯ МЕТОДОЛОГИЯ В УПРАВЛЕНИИ БЕЗОПАСНОСТЬЮ СИСТЕМ СВЯЗИ СИЛОВОЙ СТРУКТУРЫ

Пен А.Ю.
Университет общественной безопасности Республики Узбекистан,
д.ф.т.н. (PhD), доцент

Комплекс мероприятий по обеспечению безопасности систем связи силовой структуры (СССС) включает важный сегмент-подсистему её противопожарной защиты. Необходимость решения вопросов безопасности рассматриваемой направленности объясняется для СССС следующим: 1. часто встречающаяся задача быстрой (экстренной) развёртки приводит к возможным нарушениям норм и правил пожарной безопасности; 2. отсутствием возможности расчета и оперативной проводки требуемой силовой линии под дополнительно подключаемые технические средства; 3. отсутствие возможности выбора альтернатив при организации СССС, вынужденная работа в агрессивной среде, в экстремальных условия, а отсюда недостаточный уровень, возможные нарушения противопожарной защиты. Анализ деятельности пожарной охраны выделяет обоснованные требования повышения ресурса безопасности, определяемого, в том числе, надежностью технических средств (ТС) раннего обнаружения пожара [1].

Освещаемое в работе совершенствование метрологической надёжности информационно-технического обеспечения противопожарной защиты СССС рассмотрено с позиций ресурсной методологии, так как в рассматриваемом случае она охватывает весь

формат деятельности государственной противопожарной службы. Эти вопросы актуальны и непосредственно относятся ко всей элементной базе систем охранно-пожарной сигнализации (ОПС).

Надежность ОПС будет определяться сохранением заданной точности измерения параметра (температуры) отдельным ТС, что оправдывает использование терминологии теории надежности измерительных систем. [2, 3].

Под понятием ресурса «заданной надёжности» следует понимать продолжительность (т) функционирования ОПС до выхода из строя [4]. При этом т = min (т', т"), где т' - продолжительность работы системы до поломки; т"- момент времени, начиная с которого точность измерения параметра в ОПС оказывается недостаточной. Если $A_i(t)$ - погрешность измерения i-й характеристики, i=1, n при t Є [0, t_o], зависящая от времени t, а [a_i, b;]

- допуск на A_i (t), то т" - момент времени первого выхода за пределы допуска $a_j \leq Aj\ (t) \leq b_j$, при рассмотрении таких условий на интервале [0, t_o].

Величину т = min (т', т") считают случайной и называют метрологической надёжностью ОПС, т.к. она учитывает не только поломки ОПС, но и потери метрологического качества процесса измерения на заданном интервале [0, t_o].

Если считать, что величины т', и т" независимы на интервале [0, t_o], то

функция F распределения величины т и функции F_1 и F_2 распределения величин τ_j' и τ_j'' связаны очевидным соотношением

$$P\ (\tau \leq x) = F(x)=1-[1-F_1(x)]\ [1-F_2(x)], \qquad (1)$$

где P (т < x) - вероятность того, что случайная величина т не превысит x;

x - фиксированное число.

ОПС обычно включает ряд ТС: пожарный извещатель (ПИ); станция пожарной сигнализации (СПС); прибор управления (ПУ); сигнально-пусковой прибор (СПП); оповещатели (О).

Это могут быть ТС иногда однотипные и по логике своего функционирования связаны таким образом, что выход из строя одного из них приводит к выходу из строя всей (m) совокупности ТС. Тогда говорят, что m отдельных ТС в ОПС соединены последовательно. Пусть j - номер ТС в ОПС, а τ_i - его метрологическая надежность, т. е. $\tau_i = \min(\tau_j', \tau_j'')$. Тогда $\tau = \min \tau_j$, и в случае независимости величин τ_j, j=1, m выражение (1) для функции F распределения величины т меняет вид.

Получены выражения, позволяющие по известным функциям F_1 и F_2 распределения величин τ_j' и τ_j'' нахождение функции F распределения метрологической надёжности т ОПС.

Рассматривается среднее значение t_j метрологической надёжности τ_j для j-го ТС, при условии, что все m ТС в ОПС однотипны и имеют $t_o=t_j$, тогда $t=t_0/m$. Таким образом, для указанных допущений (независимости величины τ_j экспоненциального распределения этих величин) средняя надежность t в ОПС, состоящая из m однотипных ТС, каждая из которых имеет одинаковую среднюю надежность t_o, уменьшается в m раз по сравнению с t_o. Такое резкое уменьшение обусловлено прежде всего допущением независимости величин τ_j.

Интересен случай оценки среднего значения t метрологической надёжности ОПС с учётом зависимости величин τ_j. Отметим, что такой учет является проблемной задачей и может быть осуществлен в настоящее время лишь приближенно.

Рассматривая различные варианты распределения τ_j получено соотношение

$$1-F(x)=1-F_1(x) \qquad (2)$$

которое соответствует случаю $\tau_j > x \Rightarrow \tau_j > x$,

j = 1, m, т.е. случаю, когда оказывается, что ТС с фиксированным номером j=1 имеет меньшую надежность среди т всех ТС, и этот факт известен.

При этом средняя метрологическая надёжность совпадает со средней надёжностью одного «слабейшего» ТС с номером j=1,

имеющим меньшую надёжность τ_j среди m всех ТС, входящих в ОПС. Подчёркиваем, что данное утверждение является общим, справедливым не только для случая экспоненциального распределения величин τ_j.

Для повышения метрологической надёжности ОПС можно резервировать ТС, для рассматриваемого случая это использование ТС двойной технологии, т.е. независимые каналы обнаружения и формирования сигнала [5].

В такой ситуации говорят, что ОПС состоит из т блоков, соединённых последовательно, причём каждый j-й блок содержит v_j ТС, соединённых параллельно. Будем считать, что в j-м блоке ТС однотипны и независимы. Тогда, если блоки системы, в свою очередь, также независимы выполняется условие

$$1- F(x)= \prod\{1-[F_j(x)]^{vj/j}\} \quad (3)$$

Если же в силу указанных выше причин блоки зависимы, то можно использовать предложенную формулу в следующем виде:

$$L- F(x)=\{1- [F_1(x)]^{vj/}\} \prod (1 - [F_j(x)]^{vj/j}]^{1/z} \quad (4)$$

здесь коэффициент z находят по методу наименьших квадратов на основании опытных данных.

Опуская математические преобразования, можно констатировать, введение резервных элементов и учет зависимости τ_j метрологической надежности τ_j ТС, входящих в ОПС, существенно повышает среднее значение ее метрологической надежности.

Пример демонстрации предложенного подхода. В ОПС используется т различных ТС, функционирующих так, что выход из строя одного из них приводит к выходу из строя ОПС в целом, причем величины τ_j независимы при j=1, m, характерный пример с пожарной сигнализацией. Для повышения надежности всей системы пожарной сигнализации осуществлены следующие меры:

а) вместо т различных ТС (например ПИ, СПС, ПУ, СПП) введено одно - универсальное техническое средство (УТС).

б) УТС резервируется так, что при выходе его из строя включается другой аналогичный экземпляр.

Очевидно, универсальность ТС обуславливает его усложнение и соответственно более интенсивную подверженность поломкам - снижение метрологического ресурса, а с другой стороны, введение резервирования стимулирует повышение этого ресурса (увеличения числа и реализация взаимозаменяемости ТС), а значит в определённой степени компенсирует снижение надёжности процесса измерения. В описываемой ситуации функция F распределения удовлетворяет соотношению (4), в котором показатели z характеризуют зависимость величин τ_j. Последнее объясняется заменой m различных ТС одним универсальным, а также тем, что это ТС в m различных точках измеряет однородные, равнозначные параметры.

Предположим, что указанная зависимость имеет крайнее выражение, т.е. если на одной, наиболее сложной фиксированной операции ТС выполняет возложенные на него функции, то на остальных операциях эти функции тем более выполняются (коэффициент z=0).

До внедрения наших предложений резервирование ТС не осуществлялось, а величины τ_j независимы и их среднее значение соответствует $M\tau_j = 1/\lambda=1/\lambda = t$; при этом t = t/m (где t-среднее значение метрологической надежности одного ТС ОПС). Будем считать, что m=5, а интенсивность λ_1 отказов УТС превышает интенсивность λ отказов исходного ТС в таком отношении, что $\lambda_1 = 3/ 2\lambda$. Надежность ОПС t=t/m=t'/5 после введения УТС определяется t=t' т.е. за счет корреляции величин τ_j и в результате использования резервируемого УТС метрологическая надежность (ресурс) ОПС повысится в m=5 раз.

Ресурсная методология была апробирована на разработанной конструкции волоконно-оптического пожарного извещателя, обладающего многофункциональностью и выполняющего функции УТС [6].

Использованной литературы:

1. Мавлянкариев Б. А. Информационно-техническое обеспечение подсистем оперативного прогнозирования пожаровзрывоопасных ситуаций в АСУТП объекта. //Материалы 7-ой международной конференции «Системы безопасности СБ-98». М.: 1999. с.54-55.

2. Брушлинский Н.Н. и др. Игровое моделирование и пожарная безопасность. М.: 1993.

3. Мавлянкариев Б.А., Фомин В.В. Упреждающий прогноз в АСУТП пожаро-взрывоопасного производства, /Тез. Докл.9 Всес. НТК «Математическое, алгоритмическое и техническое обеспечение АСУТП». -Ташкент. 1998.

4. Надёжность систем энергетики. Терминология. М.: Наука, 1980.

5. ГОСТ 25 329-81. Установки пожаротушения автоматические и установки пожарной и охранно-пожарной сигнализации. Обозначения условно-графических элементов М.: Минприбор 1981.

6. Мавлянкариев Б.А. Многофункциональные датчики для высокорисковых пожаро и экологические опасных систем. //Материалы 8-ой международной конференции «Системы безопасности СБ-99». М.: 1999. с.58-59.

MUDOFAA SOHASIDAGI HARBIY SUN'IY INTELLEKTNING AFZALLIKLARI VA MUAMMOLARI

Saidbayev B.Dj.

"Axborot texnologiyalari" kafedrasi dotsenti t.f.f.d (PhD) dotsent,

Sun'iy intellekt (AI) harbiy sohada dala operatsiyalari samaradorligi va aniqligini oshirish, bashoratli tahlil va logistika va boshqa sohalar uchun tobora ko'proq foydalanilmoqda. Katta hajmdagi ma'lumotlarni Real vaqt rejimida qayta ishlash va avtonom tarzda o'rganish qobiliyati mudofaa va milliy xavfsizlik sohasida AIning ulkan salohiyatini keltirib chiqaradi.

Shu bilan birga, undan foydalanish, shuningdek, qarorlar qabul qilishning shaffofligi va xatolar yoki garovga yetkazilgan zarar uchun

javobgarlik kabi jiddiy axloqiy va huquqiy muammolarni keltirib chiqaradi.

Ba'zi fuqarolik texnologiya kompaniyalari, ayniqsa mudofaa pudratchilari, harbiy AI sohasida faol ish olib borishmoqda. Biroq, sun'iy intellektning harbiy tizimlari hujumlar va ruxsatsiz kirish yoki tasodifan katta zarar yetkazishi mumkin degan xavotirlar mavjud. Hozirgi geosiyosiy beqarorlik sharoitida mas'uliyat va shaffoflik masalalari ham paydo bo'lmoqda, ayniqsa AQSh, Xitoy, Rossiya, Eron, Turkiya [4] va Isroil, boshqa davlatlar qatorida [32] keng ko'lamli harbiy maqsadlar uchun sun'iy intellektni ishlab chiqishda yetakchilik qilmoqda. Harbiy darajadagi sun'iy intellektning salohiyati juda katta va xilma-xildir. Uning ahamiyati milliy xavfsizlik bilan bog'liq bo'lishi mumkin bo'lgan naqsh va tendensiyalarni aniqlash uchun sun'iy yo'ldosh tasvirlari, razvedka signallari, xabarlar va ijtimoiy tarmoqlar kabi turli manbalardan olingan katta hajmdagi ma'lumotlarni tahlil qilish qobiliyatidir. Ushbu imkoniyat bilan xavfsizlik kameralari tasvirlari va video maqsadlarini aniqlash jang maydonida muhim ma'lumotlarni taqdim etadi.

Bu bizni qurol tizimlarida va avtonom transport vositalarida, masalan, inson aralashuvi minimal bo'lgan uchuvchisiz havo vositalari, quruqlikdagi transport vositalari va havo mudofaa tizimlarida foydalanishga olib keladi.

Shu sababli, ushbu tadqiqotning maqsadi harbiy harakatlar va mudofaa tizimlarida sun'iy intellektdan foydalanishning afzalliklari va muammolarini o'rganishdir. Shu maqsadda tadqiqot savoli shakllantirildi: sun'iy intellekt imkoniyatlarini harbiy sohaga integratsiya qilish bilan bog'liq asosiy afzalliklar va axloqiy muammolar qanday? Metodologiya harbiy kontekstda sun'iy intellektni qo'llash bo'yicha mavjud adabiyotlarni sifatli ko'rib chiqishga asoslangan.

Sharh mudofaa faoliyati uchun AIning hujjatlashtirilgan afzalliklarini, shuningdek, ekspertlar va tadqiqotchilar tomonidan aniqlangan axloqiy, huquqiy va xavfsizlik bilan bog'liq xavflarni tahlil qiladi. Mudofaa sohasida AIning mas'uliyatli rivojlanishi uchun istiqbolli

yo‘nalishlar va kafolatlarni aniqlash uchun harbiy AI qobiliyatlari, nazorat va boshqaruv bilan bog‘liq asosiy mavzular umumlashtiriladi.

2 Harbiy darajali sun’iy intellekt

Harbiy darajadagi sun’iy intellekt harbiy va mudofaa maqsadlarida maxsus ishlab chiqilgan va qo‘llaniladigan AI tizimlarini nazarda tutadi [16]. Ushbu AIlar qat’iy talablarni qondirish va harbiy muhit bilan bog‘liq muammolarni hal qilish uchun mo‘ljallangan [5], bu erda potensial raqiblarga nisbatan hal qiluvchi ustunlik talab qilinadi. Ushbu turdagi AIning ba’zi xususiyatlari quyida batafsil tavsiflangan:

- Ishonchlilik va barqarorlik: ushbu sun’iy intellektlar ishonchli ishlash va og‘ir sharoitlarga bardosh berish uchun mo‘ljallangan. Ular turli xil sharoitlarda, ko‘pincha haddan tashqari stress sharoitida ishlashga qodir bo‘lishi kerak. Bu shuni anglatadiki, ular dushman muhitida harakat qilishlari va jangovar urush zonalari kabi jismoniy shikastlanishga qarshi turishlari va hatto halaqitlar yoki kiberhujumlar mavjud bo‘lganda ham o‘z funksiyalarini saqlab qolishlari kerak [6].

- Qayta ishlash quvvati: ushbu sun’iy intellekt katta hajmdagi ma’lumotlarni to‘g‘ri qayta ishlashni ta’minlaydigan ilg‘or hisoblash qobiliyatiga ega. Ular ma’lumotlarni tahlil qilish va qayta ishlashning murakkab vazifalarini tez va samarali bajarishga qodir. Bu shuni anglatadiki, ularning loyihalanishi va ishlab chiqarishi ko‘p hollarda individualdir.

– Avtonomiya: Ko‘pgina harbiy ilovalar doimiy inson nazoratisiz avtonom tarzda ishlay oladigan AI tizimlarini talab qiladi. Bu jang maydoni bo‘ylab dronni boshqarish, maqsadlarni aniqlash va kuzatish yoki logistika va ta’minot zanjirlarini boshqarish kabi vazifalarni o‘z ichiga oladi.

– Moslashuvchanlik: ushbu turdagi AI yuqori darajada moslashuvchanlikka ega va turli vaziyatlarga va jang maydonidagi o‘zgaruvchan ssenariylarga moslasha oladi.

Ular yangi ma’lumotlarni olishlari va vaziyat o‘zgarishi bilan o‘z modellari va algoritmlarini o‘rganishlari va yangilashlari mumkin.

– Qaror qabul qilish: AI tizimlari ko‘pincha ma’lumotlarning o‘zgaruvchan dinamikasi tufayli real vaqt rejimida qaror qabul qilishi kerak, ilg‘or algoritmlar va yuqori samarali hisoblash quvvati talab qilinadi.

– O‘zaro hamkorlik: bu tizimlar ko‘pincha harbiy platformalar kabi boshqalar bilan integratsiyalashishi kerak. Shuning uchun, ular imkon qadar standart protokollar va interfeyslardan foydalangan holda o‘zaro hamkorlikni hisobga olgan holda ishlab chiqilishi kerak, chunki ularning xavfsizlik xususiyatlari AES-256, OMEMO yoki ZRTP kabi mustahkam shifrlangan aloqa protokollari bilan ishlashni talab qiladi.

– Xavfsizlik va maxfiylik: Vazifalarining nozik xususiyatini hisobga olgan holda, harbiy darajadagi AI tizimlari qat’iy xavfsizlik va maxfiylik standartlariga ega bo‘lishi kerak. Bunga shifrlash, xavfsiz aloqa kanallari va buzg‘unchilik yoki ruxsatsiz kirishni oldini olish choralari kiradi. Chiplar (mikrosxema) konstruksiyasi kiberhujumlarga, ma’lumotlarning buzilishiga, uskunaning ishdan chiqishiga va boshqa tahdidlarga bardosh berishi kerak, chunki ular yuqori xavfli harbiy operatsiyalarda qo‘llaniladi.

– Chiplar konstruksiyasi kiberhujumlarga, ma’lumotlarning buzilishiga, uskunaning ishdan chiqishiga va boshqa tahdidlarga bardosh berishi kerak, chunki ular yuqori xavfli harbiy amaliyotlarda qo‘llaniladi.

– Axloqiy mulohazalar: Ushbu turdagi AIdan foydalanish bir nechta axloqiy mulohazalarni keltirib chiqaradi. Ushbu tizimlar xalqaro huquqni hurmat qiladigan va tinch aholiga zarar yetkazish xavfini kamaytiradigan tarzda ishlab chiqilishi kerak [[29]].

- Inson va mashinaning o‘zaro ta’siri: Ushbu AIlar avtonom yoki inson operatorlari bilan hamkorlikda ishlashi mumkin. Operatorlar aqlli qarorlar qabul qilishni qo‘llab-quvvatlash uchun sun’iy intellektni qayta ishlash va tahlil qilish imkoniyatlaridan foydalanishlari mumkin bo‘lgan harbiy muhitda inson va mashinaning o‘zaro ta’siri muhim ahamiyatga ega.

1-jadvalda harbiy darajadagi sun’iy intellektning konstruksiyasi, ishlashi, funksionalligi va umumiy ko‘rinishda qo‘llanilishi bo‘yicha xususiyatlari jamlangan. Buning sababi shundaki, uni amalga oshirish va

aniq spetsifikatsiyalar harbiy yoki razvedka idorasi bo‘lsin, har bir tizimning ehtiyojlari va talablariga qarab farqlanadi.

1-jadval Harbiy darajadagi sun’iy intellektning xususiyatlari

Xususiyat	Tavsif
Dizayn	Harbiy maqsadlarda foydalanish uchun maxsus ishlab chiqilgan.
	Ilg‘or algoritmlar va mashinani o‘rganish imkoniyatlarini o‘z ichiga oladi.
	Ekstremal ob-havo sharoitlari, shovqinlar va kiberhujumlar kabi qiyin muhitlarga moslashadi.
Operativlik	U avtonom yoki inson operatorlari bilan hamkorlikda ishlashi mumkin.
	Harbiy platformalar va tizimlar, masalan, uchuvchisiz uchish va transport vositalari, kuzatuv tizimlari va qurollar bilan birlashtirilgan.
	Maxfiy ma’lumotlarni himoya qilish uchun qat’iy xavfsizlik va maxfiylik protokollariga rioya qiling
Funksionallik	real vaqt rejimida tasvir va videoni tanib olish va qayta ishlash
	qaror qabul qilish uchun razvedka ma’lumotlarini tahlil qilish va baholash
	Ssenariylarni bashorat qilish va modellashtirish qobiliyati
	real vaqtda tahdidlarni aniqlash va ularga javob berishda yordam berish
Ilovalar	Jang maydonida kuzatuv va razvedka.
	Mudofaa perimetri.
	Robotlar va dronlar yordamida portlovchi moddalarni yo‘q qilish.
	Dushman nishonlarini aniqlash va kuzatish.
	Qidiruv-qutqaruv operatsiyalarida yordam berish.
	Harbiy strategiyalarni yaratish uchun ma’lumotlarni tahlil qilish.
	Harbiy xizmatchilar uchun simulyatsiya va virtual mashg‘ulotlar.

Xususiyat	Tavsif
	harbiy texnika va tizimlardagi nosozliklarni bashorat qilish va oldini olish
	Yuzni identifikatsiyalash uchun aqlli smart kameralar
	Shahar sharoitida taktik harakatlar
	Sintetik aperturali radarlar
	DNK profilini aniqlash algoritmlari.
	intellektni tiklanishi .
	assimetrik urush .
	raqamli aktivlar va muhim infratuzilmani himoya qilish uchun kiberxavfsizlik.
	Kibermudofaa va kiberhujumlar.
	Audio va tasvirlarni manipulyatsiya qiluvchi soxta dezinformatsiya.
	ob-havo sharoitlarini bashorat qilish

Ushbu turdagi sun’iy intellektning boshqa qo‘shimcha tafsilotlari shundaki, ular ko‘pincha o‘quv maqsadlari uchun katta hajmdagi ma’lumotlarga, jumladan, harbiy razvedka, kuzatuv ma’lumotlari va mojarolar va urush o‘yinlaridan olingan ma’lumotlarga kirishlari mumkin. Bu ularga tezroq o‘rganish va yuqori samaradorlik darajasiga erishish imkonini beradi.

Buning imkoni bo‘lishi uchun tijoratda mavjud bo‘lganidan tashqarida bo‘lgan zamonaviy sun’iy intellekt texnikasi talab qilinadi. Ba’zilari AIga ixtisoslashgan kompaniyalar va harbiy pudratchilar tomonidan ishlab chiqilgan bo‘lib, ularning o‘ziga xos qoidalari va siyosati mudofaa va milliy xavfsizlik bilan bog‘liq ilovalarga qaratilgan.

AI bilan bog‘liq texnologiya o‘zining ishlanmalari va qiyinchiliklarini taqdim etadi, masalan, qurolli va xavfsizlik kuchlari ichidagi turli funksiyalar uchun ixtisoslashgan AI chiplari. Masalan, havo ustunligi va mudofaa uchun sun’iy intellekt maqsadlarni aniqlash va kuzatish uchun ko‘rish tizimlari va mashinalarni o‘rganishdan foydalanadi.

Harbiy sun'iy intellektning umumiy xususiyatlari mashinani o'rganish, kompyuterni ko'rish va boshqalar nuqtai nazaridan tijorat AIga o'xshasa-da, ko'lami, ishlashi, xavfsizligi, etikasi va harbiy xizmatdagi roli bu tizimlarni tijoratda mavjud bo'lganlardan ajratib turadi. Bundan tashqari, ushbu texnologiyaga sarmoya kiritish uchun ajratilgan resurslar ko'proq va shuning uchun AI texnologiyasining chegaralarini kengaytiradi.

AIdan halokatli maqsadlarda foydalanish bilan bog'liq axloqiy savollar mavjud. Ba'zilarning ta'kidlashicha, AI hujumlarni amalga oshirish uchun emas, balki faqat himoya yoki qo'llab-quvvatlash funksiyalari uchun ishlatilishi kerak. Biroq, boshqalar AI qurollari muqarrar bo'lishiga ishonishadi va asosiy e'tibor ularning mas'uliyat bilan ishlatilishini ta'minlashga qaratilishi kerak .

Ba'zi ekspertlar odamlar sun'iy intellektni o'z ichiga olgan har qanday qurol tizimi ustidan har doim yakuniy nazoratni saqlab turishi kerakligini ta'kidlaydilar. Boshqalar, to'liq avtonomiya muqarrar va texnologik yutuqlarni potensial tahdidlardan kuzatib borish uchun zarur deb hisoblaydi, ayniqsa, bugungi kunda geosiyosiy dinamika tobora beqaror bo'lsa.

Ko'rib chiqilishi kerak bo'lgan yana bir jihat - tinch aholiga josuslik qilish uchun harbiy AIdan foydalanish mumkin. Ayg'oqchilik yangilik bo'lmasa-da, bu maqsadda sun'iy intellektdan foydalanish yangi, ayniqsa, bu harakatlar nafaqat militsiya, balki tinch aholi tomonidan ham amalga oshiriladi. Bu harbiy AI ishlanmalari shaxsiy hayot, kuzatuv va kundalik hayotning boshqa jihatlariga salbiy ta'sir ko'rsatishi mumkin bo'lgan turli kontekstlarda muqarrar ravishda fuqarolik hayotiga kirib borayotganiga misoldir.

Harbiy darajadagi AIlar boshqa jihatlar qatorida ilg'or qayta ishlash imkoniyatlari, moslashuvchanlik va xavfsizlikni hisobga olgan holda, turli sohalarda harbiylarning ehtiyojlarini qondirish uchun mo'ljallangan. Uning qo'llanilishi tan olish va kuzatishdan tortib strategik qarorlar qabul qilish uchun bashoratli tahlilgacha. Uning maqsadi avtonom transport vositalari (masalan, uchuvchisiz samolyotlar yoki uchuvchisiz

suv osti kemalari), kiber mudofaa, logistika va ta'minot zanjiri boshqaruvi kabi harbiy operatsiyalarning samaradorligi va samaradorligini oshirishdan iborat.

Binobarin, sun'iy intellekt tizimlari ham kibermudofaa, ham kiberjinoyatchilik maqsadlarida tobora ko'proq qo'llanilar ekan, ushbu texnologiyalardagi taraqqiyotning murakkab axloqiy va xavfsizlik oqibatlarini boshqarishda yordam berish uchun ehtiyotkorlik bilan xalqaro boshqaruv va nazorat kelajakda juda muhim bo'ladi.

Foydalanilgan adabiyotlar:

1. Альварес , Э. (2023). Машинное обучение: Аси функция дисциплины , которая помогает понять компьютеры ученику пор да mismas . https://tn.com.ar/tecno/novedades/2023/05/29/machine-learning-asi-funciona-la-disciplinaque-les-ensena-a-las-computadoras-a-aprender-por-si-mismas/E . [Links]

2. Балестриеро , Р., Ибрагим, М., Собаль , В., Моркос , А., Шехар , С., Голдштейн, Т., Голдблюм, М. (2023). Рецепт самостоятельного обучения. Препринт arXiv arXiv:2304.12210. DOI: 10.48550/arXiv.2304.12210. [Ссылки]

"JXU TRACKER" AXBOROT TEXNOLOGIYALARI ASOSIDA JAMOAT XAVFSIZLIGINI TA'MINLASH VOSITASI

Shaymardonov J.Z.
JXU, Ilmiy-amaliy tadqiqotlar markazi katta ilmiy xodimi.

Globallashuv jarayonlari, urbanizatsiya sur'atlarining oshishi va transport vositalari sonining keskin ko'payishi jamoat xavfsizligini ta'minlashni zamonaviy bosqichga olib chiqmoqda. So'nggi yillarda O'zbekiston Respublikasida sezilarli darajada transport vositalari soni ortib bormoqda. **2024**-yil yakuniga kelib ular **4,2 million**dan oshdi. Statistik ma'lumotlarga ko'ra, **2023**-yilda yo'l-transport hodisalari soni **10 ming**dan ortiqni tashkil qilgan. [1][2][8] Hodisalarning orasida **YPX** xodimining qonuniy talabiga bo'ysunmasdan qochishga uringanda yuzaga kelgan holatlar ham mavjud bo'lishi mumkin. Ushbu muammoni hal etish

uchun zamonaviy axborot texnologiyalariga asoslangan innovatsion vositalardan foydalanish zarur.

Shunday innovatsion vositalardan biri sifatida **JXU Tracker** qurilmasini keltirish mumkin. Uning joriy etilishi nafaqat **YPX** faoliyatini samarali tashkil qilishga, balki fuqarolarning huquq va erkinliklarini himoya qilishga ham xizmat qiladi.

JXU Tracker – GPS/GSM texnologiyalariga asoslangan kuzatuv vositasi bo‘lib, **YPX** xodimlari tomonidan to‘xtash ishorasiga bo‘ysunmasdan qochib ketayotgan transport vositalarini masofadan kuzatishda qo‘llaniladi. Qurilma transport metal qismiga maxsus magneti yordamida yopishtirish yo‘li bilan biriktiriladi hamda real vaqt rejimida transport vositasining koordinatalari, tezligi va yo‘nalishini qayd etadi. Bunday texnologiyalar jamoat xavfsizligini ta’minlash samaradorligini oshirishda muhim ahamiyatga ega.

O‘zbekiston Respublikasi **IIV Yo‘l harakati xavfsizligi bosh boshqarmasi** ma’lumotlariga ko‘ra, **2022**-yilda **9 870** ta yo‘l-transport hodisasi ro‘y bergan, **2023**-yilda esa **10 524** ta hodisa qayd etilgan. Hodisalarni tahlil qilganda, **18–20 foizi YPX**ning to‘xtash signaliga bo‘ysunmagan haydovchilar bilan bog‘liq. Ayrim hollarda qochib ketayotgan transport vositalarining **35 foizi** tezlikni keskin oshirishi oqibatida **og‘ir yo‘l-transport hodisalari**ga sabab bo‘lgan.[1]

Xorijiy davlatlar tajribasi shuni ko‘rsatadiki, **Germaniya** va **AQSh**da **GPS-treker**lardan foydalanish yo‘l-transport hodisalari sonini **12–15 foiz**ga kamaytirgan.[3][4] **Koreya Respublikasi**da esa ushbu texnologiyalar joriy qilingach, huquqbuzarliklar **20 foiz**ga qisqargan.[5] Demak, **JXU Tracker** O‘zbekistonda ham ijobiy natija berishi mumkin.



JXU Tracker qurilmasi huquqiy jihatdan ham, ijtimoiy nuqtai nazardan ham katta ahamiyat kasb etadi. U jinoyat va huquqbuzarliklarni tezkor aniqlash, dalillarni ishonchli qayd etish imkonini beradi. Fuqarolarning teng huquqliligini ta’minlash, jamoat xavfsizligini mustahkamlash va qonun ustuvorligini yuksaltirishda muhim rol o‘ynaydi.[6][10]

Xalqaro miqyosda bunday texnologiyalar ko‘plab davlatlarda qo‘llanib kelmoqda. Masalan, **AQSh**da yo‘l patrul xizmati tomonidan qo‘llaniladigan elektron kuzatuv tizimlari jinoyatlarning oldini olishda katta samara bermoqda.[10] **Germaniya**da esa ushbu qurilmalar yordamida nafaqat qochayotgan transport vositalari, balki ekologik me’yorlarni buzayotgan avtomobillar ham kuzatuvga olinmoqda.[3]

JXU Tracker qurilmasini keng joriy etish iqtisodiy nuqtai nazardan ham foydali. Chunki yo‘l-transport hodisalari oqibatida davlatga va jamiyatga yetkaziladigan moddiy zarar kamayadi.[7] Bundan tashqari, **YPX** faoliyatini optimallashtirish orqali qo‘shimcha xarajatlar qisqaradi.

O‘zbekiston sharoitida **JXU Tracker** qurilmasini samarali joriy qilish uchun bir necha choralarni amalga oshirish lozim: bosqichma-bosqich o‘rnatish, ma’lumotlarni markazlashtirish, xodimlarning malakasini oshirish va texnik xizmat ko‘rsatishni mahalliy ishlab chiqaruvchilar asosida tashkil qilish.

Yuqorida keltirilgan fikrlar asosida aytish mumkinki, **JXU Tracker** qurilmasi axborot texnologiyalari asosida jamoat xavfsizligini ta'minlashda muhim innovatsion vositadir. Qurilmani keng joriy etish **YPX** faoliyatining samaradorligini oshirish, yo'l-transport hodisalarini kamaytirish va fuqarolarning huquqlarini himoya qilishga xizmat qiladi. Shuningdek, xalqaro tajribani o'zlashtirish orqali O'zbekistonda huquqiy tizimni takomillashtirishga katta hissa qo'shadi.

Foydalanilgan adabiyotlar:

1. O'zbekiston Respublikasi Ichki ishlar vazirligi Yo'l harakati xavfsizligi bosh boshqarmasi hisobotlari, 2022–2023-yillar.
2. "Yo'l harakati xavfsizligi to'g'risida"gi Qonun, O'zbekiston Respublikasi Oliy Majlisi, 1999-yil.
3. Bundespolizei Deutschland: Traffic Safety Annual Report, Berlin, 2021.
4. U.S. Department of Transportation, Highway Safety Report, Washington DC, 2020.
5. Lee, J. & Park, S. Smart Tracking Technologies in Public Safety, Seoul, 2019.
6. Karimov, B. "Axborot texnologiyalari va jamoat xavfsizligi", Toshkent davlat yuridik universiteti ilmiy jurnali, 2022-yil.
7. International Transport Forum, OECD Report on Road Safety, Paris, 2021.
8. World Health Organization. Global status report on road safety, Geneva, 2019.
9. European Commission, Road Safety Statistics, Brussels, 2020.
10. Smith, A. Digital Policing and Public Safety, London, 2018.

VIDEOKUZATUV TIZIMLARIDA TASVIR SIFATINI BAHOLASH TADQIQOTI

Bozorov A.A.
O‘zbekiston Respublikasi Jamoat xavfsizligi
universiteti QMTT kafedrasi, o‘qituvchisi

Bugungi kunda videokuzatuv tizimlari nafaqat davlat va harbiy obyektlarda, balki transport, bank, sanoat va ijtimoiy infratuzilma xavfsizligini ta’minlashda ham muhim o‘rin tutmoqda. Videokuzatuv tizimlarining samaradorligi to‘g‘ridan-to‘g‘ri tasvir sifatiga bog‘liq bo‘lib, tasvirning aniqligi va barqarorligi xavfsizlik xodimlari yoki sun’iy intellekt algoritmlari tomonidan obyektlarni to‘g‘ri aniqlash va tahlil qilish imkoniyatini belgilab beradi [1].

Tasvir sifatini pasaytiruvchi omillar odatda ikki toifaga ajratiladi: tashqi muhit sharoitlari (yorug‘likning yetishmasligi, ob-havo ta’siri, chang va tuman) hamda texnik cheklovlar (kamera datchigi, optika sifatining pastligi, raqamli siqish algoritmlari, tarmoq kechikishlari) [2]. Shu sababli, videokuzatuv tizimlari samaradorligini ta’minlash uchun mazkur omillarni ilmiy jihatdan chuqur tahlil qilish va ularni bartaraf etish usullarini ishlab chiqish dolzarb hisoblanadi.

Videotasvir sifati subyektiv va obyektiv ko‘rsatkichlar orqali baholanadi. Xalqaro standartlar, xususan ITU-T Rec. P.910 [4] va ISO/IEC 23009-1 [5] videokuzatuv oqimlarining sifatini aniqlash va taqqoslash uchun mezonlarni belgilab bergan. Bu mezonlar orasida eng ko‘p qo‘llaniladigan obyektiv ko‘rsatkichlar – PSNR (Peak Signal-to-Noise Ratio) va SSIM (Structural Similarity Index Measure) bo‘lib, ular videokuzatuv tizimlarida sifat monitoringini amalga oshirishda keng qo‘llanadi.

Videokuzatuv tizimlarida tasvir sifatini pasaytiruvchi omillarni ilmiy asosda o‘rganish uchun ularni uch asosiy guruhga ajratish maqsadga muvofiq deb topildi:

Fizik omillar – tashqi muhit sharoitlari: yorug‘likning yetarli emasligi, tuman, chang, yomg‘ir, qor kabi tabiiy to‘siqlar. Bu omillar tasvirning kontrasti va yorqinligini sezilarli darajada kamaytiradi [2].

Texnik omillar – kamera va optik tizim sifatiga bog‘liq bo‘lgan buzilishlar. Datchiklarning past sezgirligi, linzalardagi aberatsiya va distorsiya, shuningdek raqamli siqish algoritmlarida yuzaga keladigan artefaktlar tasvirni buzadi [1], [3].

Tarmoq omillari – videoma’lumotlarni uzatish jarayonida yuzaga keladigan kechikish, paket yo‘qotish va past tarmoqli kengligi. Bu holatlar oqibatida real vaqt rejimidagi kuzatuv tizimlari uzilishlarga duch keladi [5].

Sifatni baholash metodlari

Tadqiqotlarda tasvir sifatini baholash uchun obyektiv va subyektiv yondashuvlardan foydalaniladi:

Obyektiv ko‘rsatkichlar:

PSNR (Peak Signal-to-Noise Ratio) – tasvir va etalon orasidagi shovqin darajasini aniqlashda qo‘llaniladi. Bu ko‘rsatkich asosan texnik tahlillarda keng ishlatiladi [1].

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

Bu yerda: MAX_I – maksimal yorqinlik qiymati, MSE – kvadrat xatolik o‘rtacha qiymati.

SSIM (Structural Similarity Index Measure) – inson ko‘zi qabul qiladigan strukturaviy o‘xshashlikni baholash uchun samarali ko‘rsatkich [4].

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$

Bu yerda: μ_x, μ_y – o‘rtacha qiymatlar; σ_x, σ_y – dispersiyalar; σ_{xy} – kovariatsiya; C_1, C_2 – barqarorlashtiruvchi konstantalar.

Subyektiv baholash:

Xalqaro ITU-T P.910 [4] standartida tasvir sifatini inson ishtirokida test qilish metodlari ishlab chiqilgan. Bu yondashuv foydalanuvchilarning haqiqiy vizual tajribasini hisobga olish imkonini beradi.

Shovqinlarni kamaytirish va sifatni tiklash metodlari

Metodologiyaning muhim qismi sifatida shovqinlarni kamaytirish va sifatni tiklash texnologiyalari tanlab olindi:

Klassik filtrlash usullari: Gaussian filter, Median filter, Bilateral filter – ular oddiy va tezkor, biroq yuqori sifatli tiklashda cheklovlarga ega [1].

Chuqur o‘rganishga asoslangan metodlar: Denoising CNN (DnCNN) va GAN asosidagi Super-Resolution tarmoqlari – bu usullar murakkab, ammo yuqori sifatli natijalar beradi [6], [7], [8].

Zhang va hamkorlari [7] tomonidan ishlab chiqilgan residual learning modeli tasvirlarni shovqindan tozalashda klassik Gaussian filtrlashga qaraganda samaraliroq natija bergan. Ledig va boshqalar [8] tomonidan taklif etilgan GAN asosidagi super-resolution modeli esa past sifatli kadrlarni yuqori aniqlikda qayta tiklash imkonini bergan.

Tadqiqot yondashuvi

Metodologiya quyidagi bosqichlarda amalga oshiriladi:

Videokuzatuv tizimlarida turli omillarning ta’sirini modellashtirish (yorug‘lik darajasi, shovqin darajasi, tarmoq kechikishi).

Har bir holatda tasvir sifatini obyektiv ko‘rsatkichlar – PSNR va SSIM orqali baholash.

Klassik filtrlash usullari va chuqur o‘rganishga asoslangan metodlarni taqqoslab, qaysi sharoitda samaraliroq natija berishini aniqlash.

Olingan natijalarni xalqaro standartlar (ITU-T P.910, ISO/IEC 23009-1) bilan solishtirish [4], [5].

Videokuzatuv tizimlarida tasvir sifatiga ta’sir etuvchi omillarni modellashtirish orqali ularning obyektiv ko‘rsatkichlardagi o‘zgarishlari aniqlanadi.

Kameralar turli yorug‘lik sharoitida sinovdan o‘tkazildi. Olingan natijalar quyidagi 1-jadvalda keltirilgan:

1-jadval

Kameralarning turli yorug‘lik sharoitidagi sinov tasvirlari tavsifi

Yorug‘lik darajasi (lux)	**PSNR (dB)**	**SSIM**	**Izoh**

500 lux (normal sharoit)	38.5	0.96	Tasvir juda tiniq
100 lux (past yorug‘lik)	31.2	0.85	Shovqinlar sezilarli
10 lux (juda past)	24.7	0.69	Tasvir kontrasti pasaygan
1 lux (deyarli qorong‘i)	18.9	0.52	Detallar yo‘qolib ketgan

Natijalardan ko‘rinib turibdiki, yorug‘lik darajasi pasayganda PSNR qiymati keskin tushib ketadi va SSIM ham sezilarli ravishda kamayadi. Bu inson ko‘zi uchun sezilarli sifat yo‘qotishiga olib keladi [2], [3].

Turli shovqin modellari (AWGN – additive Gauss oq shovqin, impuls shovqin, kvantlash shovqini) sinovdan o‘tkazildi. Natijalar quyidagicha bo‘ldi (2-jadval):

2-jadval

Turli shovqin modellari sinov natijalari

Shovqin turi	**Shovqin darajasi (σ)**	**PSNR (dB)**	**SSIM**	**Izoh**
AWGN	σ = 10	30.1	0.83	Tasvirdagi mayda donachalar
	σ = 20	26.8	0.72	Shovqin ko‘proq seziladi
Impuls shovqin	10%	24.5	0.64	“Tuz va murch” effektlari
Kvantlash shovqini	–	28.7	0.78	Kompressiya ta’siri sezilarli

Video oqimlarni MPEG va H.264 siqish algoritmlari orqali uzatishda Tarmoq kechikishlari va siqish algoritmlarining ta’siri baholandi [3], [5] (3-jadval).

3-jadval

Tarmoq kechikishlari va siqish algoritmlarining ta’siri

Algoritm	**Bitreyt (kbps)**	**PSNR (dB)**	**SSIM**	**Izoh**
MPEG-2	512	28.6	0.75	Artefaktlar va bloklar seziladi
H.264/AVC	512	32.4	0.84	Nisbatan sifat yaxshiroq
H.264/AVC	1024	36.7	0.91	Sifat yuqori, artefaktlar deyarli yo‘q

Natijalar shuni ko‘rsatadiki, bitreyt ortishi bilan PSNR va SSIM ko‘rsatkichlari yaxshilanadi. Shu bilan birga, H.264 algoritmi MPEG-2 ga qaraganda samaraliroq ekanligi tasdiqlandi [3], [5].

Olib borilgan tadqiqotlar natijalari videokuzatuv tizimlarida tasvir sifatiga ta’sir etuvchi omillar murakkab va ko‘p qirrali ekanligini ko‘rsatdi. Natijalardan ma’lum bo‘ldiki, yorug‘lik darajasi, shovqinlar va siqish algoritmlari sifat pasayishining eng asosiy sabablari bo‘lib hisoblanadi.

1. Yorug‘lik darajasi ta’siri

Yorug‘lik darajasi pasaygan sari PSNR va SSIM ko‘rsatkichlari sezilarli ravishda kamaygani kuzatildi. Bu inson ko‘zi uchun tasvir kontrasti va detallarining yo‘qolishiga olib keladi. Masalan, 500 lux sharoitida PSNR 38.5 dB bo‘lgan bo‘lsa, 1 lux sharoitida u 18.9 dB gacha tushib ketdi. Bu natija Szeliski [2] tomonidan ta’kidlangan fikrni tasdiqlaydi: kamera datchiklari past yorug‘likda yuqori shovqin hosil qiladi va obyektlarni aniqlash qiyinlashadi.

2. Shovqinlarning ta’siri

Oq shovqin (AWGN) va impulsiv shovqin modellashtirilganda, impulsiv shovqin eng katta salbiy ta’sir ko‘rsatdi. Bu Gonzalez va Woods [1] ta’kidlaganidek, “salt-and-pepper noise” tasvirdagi asosiy konturlarni ham buzishi bilan izohlanadi.

Shovqinlarni kamaytirishda klassik filtrlash metodlari (Gaussian filter, Median filter) qo‘llanildi. Gaussian filtr AWGN shovqini uchun samarali bo‘lsa-da, impulsiv shovqinda deyarli foyda bermadi. Median filter esa impulsiv shovqinlarga nisbatan kuchliroq natija berdi.

3. Klassik filtrlash va chuqur o‘rganish usullarining taqqoslanishi

Natijalar quyidagi jadvalda umumlashtirilgan:

4-jadval

Umumlashtirilgan natijalar

Shovqin turi	**Metod**	**PSNR (dB)**	**SSIM**	**Izoh**
AWGN (σ=20)	Gaussian filter	28.4	0.78	Mayda donachalar biroz saqlanib qoladi
AWGN (σ=20)	DnCNN [7]	32.9	0.88	Shovqin samarali bartaraf etilgan

Impulsiv shovqin 10%	Median filter	25.1	0.66	Tuz va murch effektlari kamayadi
Impulsiv shovqin 10%	DnCNN [7]	29.3	0.81	Detallar yaxshiroq tiklangan

Bu jadvaldan ko‘rinib turibdiki, chuqur o‘rganishga asoslangan DnCNN modeli klassik filtrlarga qaraganda ancha yuqori natija berdi. Bu Goodfellow va hamkorlari [6] hamda Zhang va boshqalar [7] tomonidan ilmiy asoslangan xulosalar bilan hamohangdir.

4. Siqish algoritmlari va super-resolution

Siqish algoritmlarida (MPEG-2 va H.264) sifat farqlari kuzatildi. H.264 algoritmi past bitreytlarda ham yuqoriroq PSNR va SSIM ko‘rsatkichlarini berdi [3], [5].

Sifatni tiklash uchun super-resolution GAN (SRGAN) modeli sinovdan o‘tkazildi. Ledig va boshqalar [8] tomonidan taklif etilgan ushbu model siqilgan tasvirlarni qayta tiklashda yuqori samaradorlik ko‘rsatdi (5-jadval):

5-jadval

Tahlil natijalari

Algoritm	**Siqilgan tasvir PSNR (dB)**	**SRGAN tiklangan PSNR (dB)**	**SSIM yaxshilanishi**
MPEG-2	28.6	33.1	+0.09
H.264/512k	32.4	36.8	+0.07

Bu natijalar shuni ko‘rsatadiki, chuqur o‘rganishga asoslangan GAN modellaridan foydalanish tasvir sifatini sezilarli darajada yaxshilaydi va bu amaliy qo‘riqlash tizimlari uchun dolzarb yo‘nalishdir.

5. Muhokama yakuni

Umuman olganda, natijalar quyidagilarni ko‘rsatdi:

Past yorug‘lik sharoitida sifat keskin pasayadi, kamera datchiklarining sezgirligini oshirish talab qilinadi.

Shovqinlarni kamaytirishda klassik filtrlash usullari ba’zi holatlarda samarali bo‘lsa-da, chuqur o‘rganish modellaridan foydalanish natijani ancha yaxshilaydi.

Siqish algoritmlari sifatiga ta’sir etuvchi asosiy omil bitreyt hisoblanadi, H.264 esa MPEG-2 ga qaraganda samaraliroq.

GAN asosidagi super-resolution metodlari real qo‘riqlash tizimlarida siqilgan videolar sifatini tiklashda istiqbolli yechimdir.

Videokuzatuv tizimlarida tasvir sifati kuzatuv samaradorligini belgilovchi eng muhim omillardan biridir. Ushbu tadqiqot natijalari shuni ko‘rsatdiki, tasvir sifatini pasaytiruvchi asosiy sabablar quyidagilardan iborat:

Fizik omillar – yorug‘lik yetishmovchiligi, atmosfera sharoitlari (tuman, yomg‘ir, qor) va tashqi muhitdagi sharoitlar tasvir kontrasti va aniqligini keskin pasaytiradi [2].

Texnik omillar – kamera datchiklarining sezgirligi, linzalardagi aberatsiya, hamda siqish algoritmlarida yuzaga keladigan artefaktlar sifatsiz videotasvirlarga olib keladi [1], [3].

Tarmoq omillari – bitreytning pastligi, paketlarning yo‘qolishi va tarmoqdagi kechikishlar oqibatida real vaqt rejimidagi kuzatuv tizimlarida uzilishlar yuzaga keladi [5].

Natijalar PSNR va SSIM ko‘rsatkichlari yordamida obyektiv tarzda baholandi. Yorug‘lik darajasi pasayganda PSNR 38.5 dB dan 18.9 dB gacha tushib ketishi kuzatildi, shovqin darajasi ortishi bilan SSIM 0.96 dan 0.64 gacha kamaydi. Siqish algoritmlarida esa H.264 MPEG-2 ga qaraganda yuqoriroq sifat natijalarini berdi.

Shuningdek, tadqiqotlardan aniqlandiki, klassik filtrlash usullari (Gaussian, Median) ma’lum hollarda samarali bo‘lsa-da, chuqur o‘rganishga asoslangan usullar (DnCNN, SRGAN) tasvir sifatini sezilarli darajada yaxshilaydi. GAN asosidagi super-resolution texnologiyalari siqilgan va past sifatli videotasvirlarni qayta tiklashda istiqbolli yechim sifatida ko‘rildi.

Foydalanilgan adabiyotlar:

1. Gonzalez R. C., Woods R. E. Digital Image Processing. 4th Edition. Pearson, 2018. – 1168 p.

2. Szeliski R. Computer Vision: Algorithms and Applications. 2nd Edition. Springer, 2022. – 915 p.

3. Bovik A. C. Handbook of Image and Video Processing. Academic Press, 2021. – 1384 p.

4. ITU-T Rec. P.910. Subjective video quality assessment methods for multimedia applications. International Telecommunication Union, 2019.

5. ISO/IEC 23009-1. Dynamic adaptive streaming over HTTP (MPEG-DASH), Part 1: Media presentation description and segment formats. International Standard, 2020.

6. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016. – 775 p.

XITOY, HINDISTON, ROSSIYA VA NATO TAJRIBASI ASOSIDA HARBIY SOHADA RAQAMLI TEXNOLOGIYALARNI QO‘LLASH MUAMMOLARI

Kamalov M.E.
Ichki ishlar vazirligi Akademiyasi raqamli texnologiyalar va axborot xavfsizligi kafedrasi katta o‘qituvchisi.

XXI asr harbiy sohada raqamli texnologiyalarning keng qo‘llanilishi bilan tavsiflanmoqda. Sun’iy intellekt (SI), kiberxavfsizlik tizimlari va uchuvchisiz uchish apparatlari (dronlar) qurolli kuchlarning qiyofasini tubdan o‘zgartirmoqda. Biroq mazkur jarayon nafaqat yangi imkoniyatlar, balki strategik, texnologik va huquqiy muammolarni ham keltirib chiqarmoqda. Shu bois ushbu maqolada Xitoy, Hindiston, Rossiya va NATO bloki tajribasi misolida zamonaviy raqamli texnologiyalarni harbiy sohada qo‘llashdagi asosiy muammolar tahlil qilingan.

Zamonaviy harbiy texnologiyalar haqida turli tadqiqotlar mavjud. RAND Corporation, SIPRI va NATO Review kabi manbalar raqamli texnologiyalarning harbiy strategiyaga ta’sirini yoritadi. Chatham Xaus (Chatham House) va Carnegie Endowment tahlillarida sun’iy intellektning global xavfsizlikka ta’siriga alohida urg‘u beriladi. Hindiston va Xitoy tajribasiga oid maqolalarda esa milliy mudofaa sanoati imkoniyatlari va texnologik qaramlik muammolari ko‘rsatilgan. Umuman olganda, mavjud

adabiyotlar raqamli harbiy transformatsiyada texnik rivojlanish bilan birga axloqiy va huquqiy muammolarni ham ta'kidlaydi.

Zamonaviy raqamli texnologiyalar (sun'iy intellekt, kiberxavfsizlik vositalari, dronlar va boshqalar) harbiy sohada inqilobiy o'zgarishlar yasamoqda. Ayni paytda Xitoy, Hindiston, Rossiya kabi davlatlar va NATO kabi harbiy ittifoqlar bu texnologiyalarni o'z qurolli kuchlariga joriy etish jarayonida qator muammolarga duch kelmoqda. Ushbu muammolar texnologik, strategik, huquqiy va axloqiy jihatlarni qamrab oladi. Quyida har bir mamlakat/ittifoq misolida shu yo'nalishlardagi asosiy muammolar qisqacha bayon etiladi.

Xitoy

- **Texnologik muammolar**: Xitoy armiyasida sun'iy intellektni joriy etishdan kutiladigan samara va ta'sir ko'lamini oldindan aniq baholash qiyin – AI taraqqiyoti sur'ati va yo'nalishiga oid noaniqlik mavjud[1]. Shuning uchun bu texnologiyani Xalq Ozodlik armiyasi (XOA) tuzilmasi va harbiy doktrinasiga to'g'ri integratsiya qilish zarur bo'lib, aks holda kutilayotgan afzallikka erishish qiyin bo'ladi[1].
- **Strategik muammolar**: Xitoyning sun'iy intellekt sohasidagi tez ilgarilashi mintaqada qurollanish poygasi xavfini oshirmoqda – sun'iy intellektda yetakchilikka bo'lgan raqobat yaqin kelajakda AI bo'yicha yangi qurollanish poygasini keltirib chiqarishi mumkin[2]. Bunda avtonom qurollarni nazorat qilishga doir xalqaro kelishuvlar hali ishlab chiqilmagani uchun, mazkur texnologiyalar holati strategik barqarorlikka noaniq (ba'zilarga ko'ra tazyiqni oshiruvchi, boshqalarga ko'ra tiyib turuvchi) ta'sir ko'rsatishi mumkin[2].
- **Huquqiy muammolar**: Avtonom qurollarni cheklash bo'yicha xalqaro huquqiy bazaning yetarli emasligi Xitoy uchun ham dolzarb masaladir. Masalan, 2018 yili Xitoy BMT doirasida o'limga olib keluvchi avtonom qurollar (LAWS)ni faqat qo'llashni taqiqlash yuzasidan taklif bilan chiqqan, ammo ularni yaratish va rivojlantirishni cheklashga kelishmagan – bu esa Xitoyning bunday qurollarni tahlil qilish va nazorat qilish borasida ehtiyotkor pozitsiyada ekanini ko'rsatadi[3].

- **Axloqiy muammolar**: Xitoy harbiy tahlilchilari sun'iy intellektdan foydalanishda yuzaga keladigan umumiy axloqiy masalalarni (masalan, avtonom qurol qo'llanganda kim javobgar bo'lishi) muhokama qilmoqdalar. Biroq XOAning o'zi to'g'ridan-to'g'ri Xitoy Kommunistik partiyasi (XKP) nazoratida bo'lgani bois, asosiy chaqiriq – avtonom AI tizimlaridan maksimal foyda olish barobarida XKPning armiya ustidan mutlaq nazoratini saqlab qolishdir[4]. Ya'ni, Xitoy uchun sun'iy intellektni harbiylarda qo'llash etikasi siyosiy bo'ysunuv tamoyili bilan chambarchas bog'liq va texnologiyaning ma'lum darajada "ishonchli" avtonom bo'lishiga doir shubhalar saqlanmoqda[4].

Hindiston

- **Texnologik muammolar**: Hindiston o'z qurolli kuchlarida AI va uchuvchisiz texnologiyalarni joriy etishda bir qator to'siqlarga duch kelmoqda. Avvalo, ilg'or harbiy texnologiyalarda hali ham xorijga yuqori darajada bog'liqlik saqlanayotgani mamlakatning sun'iy intellekt bo'yicha milliy imkoniyatlarini cheklamoqda – ichki ishlanmalar sust, xususiy sektor va harbiy tadqiqot muassasalari o'rtasida samarali hamkorlik to'liq yo'lga qo'yilmagan[5]. Bu esa mahalliy AI mahsulotlari va dronlar yaratish ekotizimini shakllantirishni sekinlashtiradi[5].
- **Strategik muammolar**: Hindiston uchun yana bir chaqiriq – qo'shni raqiblar (Xitoy va Pokiston)ning raqamli harbiy texnologiyalarda ilgarilashayotgani fonida texnologik ortda qolib ketmaslikdir. Masalan, Xitoyning harbiy AI va dronlar borasidagi yuksak yutuqlari va hatto Pokistonning Xitoy yordamida yangi qurollar sotib olishi Hindistonda tashvish uyg'otmoqda[6]. Shu bois Hindiston o'z mudofaa sohasida doimiy innovatsiya qilmas ekan, mintaqada raqobatda yutish qiyin; texnologik ustunlikni saqlash uchun ichki salohiyatni oshirish bilan birga xalqaro hamkorlikka ham tayanmoqda[6].
- **Huquqiy muammolar**: Sun'iy intellekt qo'llaniluvchi qurollardan foydalanishda huquqiy me'yorlarga amal qilish Hindiston armiyasi uchun muhim masala bo'lib turibdi. AI texnologiyalarini jang maydoniga joriy etish chog'ida ularni xalqaro gumanitar huquq qoidalariga mos tarzda qo'llash zarurati tug'iladi; ayniqsa, sun'iy intellekt negizida

harbiy kuch ishlatish qarorlarini qabul qilishda mas'uliyatni huquqiy jihatdan kim o'z zimmasiga olishi masalasi hal etilishi lozim[7]. Hozircha Hindiston bunday holatlarda xalqaro huquq normalariga amal qilishga intilmoqda, AI qurollarini qo'llash bo'yicha aniq milliy qonunchilik esa endilikda shakllanish bosqichida.

- **Axloqiy muammolar**: Hindiston sun'iy intellektli qurollarni ishlatishdagi axloqiy xatarlarni ham inobatga oladi. Masalan, odam aralashuvisiz avtomat rejimda o'limga doir qarorlarni qabul qilish ehtimoli va AI texnologiyalarining terrorchi guruhlar qo'liga tushishi xavfi jamoatchilikda ethical tashvish uyg'otmoqda[8]. Shu sabab, Hindiston hukumat rasmiylari mudofaa va milliy xavfsizlikda AIni "etik me'yorlarga mos holda" qo'llash lozimligini ta'kidlamoqda – ya'ni, har qanday AI-qurol qo'llash qarorida inson nazorati va axloqiy mas'uliyat saqlanishi shartligi urg'ulanmoqda[8].

Rossiya

- **Texnologik muammolar**: Rossiyaning raqamli harbiy texnologiyalar bo'yicha oldinga siljishida tashqi sanksiyalar va resurslar yetishmovchiligi jiddiy to'siqlar yaratmoqda. Jumladan, G'arb sanksiyalari tufayli Rossiya ilg'or mikrochiplar va elektron qismlarga kira olmayapti, shuningdek, yuqori malakali IT mutaxassislarining mamlakatni tark etishi ham kuzatilmoqda – bu omillar Rossiyaning sun'iy intellekt sohasida uzoq muddatda raqobatbardosh bo'lishiga xalal bermoqda[9]. Texnologiyaga doir bunday cheklovlar natijasida Rossiya o'z armiyasida AI va dronlarni keng ko'lamda joriy etishda qiyinchilikka duch kelmoqda, ayniqsa, tashqi komponentlarga qaramlik sharoitida.
- **Strategik muammolar**: Rossiya sun'iy intellektni global harbiy muvozanatda "hisobni tenglashtiruvchi" strategiya elementi sifatida ko'radi – Prezident V. Putinning 2017 yilda "AIda yetakchilik qilgan davlat butun dunyoga hukmron bo'ladi" degan gapi buning tasdig'idir[10][11]. Shu sabab, Moskva AI va avtonom qurollarga katta resurs ajratmoqda va bu boradagi har qanday xalqaro cheklovlarga rozi emas. Hatto boshqa davlatlar avtonom qurollarni taqiqlash yuzasidan takliflar bildirganda ham, Rossiya ularni qo'llab-quvvatlamaydi – bu orqali

u raqiblar (masalan, AQSh) bilan harbiy paritetga erishishni strategik maqsad qilganini anglatadi[12].

- **Huquqiy muammolar**: Rossiyaning sun'iy intellektli qurollarga doir huquqiy pozitsiyasi xalqaro hamjamiyatnikidan farq qiladi. Moskva fikricha, mavjud xalqaro gumanitar huquq qoidalari (jang olib borish qoidalari) AI asosidagi qurollarni tartibga solish uchun yetarli, shu bois yangi xalqaro shartnomalarga ehtiyoj yo‘q deb hisoblaydi[12]. Masalan, BMT doirasida ba'zi davlatlar tomonidan avtonom qurollarni to‘liq ta'qiqlash taklif etilganida, Rossiya va ayrim boshqa yirik davlatlar bunga qo‘shilmadi – natijada hozircha LAWS bo‘yicha global ta'qiq mavjud emas[12]. Milliy darajada esa Rossiyada bunday qurollarni ishlab chiqish va qo‘llashga qarshi qat'iy huquqiy cheklov ko‘zda tutilmagan.
- **Axloqiy muammolar**: Axloqiy nuqtai nazardan, Rossiya harbiy doirasi sun'iy intellektni jangovor maqsadlarda qo‘llashda inson omili va ochiqlik masalalariga kamroq e'tibor qaratadi, deyish mumkin. Ya'ni, Rossiya AI tizimlarining shaffofligi yoki ularni axloqiy jihatdan nazorat qilishidan ko‘ra ularning real sharoitdagi samaradorligiga ko‘proq ustuvorlik beradi[13]. Masalan, avtonom dronlar va robotlarga ma'lum darajada mustaqillik berish orqali jangovar vazifalarni bajartirish tendensiyasi kuchaymoqda – bunda mashina xatosi yoki noxato qurbonlar uchun javobgarlik muammolari etika jihatidan jiddiy bahslarga sabab bo‘lsa-da, Rossiya rahbariyati bunday texnologiyalarni cheklashdan ko‘ra ularni amalda sinab ko‘rishga moyilroqdir[13].

NATO

- **Texnologik muammolar**: NATO ittifoqi doirasida raqamli harbiy texnologiyalarni joriy etishda asosiy muammolardan biri – ittifoqchilar o‘rtasidagi turli imkoniyat va standartlar sababli texnologik uyg‘unlikka erishishdir. Masalan, NATOning o‘z qo‘lidagi razvedka dronlari soni yuqori intensivlikdagi mojaro uchun kamlik qiladi va mavjud dronlarni dushmanning radioelektron kurashi sharoitida birgalikda samarali qo‘llash qiyin bo‘ladi[14]. Turli davlatlarning turfa uchuvchisiz uchish apparatlari o‘rtasida to‘liq o‘zaro muvofiqlik yo‘qligi, yagona texnik standartlarning yetishmasligi ham butun Alyans miqyosida dron va

AI imkoniyatlarini birlashtirib ishlatishni qiyinlashtirmoqda[15]. Shu bois, NATO yangi texnologiyalarni joriy etishda har bir a'zo mamlakatning sohadagi salohiyatini muvofiqlashtirish va integratsiyalashtirish ustida ish olib bormoqda.

- **Strategik muammolar**: NATO uchun raqamli harbiy texnologiyalar sohasidagi global raqobatda ortda qolmaslik strategik ahamiyatga ega. Rossiyaning Ukrainaga qarshi urushi dronlar va sun'iy intellekt jang xarakterini qay darajada o'zgartirib yuborishi mumkinligini namoyon etdi – yangi texnologiyalar tez sur'atda tarqalmoqda va endi faqat NATO davlatlarigina bunday uskunalarga ega emas[16]. Dron va AI texnologiyalarining boshqa davlatlarga tarqalishi G'arbning ushbu sohadagi an'anaviy ustunligini zaiflashtirayotgani qayd etilmoqda[16]. Demak, NATO raqiblari (masalan, Rossiya yoki Xitoy)ning AI, kiberqurol va dronlarni rivojlantirishini inobatga olgan holda, texnologik afzalligini saqlash uchun yalpi strategiya ishlab chiqishi talab etiladi. Bunda ittifoqchilik doirasida ma'lumot almashish, hamkorlikda ilmiy tadqiqotlar o'tkazish va birgalikda harbiy tadbirlar orqali yangi texnologiyalarni sinovdan o'tkazib borishga urg'u beriladi.
- **Huquqiy muammolar**: NATO va uning a'zo davlatlari uchun sun'iy intellekt qo'llanilgan qurollarni qonuniy tarzda qo'llash masalasi muhimdir. Barcha holatda xalqaro gumanitar huquq qoidalariga amal qilish talab etiladi, biroq AI yordamida qaror qabul qiluvchi tizimlarda bu qoidalarga rioya qilishni ta'minlash oson emas[17]. Masalan, avtonom qurol-aslahalar odam aralashuvisiz nishon tanlaganda yoxud kiberxujumlarni AI avtonom ravishda amalga oshirganda, tinch aholiga ziyon yetkazmaslik va buzg'unchilikni cheklash kabi yuridik me'yorlarning buzilishi xavfi ortadi[17]. Shuning uchun NATO doirasida "mahsulot yaratish siklining ilk bosqichlaridanoq AI tizimlarining yuridik va etik talablarga muvofiq bo'lishini" ta'minlashga chaqiriqlar bo'lmoqda – ya'ni, har bir a'zo mamlakatning AI etikasi va qonuniylik mezonlarini muvofiqlashtirib, umumiy prinsiplar qabul qilish zarurligi ta'kidlanmoqda.
- **Axloqiy muammolar**: NATO mamlakatlarida AI va robotlashgan qurollarni qo'llash atrofida axloqiy masalalar ham

koʻndalang boʻlib turibdi. Eng avvalo, avtonom qurollarga odam hayoti va oʻlimiga doir qarorlarni topshirishning maʼnaviy oqibatlari savollar tugʻdirmoqda[18]. Masalan, "qotil robot" deb ataluvchi halokatli avtonom qurollar inson qarashisiz ish yuritganda, janglarda masʼuliyat kimga yuklanishi va bunday avtomatlashtirish inson qadr-qimmatiga qanchalik muvofiq kelishini NATO doirasidagi ekspertlar qizgʻin muhokama qilishmoqda[18]. Shu bilan birga, AI algoritmlari xato yoki qarama-qarshi maʼlumot asosida notoʻgʻri qaroriy harakat qilishi va natijada begunoh odamlar jabr chekishi ehtimoli harbiy etika uchun yangi muammolar sifatida koʻriladi[18]. Naturali, NATO rahbariyati sunʼiy intellektdan foydalanishda "inson omillari ustuvorligi" va xalqaro qonun-qoidalarga amal qilinishi shartligini taʼkidlar ekan, bu talablarni amaliy taʼminlash boʻyicha aniq mexanizmlarni ishlab chiqish dolzarbligicha qolmoqda.

Manba:

Yuqoridagi maʼlumotlar ishonchli tahliliy manbalarga asoslangan boʻlib, har bir bayon etilgan fikr oʻz manbasi bilan tasdiqlangan (manba raqamlari matnda koʻrsatilgan). Masalan, Xitoyda AIni harbiylarga joriy etish borasidagi tahlil GWU Xalqaro ishlar sharhidan olingan boʻlsa, Hindistonning ushbu sohadagi saʼy-harakatlari IMPRI tahlil markazi hisobotida yoritilgan. Shuningdek, Rossiya va NATO haqidagi maʼlumotlar Mindfoundry, CEPA va NATOning rasmiy nashrlariga asoslanadi. Har bir manbaning aniq maʼlumoti matn ichida 【manba raqami†satrlar】 koʻrinishida berilgan.

Xulosa va tavsiyalar

Tahlil shuni koʻrsatadiki, raqamli texnologiyalarni harbiy sohada qoʻllash imkoniyatlar bilan birga jiddiy muammolarni ham keltirmoqda. Xitoy global yetakchilikka intilayotgan boʻlsa, Hindiston texnologik mustaqillikni taʼminlashi kerak. Rossiya sanksiyalar sharoitida raqobatbardoshlikka intilayotgan boʻlsa, NATO interoperabellik va huquqiy meʼyorlar muammosini hal qilishi lozim. Shu bois, global darajada AI va dronlarning huquqiy va axloqiy cheklovlarini uygʻunlashtirish zarur.

Xitoy, Hindiston, Rossiya va NATO misolida ko‘rinib turibdiki, raqamli texnologiyalarni harbiy sohada qo‘llash nafaqat imkoniyat, balki katta muammolar ham keltirib chiqarmoqda.

- Xitoy — global yetakchilik uchun harakat qilmoqda.
- Hindiston — texnologik mustaqillikka intilmoqda.
- Rossiya — sanksiyalar ostida strategik paritet qidirmoqda.
- NATO — uyg‘unlik va qonuniylikni ta’minlashga urinayotgan ittifoq.

Demak, XXI asrning asosiy vazifasi — raqamli harbiy texnologiyalarning samarasini oshirish bilan birga ularning huquqiy va axloqiy cheklovlarini global darajada uyg‘unlashtirishdir.

Foydalanilgan adabiyotlar:

1. [1] [2] [3] China’s Military Employment of Artificial Intelligence and Its Security Implications // *The International Affairs Review*. – URL: https://www.iar-gwu.org/print-archive/blog-post-title-four-xgtap (дата обращения: 25.09.2025).
2. [4] The PRC considers military AI ethics: Can autonomy be trusted? // *PubMed*. – URL: https://pubmed.ncbi.nlm.nih.gov/36387011/ (дата обращения: 25.09.2025).
3. [5] [6] [7] [8] India’s Developing AI in National Security and Defence // *IMPRI Impact and Policy Research Institute*. – URL: https://www.impriindia.com/insights/india-ai-security-defence/ (дата обращения: 25.09.2025).
4. [9] [10] [11] [12] [13] Defence and National Security AI Strategies The Global Landscape // *Mind Foundry*. – URL: https://www.mindfoundry.ai/blog/international-ai-strategies-for-defence-and-national-security (дата обращения: 25.09.2025).
5. [14] [15] [16] An Urgent Matter of Drones: Lessons for NATO from Ukraine // *CEPA*. – URL: https://cepa.org/comprehensive-reports/an-urgent-matter-of-drones/ (дата обращения: 25.09.2025).
6. [17] [18] Navigating the AI battlefield: Opportunities and ethical frontiers // *NRDC Italy*. – URL: https://nrdc-ita.nato.int/newsroom/insights/navigating-the-ai-battlefield-opportunities-

-challenges--and-ethical-frontiers-in-modern-warfare (дата обращения: 25.09.2025).

7. Allen G., Chan T. Artificial Intelligence and National Security. – Harvard: Belfer Center, 2017. – 112 p.

8. Boulanin V., Verbruggen M. Mapping the Development of Autonomy in Weapon Systems. – Stockholm: SIPRI, 2017. – 88 p.

YO‘L HARAKATI XAVFSIZLIGI XIZMATI FAOLIYATIDA UCHUVCHISIZ UCHISH APPARATLARIDAN FOYDALANISH IMKONIYATLARI

Xamidov G‘.S.

O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti, t.f.n., professor

XXI asrdagi jadal ilmiy-texnikaviy taraqqiyot natijalari, birinchi navbatda, samolyotlar va aeronavtika qurilmalarini takomillashtirish hamda ularni boshqa maxsus texnik vositalar bilan jihozlash imkoniyatlari hisobiga uchuvchi qurilmalardan samarali foydalanish sohalarini kengaytirish imkonini berdi. Turli xil texnik vositalarning noyob imkoniyatlarining kompleks kombinatsiyasi murakkab muammolarni hal qilish imkonini berdi. Samolyotlar yoki aviatsiya qurilmalari komponovkasi asosidagi birlashtirilgan texnik vositalardan (tizimlardan) foydalanish ijtimoiy-iqtisodiy sohalarda, ilmiy-tadqiqot faoliyatida va mamlakatimiz xavfsizligini ta’minlash faoliyatida talabga ega bo‘lgan bir qator yangi aviatsiya imkoniyatlarini olish imkonini berdi [1; b. 7].

Yo‘l tarmog‘ida yo‘l harakati xavfsizligini samarali ta’minlashning asosi, kelajakda Davlat yo‘l harakati xavfsizligining yo‘l-patrul guruhlari va brigadalarining faoliyati, yo‘lda harakatlanishni nazorat qilish, uning ishtirokchilari tomonidan sodir etilgan huquqbuzarliklarni aniqlash va hisobga olish uchun texnik vositalardan foydalangan holda xizmatga yuklangan vazifalarni mukammal bajarish imkoniyatini yaratadi. Hozirgi vaqtda nazoratni amalga oshirish, xususan, inspektorlar tomonidan yo‘l harakati qoidalarini buzish holatlarini aniqlash uchun turli texnik vositalardan foydalanilmoqda, faoliyatni yanada samaradorligini oshirish innovatsion yondashuvlarni talab etadi jumladan, uchuvchisiz uchish

apparatlari (UUA)larni qo‘llashni [2; b. 46]. Ushbu imkoniyatlardan yo‘l harakatini tashkil etish, boshqarish va sodir etilgan yo‘l transport hodisalarini tadqiq qilishda foydalanish avzalliklarini, hozirgi kunda amalda qo‘llayotgan Rossiya Ichki ishlar vazirligining Adigey Respublikasi bo‘yicha davlat yo‘l harakati xavfsizligi inspeksiyasi misolida ko‘rib chiqish mumkin.

Ushbu bo‘linma tashabbusi bilan Rossiya Federatsiyasi hukumatining 2017-yil 27-dekabrdagi 1669-sonli qaroriga muvofiq Rossiya Milliy gvardiyasining Adigeya Respublikasi bo‘yicha direksiyasining **(keyingi o‘rinlarda MMAO AOSN deb yuritiladi)** maxsus maqsadli aviatsiya otryadi bilan o‘zaro hamkorlik tashkil yetildi.

Maxsus operatsiyalar agentligining kuchlari va vositalarining samolyotlari federal va mintaqaviy yo‘llarning avtohalokatga moyil bo‘lgan qismlarida yo‘l harakati xavfsizligini ta’minlash uchun, qarama-qarshi harakatlanish uchun mo‘ljallangan bo‘lakka chiqish natijasida yuqori baxtsiz hodisalardan foydalaniladi.

2018-yilda uchuvchisiz uchish apparatlaridan foydalanish natijasida qarama-qarshi harakatlanish uchun mo‘ljallangan bo‘lakka chiqib ketish bilan bog‘liq 136 ta ma’muriy yo‘l harakati qoidabuzarliklari aniqlangan (jami parvoz vaqti 132 soat bo‘lgan 75 ta reys bajarilgan).

2019-yilning 12 oyi davomida 83 ta shu kabi ma’muriy huquqbuzarliklar aniqlangan (88 ta reys amalga oshirilgan, jami 119 soat parvoz). Davlat Yo‘l harakati xavfsizligi inspeksiyasi (DYHXI) (STSI) bo‘limlari MMAO bilan quyidagicha o‘zaro hamkorlik qiladi:

1. Har bir uchishni bajarish uchun Adygeya Respublikasi Ichki ishlar vaziri tomonidan imzolangan ariza shakli Adygeya Respublikasi bo‘yicha Rosgvardiya boshqarmasi boshlig‘i nomiga, aviatsiya qo‘llaniladigan sana, maydon va yo‘l uchastkasi ko‘rsatilgan ilova bilan tayyorlanadi.

2. Ariza belgilangan tartibda tasdiqlanganidan so‘ng Adygeya Respublikasi Ichki ishlar vazirligi va Rossiya Milliy gvardiyasining Adigey Respublikasi bo‘yicha boshqarmasi o‘rtasida hamkorlik qilish to‘g‘risida qo‘shma buyruq chiqariladi.

3. Maxsus rang sxemasiga ega bo‘lmagan Ford Tranzit xizmat avtomashinasi bazasida jihozlangan ko‘chma uchuvchisiz havo vositalarini boshqarish markazi hamda yo‘l harakati politsiyasining identifikatsiya belgilari bilan yo‘l harakati xavfsizligini ta’minlovchi avtomashina yo‘l harakati qatnashchilari uchun maqbul ko‘rinishga ega bo‘lgan joylarga joylashtiriladi.

Yo‘l harakati monitoringi uchun MMAO xodimlari Rossiya Federatsiyasi Milliy gvardiyasi qo‘shinlari Federal xizmati bilan xizmat ko‘rsatadigan sertifikatlangan tizimlardan foydalanadilar:

– yuqori balandlikdagi videokuzatuv aerostati (“OKO-1” bog‘langan aerostat);

- uchuvchisiz "ZALA 421-16YE".

Yuqorida tilga olingan videokuzatuv tizimlarining texnik imkoniyatlari har ikki yo‘nalishda ham uzunligi 5 kilometrgacha bo‘lgan yo‘l uchastkalarini kuzatish imkonini beradi. ZALA 421-16YE UUA bitta batareyalar to‘plamida 3 soatdan ortiq uzluksiz ishlashi mumkin (to‘plamga almashtiriladigan batareyalar kiradi).

Agar transport vositasi yo‘l belgilarini buzgan holda qarama-qarshi harakat chizig‘iga kirayotgani aniqlansa, operator (MMAO xodimi) nishonni “avtomatik ravishda blokirovka qilish” buyrug‘ini beradi. UUAning dasturiy ta’minoti yo‘l harakati politsiyasi xodimi tomonidan to‘xtatilgunga qadar nishonni avtomatik kuzatish imkonini beradi. Bunday holda, qoidabuzarlik va transport vositasining to‘xtagunga qadar harakatining videoyozuvi UUA operatorining avtomatlashtirilgan ish stansiyasining qattiq diskida saqlanadi. Avtotransport vositasi to‘xtatilgandan so‘ng haydovchiga huquqbuzarlik to‘g‘risidagi videoyozuv ko‘rsatiladi va u ma’muriy huquqbuzarlik to‘g‘risidagi bayonnomaga dalil sifatida kiritish uchun optik diskka ko‘chiriladi.

Ma’muriy huquqbuzarlik to‘g‘risidagi yuqorida qayd etilgan materiallar sud tomonidan ko‘rib chiqilayotganda yo‘l harakati qoidalarini buzgan shaxslarni ma’muriy javobgarlikka tortish to‘g‘risida qarorlar qabul qilinadi.

UUAlardan foydalangan holda qayd etilgan ma'muriy huquqbuzarliklar to‘g‘risidagi ishlar bo‘yicha sudlar tomonidan ish yuritishni yetarlicha yoki asossiz bo‘lganligi sababli tugatish holatlari kuzatilmagan.

OKO-1 balandlikdagi videokuzatuv tizimidan foydalanish sezilarli profilaktika ta'siriga ega va haydovchilarni intizomli qiladi.

Ta'kidlash joizki, bog‘langan shardan foydalanish davrida yo‘l uchastkalarida hech qanday yo‘l-transport hodisalari qayd etilmagan.

Shu bilan birga, katta manevrga ega bo‘lgan ZALA 424-16YE UUAdan foydalanish avtomobil yo‘llarining uzunroq va murakkabroq uchastkalarida yo‘l harakati xavfsizligini nazorat qilish imkonini beradi.

Bundan tashqari, yo‘l harakati xavfsizligini axborot va tashviqot qo‘llab-quvvatlash maqsadida Adygeya Respublikasining yo‘llarida UUAlardan foydalanish to‘g‘risidagi ma'lumotlar Respublika Ichki ishlar vazirligi va Davlat yo‘l harakati inspeksiyasi veb-saytlarida, ommaviy axborot vositalarida (televideniye, radio, bosma ommaviy axborot vositalari), Internetda, shu jumladan ijtimoiy tarmoqlarda va turli xil messenjerlarda yoritilgan.

Shunday qilib, UAVlardan foydalanish bir qator afzalliklarga ega:

- teplovizirli kuzatuv kameralarini o‘rnatish imkoniyati tufayli yo‘l harakati qoidalarini buzuvchilarni tezkor aniqlash va ta'qib qilish;
- hatto tungi vaqtda ham yo‘l harakati qoidalarini buzgan transport vositasining davlat raqami va markasini aniqlash mumkin;
- voqea sodir bo‘lgan ishtirokchilarni hibsga olish vaqtida qochib ketgan taqdirda tezkor qidiruv va ta'qib qilish;
- belgilangan joylarda yaqinda o‘g‘irlangan transport vositalarini kuzatish va aniqlash;
- ma'muriy binolar va davlat idoralari yaqinida qonunga xilof ravishda qo‘yilgan transport vositalarini tekshirish va aniqlash;
- elektr motorlar yuqori operatsion xarajatlarni talab qilmaydi;
- ular faqat vaqti-vaqti bilan quvvat manbalaridan zaryadlanishi kerak.

UUA imkoniyatlarini, xususan kuch va vositalardan foydalanish samaradorligi oshishini, tezkorlik va tadbir vaqtining birmuncha qisqarishi kabi afzalliklarni e'tiborga olgan holda O'zbekiston Respublikasi IIV Jamoat xavfsizligi Departamenti YHXXida UUAlaridan foydalanish maqsadga muvofiq deb hisoblayman. Shuningdek zamonaviy aviatsiya UUA maxsus texnik tizimlar bilan jihozlashga innovatsion yondashuvlar orqali jamoat tartibini saqlash va jamoat xavfsizligini ta'minlashda ichki ishlar organlari faoliyati samaradorligini sezilarli darajada oshirishi mumkin. Yirik shaharlarda eng murakkab vaziyatlarda yo'llarda xavfsiz harakatlarni tashkil etishda, UUAlarining yuqori harakatchanligi, tezkorligi va hodisa zonalariga yetib borish qobiliyatlari ularni YHXX faoliyatida vazifalarini hal qilishda chinakam ishonchli va ajralmas yordamga aylantiradi.

Foydalanilgan adabiyotlar:

1. Бетсков А.В. Применение аэромобилних ком плексов МВД России при противодействии преступности : учеб. пособие. М. : Академия управления МВД России, 2017. С. 7.

2. Туманов Е.А. Возможности применения беспилотних летателних аппаратов на службе госавтоинспексии / Е.А. Туманов, С.В. Назаров, Д.А. Тарасенков, В.Д. Головкин // Дневник науки. 2019. № 12. С. 46.

IOT-TEXNOLOGIYALARNI QUROLLI KUCHLARDA QO'LLASH: IMKONIYATLAR VA TAHDIDLAR

Baxtiyorova S.U.
O'zbekiston Respublikasi Jamoat xavfsizligi universiteti,
373-o'quv guruhi kursanti
Xatamov B.B.
O'zbekiston Respublikasi Jamoat xavfsizligi universiteti, kafedra
boshlig'ining o'rinbosari, t.f.f.d. (PhD)

Zamonaviy raqamli texnologiyalar taraqqiyoti mudofaa va xavfsizlik sohasiga sezilarli ta'sir ko'rsatmoqda. XXI asrda raqamli texnologiyalarning rivojlanishi harbiy boshqaruvni tashkil etishda yangi

yondashuvlarning paydo bo‘lishiga olib keldi. Eng istiqbolli konsepsiyalardan biri bu – Internet narsalar (Internet of Things – IoT) bo‘lib, u turli xil datchiklar, qurilmalar va tizimlarni yagona tarmoqqa birlashtirishni, shuningdek, ular orasida inson ishtirokisiz ma’lumot almashish imkoniyatini nazarda tutadi. IoTning muhim yo‘nalishlaridan biri harbiy texnika, aloqa vositalari, datchiklar, uchuvchisiz apparatlar va hisoblash tizimlarini yagona tarmoqqa birlashtirishdir. Shu asosda qo‘shinlarni boshqarishning intellektual tizimlari (QBIT) shakllanadi, ular qaror qabul qilish tezligini, vaziyatni baholash aniqligini va jangovar vazifalarni bajarish samaradorligini oshiradi. Harbiy sohada IoT qo‘shinlarni boshqarish samaradorligini sezilarli darajada oshirishi, logistika, tibbiy ta’minot va harbiy texnikani nazorat qilishni yaxshilashi mumkin. Biroq, bu texnologiyalarning keng joriy etilishi kiberxavfsizlik, ishonchlilik va tizimlarning zaifliklari bilan bog‘liq bir qator jiddiy tahdidlar bilan hamrohlanadi.

IoTni Qurolli Kuchlarda qo‘llash imkoniyatlari haqida gapirganda, ularning turli xil jangovar vazifalarni bajarishda qo‘llanishining ayrim jihatlarini ta’kidlash lozim. Masalan, IoTdan foydalanish texnika, qurol-yarog‘, yoqilg‘i va oziq-ovqat harakatini real vaqt rejimida kuzatish imkonini beradi. Bu esa logistika zanjirlarining shaffofligini ta’minlaydi va qo‘shinlarni ta’minlashdagi uzilishlar xavfini kamaytiradi [1].

Datchiklar va GPS-modullaridan foydalanish harbiy texnika, omborlar va ta’minotning joylashuvini real vaqt rejimida nazorat qilish imkonini beradi. Sensor tarmoqlari va RFID-yorliqlar qurol-aslaha, o‘q-dorilar, yoqilg‘i va oziq-ovqatni avtomatik hisobga olish imkoniyatini yaratadi. Bunday yondashuv inson omilini minimal darajaga tushiradi va hisobotdagi xatoliklarni istisno qiladi.

Transport vositalariga o‘rnatilgan datchiklar dvigatellar, yurish qismi va boshqa elementlarning holatini nazorat qila oladi. IoT tizimi olingan ma’lumotlarni tahlil qiladi va mumkin bo‘lgan nosozliklarni bashorat qiladi, bu esa rejasiz to‘xtash ehtimolini kamaytiradi. Harbiy texnikaga o‘rnatilgan raqamli datchiklar uning texnik holatini nazorat qilish, mumkin bo‘lgan nosozliklarni oldindan prognoz qilish va o‘z vaqtida texnik xizmat

ko‘rsatishni amalga oshirish imkonini beradi. Bunday yondashuv xarajatlarni kamaytiradi va jangovar shaylikni oshiradi [2].

IoT ma’lumotlarini qayta ishlash algoritmlari yo‘l sharoitlari, ob-havo omillari va dushman faolligini inobatga olib, eng xavfsiz va tezkor yetkazib berish yo‘nalishini taklif qilishi mumkin. IoT yoqilg‘i, elektr energiyasi va boshqa resurslar sarfini nazorat qilishga yordam beradi, bu esa moddiy vositalardan yanada oqilona foydalanish imkonini beradi.

Bundan tashqari, taqiladigan IoT qurilmalari (aqlli bilaguzuklar, sensorlar) askarlarning hayotiy ko‘rsatkichlarini – yurak urishi, harorat, kislorod darajasini kuzatishi mumkin. Ma’lumotlar tibbiy xizmatlarga uzatiladi, bu esa sog‘liqning yomonlashuviga tezkor javob qaytarish imkonini beradi [3].

IoT tarmoqlari razvedka ma’lumotlarini, uchuvchisiz apparatlar va yer usti datchiklaridan olingan ma’lumotlarni integratsiya qiladi, shu orqali QBITni shakllantiradi. Bu esa qo‘mondonlarning vaziyatdan xabardorligini oshiradi va asosliroq qarorlar qabul qilishga ko‘maklashadi [4].

Harbiy sohada IoTdan foydalanish an’anaviy qo‘mondonlik sxemalaridan tarmoq-markazli boshqaruv tizimlariga o‘tish uchun zamin yaratadi. Bu quyidagi imkoniyatlarda o‘z ifodasini topadi:

1. **Vaziyatdan xabardorlik.** IoT tarmog‘iga integratsiya qilingan datchiklar, kameralar, uchuvchisiz apparatlar va razvedka tizimlari jang maydonining yaxlit manzarasini real vaqt rejimida shakllantiradi. Qo‘mondonlar qo‘shinlarning joylashuvi, resurslar va dushman harakatlari haqida aniq ma’lumot oladilar.
2. **Boshqaruv jarayonlarini avtomatlashtirish.** IoT ma’lumotlari asosida sun’iy intellekt algoritmlari resurslarni avtomatik taqsimlashi, optimal manevr yoki yo‘nalish variantlarini taklif qilishi, shuningdek, turli qarorlarning oqibatlarini bashorat qilishi mumkin.
3. **Yagona axborot makoni.** Aloqa vositalari, sensor tizimlari va hisoblash markazlarining integratsiyasi barcha qo‘mondonlik darajalarida mavjud bo‘lgan umumiy raqamli muhitni yaratadi. Bu esa ma’lumotlarni uzatishda buzilishlar va kechikishlar xavfini kamaytiradi.

4. **Uchuvchisiz tizimlar bilan integratsiya.** IoT uchuvchisiz uchish apparatlari, yer usti va dengiz robotlashtirilgan platformalarini boshqarishni ta'minlaydi, ular razvedka, hujum va logistika vazifalarini bajarishi mumkin.

5. **Prediktiv analitika.** Katta hajmdagi ma'lumotlarni yig'ish va qayta ishlash jangovar vaziyat rivojlanishini modellashtirish, mudofaa tizimidagi zaif tomonlarni aniqlash va ularni bartaraf etish choralarini oldindan ko'rish imkonini beradi.

Intellektual qo'shinlarni boshqarish tizimlarining afzalliklariga quyidagilarni kiritish mumkin:

- «aniqlash – qaror – harakat» siklining vaqtini qisqartirish;
- obyektiv ma'lumotlar hisobiga jangovar qarorlarning aniqligini oshirish;
- tez o'zgarayotgan sharoitlarda ham boshqaruvning moslashuvchanligi;
- ma'lumotlarni avtomatlashtirilgan qayta ishlash tufayli qo'mondonlarga tushadigan yukni kamaytirish;
- turli qo'shin turlari o'rtasida o'zaro hamkorlik samaradorligini oshirish.

Shu tariqa, qo'shinlarni boshqarish sohasida IoTdan foydalanish tamomila yangi, intellektual va tarmoq-markazli qo'mondonlik tizimlarini barpo etish imkoniyatini ochadi. Bunday tizimlar vaziyatni uzluksiz monitoring qilishni, qaror qabul qilish tezligi va sifatini oshirishni, shuningdek, qurolli kuchlarning barcha elementlarini – askarlar va texnikadan tortib uchuvchisiz majmualar va qo'mondonlik punktlarigacha yagona tarmoqqa integratsiya qilishni ta'minlaydi.

Biroq ushbu imkoniyatlarni samarali amalga oshirish faqatgina himoyalangan aloqa kanallarini rivojlantirish, barqaror kiberhimoya hamda IoT texnologiyalarini jangovar harakatlar xususiyatlariga moslashtirish sharti bilan mumkin bo'ladi.

IoTning harbiy sohadagi asosiy muammosi uning kiberhujumlarga nisbatan zaifligidadir. Datchiklar yoki tarmoq tugunlari buzib kirilishi

maxfiy ma'lumotlarning sizib chiqishiga yoki butun tizimning ishdan chiqishiga olib kelishi mumkin [5].

Shundan kelib chiqib, Qurolli kuchlarda IoTning asosiy kiberxavf-xatarlariga quyidagilarni kiritish mumkin:

1. **Ruxsatsiz kirish.** Dushman IoT qurilmalarini, jumladan sensorlar, kameralar va uchuvchisiz apparatlarni nazoratga olishi mumkin, bu esa maxfiy ma'lumotlarning sizib chiqishiga yoki jangovar operatsiyaning buzilishiga olib keladi;

2. **«Xizmatdan voz kechish» hujumlari (DoS/DDoS).** IoT tarmoqlari sun'iy ravishda yaratilgan trafik bilan ortiqcha yuklanishi mumkin, bu esa real vaqt rejimida muhim axborotni uzatishni imkonsiz qiladi;

3. **Ma'lumotlar bilan manipulyatsiya qilish.** Sensor ko'rsatkichlarini o'zgartirish yoki qo'shinlarning joylashuvi haqidagi ma'lumotni soxtalashtirish qo'mondonlik tomonidan noto'g'ri qarorlar qabul qilinishiga olib kelishi mumkin;

4. **Zararli dasturiy ta'minot.** IoT qurilmalari viruslar va «trojanlar»ni joylashtirish uchun nishonga aylanishi mumkin, ular harbiy infratuzilmani yashirincha nazorat qilish imkonini beradi;

5. **Aloqa protokollaridagi zaifliklardan foydalanish.** Ko'pchilik IoT qurilmalari ma'lumotlarni tutib qolish yoki soxtalashtirishga zaif bo'lgan simsiz protokollardan (masalan, Wi-Fi, Bluetooth, ZigBee) foydalanadi, bu esa qo'shimcha xatarlarni yuzaga keltiradi;

6. **Ta'minot zanjiri orqali hujumlar.** IoT qurilmalari mikrosxema yoki dasturiy ta'minot darajasida «yashirin qurilmalar» bilan ta'minot va ishlab chiqarish bosqichidayoq zararli tarzda kiritilishi mumkin.

Harbiy IoT tizimlarining zaifliklariga kelsak, bu yerda ko'plab IoT qurilmalari past hisoblash quvvatiga ega ekanligini ta'kidlash lozim. Cheklangan xavfsizlik resurslari murakkab shifrlash algoritmlaridan foydalanishni qiyinlashtiradi. Ishlab chiqaruvchilar va standartlarning ko'pligi, qurilmalar va protokollarning xilma-xilligi yagona kiberxavfsizlik tizimini ta'minlashda qiyinchilik tug'diradi. Ko'plab

qurilmalar yetib borish qiyin hududlarda ishlaydi, bu esa ularning texnik xizmat ko‘rsatish va yangilanish imkoniyatlarini cheklaydi. Sun’iy yo‘ldosh navigatsiyasi, bulutli servislar va ma’lumot uzatish kanallaridan foydalanish kiber tizimlarning zaifligini oshiradi.

Shunday qilib, IoT Qurolli kuchlar samaradorligini oshirish uchun keng istiqbollarni ochib beradi, intellektual boshqaruv, monitoring va o‘zaro hamkorlik tizimlarini yaratishni ta’minlaydi. Biroq yuqori darajadagi raqamlashtirish yangi tahdidlarni ham yuzaga keltiradi: IoT tarmoqlariga kiberhujumlar kelajakdagi urushlarda dushman uchun asosiy qurolga aylanishi mumkin.

Tashkiliy-texnik chora-tadbirlar orqali kiberxatarlarni kamaytirish.

1. Kriptografik himoyani kuchaytirish:

- ma’lumotlar va aloqa kanallari shifrlashning barqaror algoritmlaridan foydalanish;
- foydalanuvchilar va qurilmalar uchun ko‘p darajali autentifikatsiyani joriy etish;
- ma’lumotlarni “harakatda” va “xotirada” majburiy shifrlash.

2. Harbiy IoT standartlarini ishlab chiqish:

- apparat va dasturiy ta’minotga milliy talablarni shakllantirish;
- harbiy IoT qurilmalarini yagona sertifikatlash tizimini yaratish;
- kuchaytirilgan himoyasiz fuqarolik protokollaridan foydalanishni rad etish.

3. Ta’minot zanjirini nazorat qilish:

- uskunalarni yashirin qurilmalar va zaifliklarga tekshirish;
- mahalliy yoki ishonchli ishlab chiqaruvchilardan foydalanish;
- komponentlarni markalash va kuzatish texnologiyalarini joriy etish.

4. Doimiy yangilash va monitoring:

- mikrodastur (firmware) va dasturiy ta’minotni muntazam yangilash;
- IoT qurilmalarining tarmoq faoliyatini monitoring qilish vositalaridan foydalanish;

- hujumlarni aniqlash tizimlarini (IDS/IPS) joriy etish.

5. Sun'iy intellekt va mashinaviy o'qitish:

- IoT tizimlarida anomaliyalarni aniqlash uchun AI algoritmlarini qo'llash;
- kiberxatarlarni tahlil qilish va hujumlarni bashorat qilishni avtomatlashtirish;
- intellektual o'zini-o'zi himoya qilish tizimlarini ishlab chiqish.

6. Tashkiliy choralar:

- maxsus kiberqo'shin bo'linmalarini shakllantirish;
- shaxsiy tarkibni kiberxavfsizlik asoslariga o'qitish;
- kiberhodisalarga javob berish ssenariylarini ishlab chiqish.

IoT-tizimlari Qurolli Kuchlarda harbiy sohani raqamlashtirish uchun yangi ufqlarni ochmoqda, biroq uning qo'llanishi yuqori xatarlar bilan bog'liq. Ishonchli kiberhimoya harbiy IoT tizimlarining ajralmas elementi sifatida ko'rib chiqilishi lozim. Kiberxatarlarni kamaytirish faqat kompleks yondashuv orqali mumkin bo'lib, u texnologik (kriptografiya, standartlar, AI) va tashkiliy (kiberqo'shinlar, kadrlar tayyorlash, ta'minot nazorati) choralarni o'z ichiga oladi. Aks holda, IoT zamonaviy urush sharoitida ustunlik emas, balki zaiflikka aylanishi mumkin.

Xulosa. Qurolli kuchlarda IoTni joriy etish harbiy operatsiyalarning samaradorligi va tezkorligini oshirish uchun yangi ufqlarni ochadi. Biroq bu imkoniyatlarning muvaffaqiyatli amalga oshirilishi kompleks himoya tizimi, barqaror aloqa protokollari va radioelektron qarshi harakat sharoitida avtonom faoliyat yuritish usullarisiz mumkin emas.

Harbiy logistika sohasida Internet of Things qo'llanilishi qo'shinlarni ta'minlash samaradorligini oshirish uchun yangi istiqbollarni ochadi. "Aqlli logistika" tizimi nafaqat yuklar va texnikaning harakatini kuzatish, balki ehtiyojlarni prognoz qilish, marshrutlarni optimallashtirish va ta'minot operatsiyalarining xavfsizligini oshirish imkonini beradi.

IoT asosidagi QBIT qurolli kuchlarning raqamli transformatsiyasining muhim elementi bo'lib, ularning raqobatbardoshligini va yangi avlod urushlarini olib borishga tayyorligini ta'minlaydi.

Shu bilan birga, IoTni muvaffaqiyatli joriy etish kiberxavfsizlik, aloqa kanallarining barqarorligi va texnologiyalarning jangovar sharoitlarga moslashtirilishi masalalariga alohida e'tibor talab qiladi. Harbiy sohada IoTni rivojlantirish texnologik hamda tashkiliy choralarni o'z ichiga olgan kompleks kiberhimoya tizimini yaratish bilan birga olib borilishi lozim. Faqat shunda IoT texnologiyalari davlat mudofaa qobiliyatini ta'minlashda ishonchli vositaga aylanishi mumkin.

Shunday qilib, IoT mudofaa qobiliyatini kuchaytiruvchi qudratli vosita ham, kelajakdagi raqamli armiya uchun zaif bo'g'in ham bo'lishi mumkin.

Fodalanilgan adabiyotlar:

1. Greengard S. The Internet of Things. MIT Press, 2021.
2. Lee I., Lee K. "The Internet of Things (IoT): Applications, investments, and challenges for enterprises." Business Horizons, 2015.
3. Da Xu L., He W., Li S. "Internet of Things in Industries: A Survey." IEEE Transactions on Industrial Informatics, 2014.
4. Gubbi J., Buyya R., Marusic S., Palaniswami M. "Internet of Things (IoT): A vision, architectural elements, and future directions." Future Generation Computer Systems, 2013.
5. Roman R., Zhou J., Lopez J. "On the features and challenges of security and privacy in distributed internet of things." Computer Networks, 2013.

TOR HUDUDDA JOYLASHGAN RADIOELEKTRON VOSITALARNING ELEKTROMAGNIT MOSLASHUVCHANLIGINI BAHOLASH ALGORITMI

Asqarov U.J.
Mamatqulov M.Y.
Uzaqov V.R.

O‘zbekiston Respublikasi Mudofaa vazirligi
Maxsus avariya tiklash boshqarmasi
O‘zbekiston Respublikasi Qurolli Kuchlari Akademiyasi

Kompleks aloqa apparatxonalari tarkibida ko‘p miqdordagi turli chastota diapazoni va nurlatish quvvatiga ega radioelektron vositalarning (REV) mavjudligi o‘zaro halaqitlar hosil bo‘lishini oldini olishga alohida e’tibor qaratishni taqozo etadi. Bu muammoni samarali yechish usullaridan biri radioelektron vositalarning qabul qiluvchi antennalari o‘rnatilgan joylarda radionazorat natijalari asosida radioelektron vositalarning elektromagnit moslashuvchanligini baholash sanaladi [1].

Radionazorat vositalari radioqabul qilish qurilmalarining antennalari o‘rnatilgan yoki o‘rnatilishi belgilangan joylardagi shovqinlarning foydali signalning sifatiga ta’sir ko‘rsatishi mumkin bo‘lgan chastota oraliqlaridagi (yoki alohida chastotalardagi) elektromagnit vaziyat (EMV) haqida axborot olish imkoniyatini beradi. Ushbu axborotlarni radioqabul qilish qurilmalari va qabul qiluvchi antennalar parametrlari haqidagi ma’lumotlar bilan birgalikda radioelektron vositalarning o‘zaro elektromagnit moslashuvchanligini (EMM) baholash uchun foydalanilishi mumkin [2,3].

Radionazorat natijalari asosida EMMni baholash uchun qabul qilgich preselektorining (kirish konturining) o‘tkazuvchanlik oralig‘ida qabul qilish qurilmasiga va qabulning yon kanallari (QYK) chastotalarida kelib tushayotgan signal parametrlari haqida ma’lumotlar olinishi kerak. QYKlar soni ixtiyoriy bo‘lishi mumkin [4]. Masalan, akslangan kanal hamda geterodinning ikkinchi va uchinchi garmonikalari to‘qnashuvi natijasida hosil bo‘lgan ikkitadan chiziqli yon kanaldan iborat beshta QYK

yetarli bo‘lishi mumkin. Bu holda, EMMni baholash uchun radionazorat vositalari orqali quyidagi ma’lumotlarni olinishi zarur bo‘ladi:

1. Tekshirilayotgan qabul qilgich pereselektori oralig‘ida aniqlangan signal parametrlari:

aniqlangan signallarning umumiy soni N;

signallar aniqlangan chastotalarning tartibli ro‘yxati: $f_1<f_2< \ldots <f_N$;

ushbu chastotalarda radionazorat qurilmasida o‘lchangan $E_1, E_1, \ldots, E_N$ elektr maydoni kuchlanganligi yoki signallarning $P_1, P_2, \ldots, P_N$ quvvati ;

har bir aniqlangan signalning spektr maksimumiga nisbatan -3 dB sathdagi $B_{31}, B_{32}, \ldots, B_{3N}$ spektr kengligi.

2. Signalning radionazorat vositalari yordamida QYK chastotalarida o‘lchangan parametrlari:

o‘lchash bajarilgan QYK chastotalari: qabulning akslangan kanalining (QAK) f_1 va QYKning f_2, f_3, f_4 va f_5 chastotalari;

signallarning belgilangan chastotalarda radionazorat qurilmalari yordamida o‘lchangan P_1, P_2, P_3, P_4 va P_5 quvvati;

har bir aniqlangan halaqit qiluvchi signalning spektr maksimumiga nisbatan -3 dB sathdagi $B_{31}, B_{32}, B_{33}, B_{34}$ va B_{35} spektr kengligi.

EMMni baholash uchun o‘zaro halaqit beruvchi signalning sathi haqida parametrlardan tashqari foydali signalning sathi haqida ham axborot kerak bo‘ladi. Bunday axborot mavjud bo‘lmasa (masalan, chastotaviy-hududiy rejalashtirish bosqichida), uning qiymati qabul qilgichning sezgirligidan 3 dB yuqori olinadi [5].

Radio qabul qilgich uskunasining (RQU) baholash uchun kerak bo‘ladigan parametrlari 1-jadvalda keltirilgan.

Qabul qilgich signallari quvvati va sezgirligi ko‘pincha millivattga nisbatan detsibellarda (dBm) ko‘rsatiladi. Agar qabul qilgichda U sezgirlik ko‘rsatkichi mikrovoltlarda berilgan bo‘lsa, 30 MGsdan yuqori chastota oraliqlarida ishlayotgan RQUning kirish qarshiligini 50 Om sanalib, $P_r[dBm] = -107 + U\ [dB \cdot mkV]$ formula bo‘yicha hisoblanishi mumkin (U mikrovoltga nisbatan detsibellarda o‘lchanadi).

Bir qator holatlarda himoya nisbatlari halaqit qiluvchi signalni qabul qilgich sozlangan $\Delta f=0$ chastotadan farqlash uchun ma'lum bo'ladi. Bu holda ushbu farqni himoya nisbatlariga ta'sirini hisobga olish uchun asosiy qabul kanali (AQK) amplituda-chastota tavsifining to'g'ri burchaklilik koeffiyenti $T_{60} = B_{60}/B_r$, B_{60} – qabul qilgichning 60 dB sathdagi o'tkazuvchanlik qobiliyati, ma'lum bo'lishi lozim.

Yuqorida sanab o'tilgan parametrlarga qo'shimcha ravishda radionazorat o'lchov uskunasi hamda tekshirilayotgan qabul qilgich antennalarining kuchaytirish koeffitsiyenti haqida ma'lumotlar ham EMMni baholashda zarur bo'ladi [6].

Ushbu sanab o'tilgan parametrlar ma'lum bo'lgan holda EMMni baholash algoritmining blok-chizmasini 1-rasmda keltirilgan ko'rinishda tasvirlash mumkin bo'ladi. Taklif etilayotgan algoritm to'rtta (I, II, III va IV) asosiy blokdan tashkil topib, foydali signalga qabul qilishga QAK bo'yicha, qabul qo'shni kanali (QQK) bo'yicha, QYK bo'yicha keladigan halaqitlarning, ta'sirini, shuningdek qabul qilgichda bo'lishi mumkin bo'lgan nochiziqli (bloklash va 3-tartibdagi intermodulyatsiya) effektlarini baholash imkonini bera oladi.

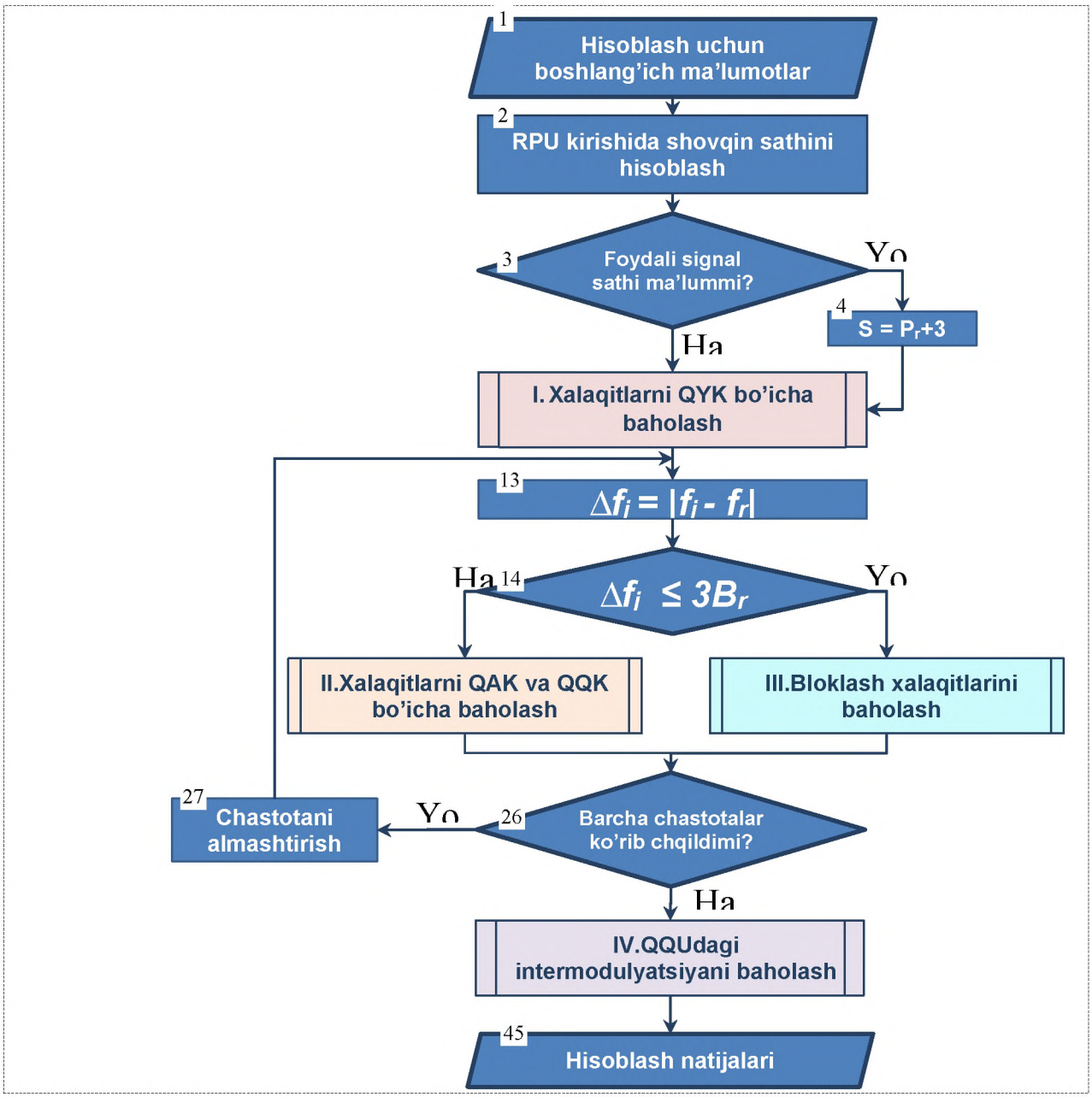
Tasvirlangan chizma bo'yicha EMMni baholash quyidagicha yuz beradi.

Kompleks apparatxonada radionazorat vositalarida olib borilgan o'lchashlar natijasida olingan dastlabki ma'lumotlar hamda tekshirilayotgan REVning parametrlari (1-jadval) kiritilgandan (1-qadam) keyin qabul qilgich kirishida aniqlangan halaqitlar quvvati hisoblanadi (2-qadam). Radionazorat natijalariga ko'ra qabul qilish antennasi o'rnatilgan joydagi maydon kuchlanganligi qiymati olingan bo'lsa, qabul qilgichning antenna-fider tarktiga (AFT) kelayotgan signalning P, dBm, quvvati quyidagi ifodaga muvofiq aniqlanadi:

$$P = E - 20\lg f + G - 77.2, \qquad (1)$$

bu yerda, Ye – qabul qilish antennasi o'rnatiladigan joydagi maydon kuchlanganligi, dB (mkV/m); f – signal chastotasi, MGs; G – qabul qilish antennasining izotrop antennaga nisbatan kuchaytirish koeffitsiyenti, dB.

Agar, o‘lchayotgan qabul qilgichining kirishidagi signal quvvati ma’lum bo‘lsa, tekshirilayotgan qabul qilgich kirishidagi signal quvvati quyidagicha aniqlanadi:



1-rasm. EMMni baholash algoritmining umumiy blok-chizmasi.

$$P_{qq} = P_{o‘lch} - G_{qq} + G_{o‘lch}, \qquad (2)$$

bu yerda, $P_{o‘lch}$, P_{qq} – mos ravishda, o‘lchayotgan va tekshirilayotgan qabul qilgichlar AFT kirishidagi signallar quvvatlari, dBm; $G_{o‘lch}$, G_{qq}– mos ravishda, o‘lchayotgan va tekshirilayotgan antennalarning kuchaytirish koeffitsiyentlari, dB.

AFTdagi omik yo‘qolishlar hisobga olmasa va AFTning moslashuvi ideal (1 ifoda uchun) yoki o‘lchayotgan va tekshirilayotgan qabul qilgichlarda bir xil (2 ifoda uchun) deb hisoblansa, keltirilgan ifodalar tekshirilayotgan qabul qilgichning kirishidagi signal quvvati qiymatini bera oladi deyish mumkin. Aks holda (1) va (2) ifodalarda olingan quvvatlar qiymatlarini tekshiriluvchi va o‘lchovchi qabul qilgichlar AFTdagi omik yo‘qotishlardagi hamda ushbu traktlarning antennalar bilan moslashmaganligi natijasida hosil bo‘ladigan yo‘qotishlardagi farqlar hisobga olingan qiymatlar bilan almashtirilishi lozim bo‘ladi.

Foydali signal sathi yuqorida ko‘rsatilgan kabi noma’lum bo‘lsa, uning qiymati qabul qilgichning sezgirligidan 3 dB yuqori qiymatda olinadi (3 va 4-qadamlar).

EMM tahlili halaqitlarning qabulning yon kanali (QYK) bo‘yicha ta’sirini baholashdan boshlanadi (I bloki).

QAK va QQK bo‘yicha halaqitlarni baholash halaqitlar chastotasidagi farq qabul qilgichning 3 o‘tkazuvchanlik polosasidan katta bo‘lmagan shartga ko‘ra II blokda bajariladi.

Bundan so‘ng keyingi chastotadagi tahlilga o‘tiladi (26, 27-qadamlar).

Halaqit qiluvchi j-signalni $\Delta f_j > 3B_r$ aniqlashda mumkin bo‘lgan bloklash effektiga ham tekshiriladi (III bloki). Qabul qilgichning turiga (analog yoki raqamli) muvofiq bloklash tahlili quyidagicha bajariladi.

Yakunlovchi bosqichda qabul qilgichdagi 3-tartibli ikki signalli intermodulyatsion halaqitlar tahlil qilinadi (IV bloki). Tahlil natijalari sifatida

Kesishish nuqtasi haqida ma’lumot mavjud bo‘lmasa, qabul qilgichning turiga (analog yoki raqamli) muvofiq intermodulyatsion halaqit quyidagicha baholanadi [8].

Analog qabul qilgich uchun uning 3-tartibdagi intermodulyatsiyaga ta’sirchanligi $I_{IM3} = P_r + D_{IM3}$, dBm, hisoblanadi. Intermodulyatsion halaqit $2P_j + P_i > 3I_{IM3}$ bo‘lganda xavfli sanaladi. Raqamli qabul qilgich uchun 3-tartibdagi intermodulyatsion halaqitning P_{IM3}, dB, quvvati qabul qilgichning xususiy shovqiniga nisbatan quyidagi ifoda bilan aniqlanadi:

$P_{IM3} = 2P_j + P_i - 3P_R - 3IMR - 9$, bu yerda IMR parametri qabul qilgich sezgirligidan 3 dB yuqori bo‘lgan signal sathi uchun aniqlangan. Agar, $P_{IM3} > 0$ bo‘lsa, intermodulyatsion halaqit raqamli qabul qilgich uchun xavfli sanaladi. Barcha juftliklar potensial xavfli chastota alomati bo‘yicha energetik baholangandan keyin algoritm ishi yakunlanadi.

Ko‘rib chiqilgan algoritm bo‘yicha hisob-kitoblar amalga oshirilishi natijasida MATB mutaxassislari tomonidan yaratilgan mobillashtirilgan boshqaruv punkti radioelektron vositalarining EMMni baholash ishlari amalga oshirildi (1-jadval).

1-jadval.

Kompleks apparatxona REQ EMMni taklif etilgan algoritm bo‘yicha baholash natijalari.

Qabulning yon kanallari bo‘yicha halaqitlar						
Kanal raqami	Chastota, MGs	Sath, dBm	Spektr kengligi, kGs	“Signal / halaqit” nisbat, dB	Himoya nisbatining me’yordan oshishi, dB	Bloklashga ta’sirchanlikni me’yordan oshishi, dB
1	928,8	– 60	300	– 43,24	– 2,24	
3	1901,4	– 70	-*	– 35,0	16,0	
Preselektordagi (kirish konturidagi) halaqitlar						
-	938,0	– 15	-*	-		5
-	938,4	– 55	-“-	-		– 35
	938,8	– 60	-“-	-		– 40
	939,2	– 30	-“-	-		0
	940,4	– 40	-“-	– 65	16,7765	-
	941,0	– 55	-“-	-		– 35
	941,6	– 25	-“-	-		– 5
	942,0	– 30	-“-	-		– 10
	942,8	– 15	-“-	-		2

* halaqitlar spektrining kengligi qabul qilgichning o‘tkazuvchanlik qobiliyatidan oshmaydi deb sanaladi.

Tahlil natijalariga ko‘ra QQU uchun o‘zaro halaqitlar xosil bo‘lishi mumkin bo‘lgan xavfli chastotalar, foydali signalni qabul qilish sifatiga ta’sir ko‘rsatuvchi kanallar, QQU ishi sifatining ruxsat etilgan darajadan pastlashiga sabab bo‘luvchi nochiziqli omillar aniqlanib, mobillashtirilgan

boshqaruv punkti antenna-fider qurilmalarining joylashuvini optimallashtirish natijasida radioelektron vositalarning o‘zaro ta’siri kamaytirildi.

Optimallashtirilgan apparatxona O‘zbekiston Respublikasi Elektromagnit moslashuv maxsus markazi davlat unitar korxonasi (DUK) mutaxassislari tomonidan maxsus tekshiruv o‘tkazilganda apparatxona tarkibidan mavjud barcha REQning yon nurlanishlari darajasi me’yor darajasida ekanligi aniqlandi, o‘zaro halaqitlari mavjud emasligi tegishli bayonnomalar bilan tasdiqlandi.

Bayon etilgan ma’lumotlardan quyidagilarni xulosa qilish mumkin:

REVlari hamda ularning texnik parametrlarini baholash asosida harbiy aloqa tizimida keng qo‘llaniladigan kompleks apparatxonalarning EMMni baholash usuli va algoritmi taklif etildi;

taklif etilayotgan algoritm halaqitlar hosil qilayotgan nurlanishlarni aniqlash, baholash hamda foydali signalni qabul qilishga ta’sirini, ya’ni EMM talablariga muvofiq REVlar ishidagi istalgan nomuvofiqliklarni bartaraf etish choralarini ko‘rish uchun yetarli axborot olish imkoniyatini beradi;

tadqiqod natijalari radiosignallarning va RQQUlarining elektromagnit moslashuvni tahlil etish uchun shart bo‘ladigan parametrlar va nisbatlarni belgilab berdi.

Foydalanilgan adabiyotlar:

[1] Антипин Б. М., Виноградов Ye. М. Оценка электромагнитной совместимости радиоэлектронных средств по результатам радиоконтроля // Изв. вузов России. Радиоэлектроника. 2012. Вып. 6. С. 97–104.

[2] Милютин Е. Р., Василенко Г. О., Сиверс М. А. Методы расчета поля в системах связи дециметрового диапазона / СПб.: Триада, 2003. 160 с.

[3] Иванов, В.А. Электромагнитная совместимость радиоэлектронных средств / В.А. Иванов, Л.Я. Ильинский, М.И. Фузик. – К. : Техника, 1983. – 120 с.

[4] Князев, А.Д. Элементы теории и практики электромагнитной совместимости радиоэлектронных средств. – М. : Радио и связь, 1984. – 336 с.

[5] Уайт, Д. Электромагнитная совместимость радиоэлектронных средств и непреднамеренные помехи / Д. Уайт; пер. с англ. – М. : Советское радио, 1977. – Вып. 1. – 348 с.

[6] Михайлов, А.С. Измерение параметров ЭМС РЭС / А.С. Михайлов. – М. : Связь, 1980. – 244 с.

[7] The Impact of ESD on Microcontrollers / Gennady A. Piskun, Viktor F. Alexeev, Sergey M. Avakov, Vladimir E. Matyushkov, Dmitry S. Titko; Edited by PhD, Aassociate professor Viktor F. Alexeev. – Minsk : Kolorgrad, 2018. – 184 p. – ISBN 978-9857-148-40-0.

[8] Князев, А. Д. Конструирование радиоэлектронной и электронно-вычислительной аппаратуры с учетом электромагнитной совместимости / А. Д. Князев. – Минск : Радио и связь, 1989. – 221с.

AXBOROT-O‘QUV TRENAJORLARINI ISHLAB CHIQISHDAGI ASOSIY QONUNIYATLAR VA PRINSIPLAR TAHLILI

Tuxliyev Sh.Yu.
Misirov Sh.Ch.
O‘R Harbiy xavfsizlik va mudofaa universitet Ilmiy-tadqiqotlar instituti ilmiy ishlar va innovatsion g‘oyalarni tashkil etish markazi boshlig‘i t.f.f.d., K.I.X., podpolkovnik.
O‘R Harbiy xavfsizlik va mudofaa universitet tabiiy fanlar kafedrasi dotsenti QKX t.f.n., dotsent.

Barcha bo‘limdagi professional harbiy kadrlar tayyorlash tizimini takomillashtirish, ta’lim jarayoniga eng yangi usul va texnologiyalarni joriy etish, o‘quv auditoriyalarini zamonaviy trenajyorlar, o‘quv va laboratoriya asbob-uskunalari hamda kompyuter texnikalari bilan jihozlash lozimligini O‘zbekiston Respublikasi Prezidenti Shavkat Miromonovich Mirziyoyev O‘zbekiston Respublikasi Qurolli Kuchlarining 25 yilligi munosabati bilan Vatan himoyachilariga yo‘llagan bayram tabriklarida alohida ta’kidlaganlar[1].

Kursantlarning harbiy-texnik va harbiy - maxsus tayyorgarligi, bu ta'lim oluvchilar tomonidan tizimli bilimlarni o'zlashtirish, qurol-aslaha va jangovar texnikalarni ishonchli qo'llash hamda ularni ekspluatasiya qilish va ta'mirlash asosida jangovar vazifalarni bajarish malakasi va ko'nikmalarini shakllantirish jarayonidir. Uning mohiyati oliy harbiy ta'lim sohasi bo'yicha Davlat ta'lim standartlari, bitiruvchilarga qo'yilgan malaka talablari va bitiruvchilarning bilimi, malakasi, ko'nikmasi hamda o'quv va jangovar vazifalarni bajarishga ruhiy jihatdan tayyorligi bilan belgilanadi.

Ma'lumki, ofitserlarning harbiy-maxsus tayyorgarligining asosiy poydevori Oliy harbiy ta'lim muassasalarida nazariy va amaliy tayyorgarlik jarayonida shakllanadi. Boshqaruv taktik darajasidagi ofiserlarning harbiy-maxsus tayyorgarligining asosiy natijalari quyidagilardan iborat: qurol va harbiy texnikani ishlatish va ta'mirlash ko'nikmalari, barcha turdagi qurollardan o'q otish, barcha turdagi avtomobil va zirhli texnikalarni boshqarish va boshqalar.

Harbiy-texnik va harbiy-maxsus tayyorgarlik bo'yicha kursantlarda kasbiy malaka va ko'nikmalarni shakllantirish samaradorligini oshirish maqsadida Oliy harbiy ta'lim muassasalarda turli o'quv trenajyorlaridan foydalaniladi. Biroq, o'quv mashg'ulotlari davomida kafedralarda mavjud bo'lgan o'quv trenajyorlaridan foydalanish orqali erishiladigan o'quv hamda didaktik maqsadlarga erishish ko'rsatgichi lozim darajaga yetkazilmagan.

Shuningdek, Oliy harbiy ta'lim muassasalarda trenajyor komplekslaridan harbiy maxsus fanlarning o'qitilishida samarali va oqilona foydalanish, ular yordamida kursantlarning tayyorgarligini tahlil qilish tajribasi hamda pedagogik amaliyotga to'liq tadbiq qilish yetarli darajada amalga oshirilmayapti. Shu va boshqa shu kabi kamchiliklarning mavjudligi o'quv trenajyorlaridan foydalangan holda kursantlarning harbiy – maxsus tayyorgarligini oshirish metod va uslublarini faol izlash zarurligini ko'rsatadi. Bunday uslublardan biri nafaqat maxsus harbiy mashg'ulotlarda an'anaviy trenajyorlardan foydalanish, balki yangi zamonaviy dasturlash vositalari asosida ishlab chiqilgan o'quv

trenajyorlarini yaratish va ularni samarali qo‘llashdan iborat bo‘lmog‘i lozim[2].

Kursantlarda “Jangovar mashinalarni boshqarish”, “Otish tayyorgarligi” va “Taktika” fanlaridan amaliy bilim, ko‘nikma va malakalarni shakllantirishda o‘quv tajribalarining ahamiyati beqiyosdir. O‘quv tajribalarining asosini esa amaliy ishlar tashkil etadi. Hozirgi kunda ta’lim muassasalarida va O‘zbekiston Respublikasi Mudofaa vazirligiga qarashli harbiy qismlarda alohida jangovar mashinalarni boshqarish trenajyorlari va alohida yo‘naltiruvchi-operatorlarning (mo‘ljalga oluvchilarning) trenajyorlari mavjud.

Shu bilan birga, jangovar mashina ekipaji a’zolarini jang maydonidagi harakatlarni to‘liq ekipaj tarkibida va bo‘linmalar tarkibida mashq qildirish imkoniyati mavjud bo‘lgan majmuaviy trenajyorlar yo‘q. Harbiy trenajorlarni qo‘llashning foydaliligi keyingi paytlarda Iroqda, Bosniyada, Yugoslaviyada, Afg‘onistonda yuz bergan cheklangan harbiy nizolarning barchasida bir necha marta isbotlangan. Trenajorlar jangovar harbiy harakatlarni rejalashtirishda, u yoki bu vazifani bajarish bo‘yicha harbiy kuch va vositalarni optimallashtirishda, biror bir holatdan chiqishning ko‘p sonli variantlari ishlab chiqilgan qurilmalardir. Masalan, Iroq, Bosniya, Yugoslaviyadagi nizolarni hal etishda kuchli darajadagi past-balandliklardan iborat tog‘li joy uchun majmuaviy aviasiya trenajorlari yordamida aviatsiya zarbalari berishning ishlab chiqilishi, birinchi urinishdayoq, eng kam miqdordagi qurollar va jangovar yo‘qotishlar sarfi bilan qo‘yilgan topshiriq natijalariga erishilgan[3].

Zamonaviy urushning har kunida, u cheklangan nizomi yoki dunyo miqyosidagi jangovar harbiy harakatlarmi, ular urishayotgan mamlakatlarning odamlari va moddiy resurslarini kamaytiradi. Vaqt o‘tishi bilan, qurolli kuchlarning turli xillarini ommaviy qo‘llash maqsadi qo‘yilsa, qo‘yilgan maqsadlarga qisqa vaqtlarda, kuch va vositalarni eng kam sarflagan holda erishish talab etilsa, harbiy harakatlar puxta rejalashtirilishi va nafis amalga oshirilishi lozim bo‘ladi. Buni amalga oshirish uchun esa barcha topshiriqlar avvalo trenajorlarda ko‘plab marta ishlab chiqilishi talab etiladi.

Shunga asoslanib, agar biz buning uchun xarajatlarni kamaytirmoqchi bo‘lsak, unda trenajor mashg‘ulotlari ko‘p soatlik takrorlanadigan va asta-sekin murakkablashib boradigan mashqlarga asoslangan bo‘lishi kerak, bu esa individual va jamoaviy ko‘nikmalarni singdirishga, so‘ngra ularni rivojlantirishga imkon beradi va bunga iqtisodiy nuqtai nazardan kompleks trenajorlar va modellashtiruvchi tizimlardan foydalanish orqali eng oson erishiladi [4].

Amaldagi harbiy tayyorgarlik texnologiyalaridan foydalanishni tahlil qilish shuni ko‘rsatadiki, ushbu texnologiyalardan turli davlatlar armiyalarida foydalanish qor ko‘chkisi singari o‘sib bormoqda. Harbiy trenajorlardan foydalanishning amaliy foydaliligi so‘nggi mahalliy qurolli to‘qnashuvlarda (Iroq, Bosniya, Yugoslaviya, Afg‘oniston, Ukraina) bir necha bor isbotlangan. Jangovar operatsiyalarni rejalashtirishda trenajorlardan foydalanilgan, ular ma’lum bir vazifani bajarish uchun kuchlar va aktivlarning otryadlarini optimallashtirish uchun ishlatilgan va turli xil ma’lumotlar bilan muayyan vaziyat natijalarining ko‘plab variantlari ishlab chiqilgan.

Masalan, kuchli darajadagi past-balandliklarga ega bo‘lgan tog‘li yerlarda jang qilishni mashq qilishda, kompleks aviatsiya trenajorlarida havo hujumlarini amalga oshirish, birinchi birinchi urinishdan boshlab, qimmat qurollarni eng kam sarf qilish va minimal jangovar yo‘qotishlar bilan belgilangan natijalarga erishishga imkon berdi (Iroq, Bosniya, Yugoslaviya, Ukraina).

Bugungi kunda harbiy tayyorgarlik texnologiyalari armiya oldida turgan deyarli barcha vazifalarni qamrab olgan. Maxsus o‘quv majmualari, shuningdek, barcha darajadagi qo‘mondonlik shaxsiy tarkibi, qo‘shinlarning barcha tarmoqlari va turlari uchun ishlatiladi. Bunday trenajorlar turli xil miqyosdagi harbiy operatsiyalar o‘ynaladigan harbiy operatsiyalar teatrining raqamli modeli deb nomlanadi, uning davomida qurolli kuchlarning qo‘mondonligi harbiy operatsiyalarni rejalashtirish va boshqarish bo‘yicha zarur ko‘nikmalarga ega bo‘ladi.

Yuqoridagi trenajor majmualari kompyuter texnologiyalarining so‘nggi yutuqlari asosida qurilgan. Trenajorlarda ishlatiladigan

kompyuterlar turli xil trenajorlarni katta kompyuter tarmog‘iga birlashtirishga imkon beradi va shu bilan real vaqtda turli kuchlarning o‘zaro harakatini simulyatsiya qiladi.

O‘z navbatida, har bir trenajorning o‘ziga xos xususiyati (askarlar va ofitserlar, jangovar texnika, samolyotlar, kemalar va boshqalar ekipajlarini individual yoki jamoaviy o‘qitish uchun) u yoki bu to‘liq miqyosdagi, yarim tabiiy yoki virtual (ya’ni to‘liq elektron) bilan aniqlaniladigan harbiy obyekt, bu mashg‘ulotlar olib boriladigan harbiy harakatlar teatri texnikasi yoki modellaridir.

Taktik tayyorgarlikning axborot-oquv trenajorlarining tahlili shuni ko‘rsatdiki, ular taktik mashg‘ulotlar pedagogik jarayonining ajralmas qismi hisoblanadi. Ushbu jarayonning maqsadi harbiy xizmatchilarni ma’lum bilim, ko‘nikma va malakalarga o‘rgatishdir. O‘qitishning umumiy pedagogik tamoyillari trenajorlar rivojlanishining asosiy qonuniyatlarini o‘quv vositalari tizimining ajralmas qismi va taktik tayyorgarlik pedagogik jarayonining ajralmas qismi sifatida aniqlashga imkon beradi.

Axborot-o‘quv trenajor (AO‘T) larini ishlab chiqishda *asosiy qonuniyat - bu ularning didaktik va texnik imkoniyatlarining taktik tayyorgarlik tizimidagi mashg‘ulotlar vazifalariga muvofiqligi.*

Motoo‘qchi bo‘linmalari taktikasini takomillashtirish shaklida yuz beradigan o‘quv vazifalarining doimiy o‘zgarishi, O‘zbekiston Respublikasi Mudofaa vazirligining harbiy qismlar va bo‘linmalarni butlash uslubidagi o‘zgarishlar, tashkiliy-shtat tuzilishdagi o‘zgartirishlar, armiyani qurollantirishga yangi murakkab qurol-yarog‘ va harbiy texnika (JZT) foydalanishga topshirilganda, tegishli AO‘T mavjudligini talab qiladi (yangisini ishlab chiqish yoki mavjudlarini takomillashtirish).

Motoo‘qchi qismlari va bo‘linmalari turli ixtisosliklari bo‘yicha harbiy xizmatchilarni tayyorlash uchun (doimiy tayyorlik darajasi), ularning belgilangan darajadagi tayyorgarligini to‘liq ta’minlaydigan, zarur ko‘nikmalarni saqlab turadigan va kerak bo‘lganda ularni qayta tiklaydigan axborot-o‘quv trenajorlarini yaratilishi kerak.

Kompyuter texnologiyalaridan foydalanishga asoslangan zamonaviy koompleks harbiy trenajorlar murakkab dasturiy ta'minot va qurilmalardir. Yangi axborot texnologiyalarining sezilarli darajada rivojlanishi istiqbolli axborot - mashq trenajorlarini yaratishda kompyuter modellashtirish, atrof-muhit va fono-maqsadli muhitni audio-vizuallashtirish, axborot uzatish vositalarining so'nggi yutuqlaridan foydalanishni talab qiladi.

Shuni hisobga olgan holda trenajorlarni ishlab chiqishni rivojlantirishning yana bir qonuniyati, ularning mukammalligi darajasining ulardagi axborot texnologiyalarining so'nggi yutuqlaridan foydalanishga bog'liqligi deb hisoblash kerak. Axborot-o'quv trenajyorlari o'rganuvchilarda zarur ko'nikma va malakalarni shakllantirishni ta'minlaydigan o'quv vositalari tizimining ajralmas qismidir.

Shuni yodda tutish kerakki, o'quv vositalari o'quvchilarga pedagogik ta'sir ko'rsatadigan moddiy obyektlardir.

Yangi didaktik imkoniyatlarga ega bo'lgan axborot – o'quv trenajyorlarini yaratish, avvalo, o'qitish pedagogikasi va psixologiyasi talablariga asoslanishi kerak.

Shundan kelib chiqadigan bo'lsak, axborot – o'quv trenajorlarini rivojlantirishning quyidagi qonuniyati amalga oshiriladi - *istiqbolli trenajorlar, o'quv majmualari va o'quv metodik talablarni ishlab chiqishda kompyuterli o'qitish dasturlarini yaratish to'g'risida o'qitish pedagogikasi va psixologiyasi sohasidagi so'nggi yutuqlarning hal qiluvchi va bevosita ta'siri bo'lishi kerak.* Yangi didaktik imkoniyatlar bilan istiqbolli AO'T dan samarali foydalanish, ularni qo'llash usullarini takomillashtirmasdan mumkin emas.

Shuning uchun yangi yuqori texnologik AO'T ni yaratish, ularni qo'llashning yangi usullarini yaratish, jangovar tayyorgarlik dasturi, o'q otish kursi va taktik va otish tayyorgarligi metodikalarini yaratish bilan birga bo'lishi kerak.

Shularni hisobga olgan holda, AO'T ni rivojlantirishning yana bir qonuniyatini ta'kidlash kerak - *AO'T ni takomillashtirish yangi o'quv uslublari, mashg'ulotlar darajasini baholashning yangi usullari, harbiy xizmatchilar va qismlarning taktik tayyorgarligini tashkil etish, o'tkazish*

va monitoringini olib borish tartibini belgilaydigan hujjatlarning yaxshilanishi bilan chambarchas bog'liq holda amalga oshirilishi kerak.

Harbiy trenajorlardan samarali foydalanish, ularga (kafolat va kafolatdan keyingi) texnik xizmat ko'rsatish, ta'mirlash va modernizatsiya qilish tizimini takomillashtirmasdan ham mumkin emas. Shu nuqtai nazardan, *rivojlanishning qonuniyatligini ta'kidlash kerak, chunki ularga texnik xizmat ko'rsatish va ta'mirlash tizimini bir vaqtning o'zida qo'shinlarga taktik o'quv mashg'ulotlarining yangi tizimlarini kiritish kerak.*

Shunday qilib, AO'T taktik tayyorgarligini rivojlantirishning asosiy qonuniyatlariga quyidagilarni kiritish kerak: simulyatorlarni ishlab chiqish taktik tayyorgarlik tizimining barcha elementlari bilan yaqin aloqada bo'lishi kerak; istiqbolli harbiy trenajorlarni yaratish va ulardan foydalanishga o'qitish pedagogikasi va psixologiyasi qonunlari va tamoyillarining asosiy ta'siri; rivojlangan integral harbiy trenajorlarga qo'yiladigan didaktik va texnik talablar o'quv maqsadlariga mos kelishi kerak; harbiy trenajorlarning takomillashish darajasining yangi axborot texnologiyalaridan foydalanishga bog'liqligi; prinsipial jihatdan yangi o'quv binolarini yaratish, ulardan foydalanish usullarini ishlab chiqish bilan bir qatorda jangovar tayyorgarlik dasturi, o'q otish kursi hamda taktik va otish tayyorgarligi mashqlari uslublarini o'zgartirish bilan birga bo'lishi kerak.

AO'T ning taktik tayyorgarlik tizimidagi roli va o'rni, o'qitish vositalarini takomillashtirishga ta'sir etuvchi omillar va AO'T ni rivojlantirish qonuniyatlarini tahlil qilish bizga *o'qitishning istiqbolli tizimini yaratish uchun eng umumiy tamoyillarni shakllantirishga* imkon beradi.

O'qitishning istiqbolli tizimini yaratish uchun asos bo'lishi kerak bo'lgan *asosiy prinsip - bu o'quv vositalarining o'quv mazmuni va didaktik vazifalarga muvofiqligi prinsipi.*

Istiqbolli o'quv vositalarini yaratish asosida yotadigan boshqa prinsiplar:

ratsionallik prinsipi - yaratilgan o‘quv vositalariga muvofiq o‘quv vazifalarini oqilona taqsimlash, ya’ni ishlab chiqilayotgan vositalarning murakkabligi (har doim ham texnik emas) ular bo‘yicha hal qilingan o‘quv vazifalarining ahamiyatiga mos kelishi kerak;

izchillik prinsipi - barcha o‘quv vositalari ma’lum bir tizim uchun umumiy va yagona baholash me’yorlari bilan o‘zaro bog‘liq bo‘lishi kerak, ya’ni o‘rganuvchining bir texnik o‘qitish vositasidan boshqasiga o‘tishi faqat uning faoliyatini avvalgi vositalar bo‘yicha baholash asosida amalga oshirilishi kerak;

yetarlilik prinsipi - tizimning har bir texnik vositalari tizimning boshqa vositalari bilan yechilgan vazifalarni takrorlamaydigan ma’lum o‘quv vazifalarini hal qilishi kerak;

uzluksizlik prinsipi – o‘quv vositalari tizimini tashkil etadigan vositalarning soni va texnik tavsiflari, uni amalga oshiradigan vositalarning to‘liq yuklanishi bilan uzluksiz o‘quv jarayonini ta’minlaydigan tarzda tanlanishi kerak. Mazkur tamoyil o‘quv jarayonida mutaxassis faoliyatining o‘ziga xos xususiyatlarini hisobga olishni talab qiladi.

Shu bilan birga, ko‘p vaqt talab qiladigan faoliyatning eng qiyin elementlari (harakatlar, operatsiyalar) yuqori o‘tkazuvchanlik qobiliyatiga ega qurilmalarda mashq qilinishi kerak;

funksional moslashuvchanlik prinsipi – o‘qitish vositalari tizimining elementlari o‘quv tizimining hayoti davomida yuzaga keladigan kasbiy faoliyatning mohiyati va tarkibidagi mumkin bo‘lgan o‘zgarishlarni hisobga olgan holda ishlab chiqilishi kerak;

meros bo‘lib qolishlik prinsipi - mavjud bo‘lgan har bir yangi tizim vositasini ishlab chiqishda, ilgari yaratilgan vositaning tuzilishi va ishlash tajribasini hisobga olish kerak. Yangi vosita, sezilarli o‘zgarishsiz, mavjud o‘quv tizimiga ham metodik, ham konstruktiv tarzda mos kelishi kerak. Axborot-mashq trenajorlari va ularni ishlab chiqish tamoyillarining rivojlanish qonuniyatlarini aniqlash istiqbolli harbiy trenajorlarning rivojlanish tendensiyalari va o‘quv-uslubiy talablarni oqilona aniqlashga imkon beradi[4].

Shu bilan birga, barcha o‘quv-mashq va trenajor vositalari quyidagi umumiy talablarga javob berishi kerak:

mashg‘ulotlarda ko‘rgazmalilikni va mavjudlikni maksimal darajada ta’minlash, mashg‘ulot vaqtidan samarali foydalanish, qiziqish uyg‘otish va o‘qitish jarayonda shaxsiy tarkibning faolligini oshirish;

rahbarga mashg‘ulotlar jarayonida o‘rganuvchilardan mustaqil ravishda va ilgari olingan bilim, ko‘nikma va malakalarni amalda qo‘llashni talab qiladigan harakatlari uchun turli xil sharoitlarni yaratishga imkon berish;

o‘rganuvchilarning xatti-harakatlari va ular o‘rgangan materiallarni o‘zlashtirishi ustidan obyektiv nazoratni amalga oshirish, kursantlar tomonidan yo‘l qo‘yilgan xatolar va yetarli darajada o‘zlashtirilmagan savollarni aniqlash;

tuzilishi jihatidan sodda, ishlatishda ishonchli va barqaror bo‘lishi, ish va texnik xizmat ko‘rsatishga tayyorgarlik ko‘rish uchun minimal vaqtni talab qilishi;

mashg‘ulotlar davomida o‘rganuvchilarning xavfsizligini to‘liq ta’minlash [5].

Jangovar tayyorgarlikni rivojlantirishning yuqorida qayd etilgan qonuniyatlari va tamoyillarini aniqlab, shuningdek ularga Axborot – o‘qitish trenajorlari (AO‘T) ning rivojlanishiga ta’sir ko‘rsatishi uchun asos yaratib, hozirgi vaziyatni tanqidiy tahlil qilish, va jangovar vazifalarning bajarilishini ta’minlashga imkon beradigan harbiy trenajorlar (trenajor majmualari) bilan O‘zbekiston Respublikasi Mudofaa vazirligining harbiy qismlarini jihozlash nuqtai nazaridan tanqidiy tahlil qilish mumkin .

Shuni ta’kidlash kerakki, so‘nggi yillarda O‘zbekiston Respublikasi Qurolli Kuchlari kundalik xizmat va jangovar harakatlarida, harbiy oliy ta’lim muassasalari bazalari asosida, kurs davomida ham motoo‘qchi, tank, maxsus va boshqa tuzilmalar (qismlar) shaxsiy tarkibini tayyorlash uchun kompyuter vositalaridan tobora ko‘proq foydalanmoqdalar.

Qo‘shinlarda trenajor vositalarini ishlab chiqish va amalda qo‘llash bo‘yicha quyidagi asosiy vazifalarni hal etish tavsiya etiladi:

mashg‘ulotlar vaqtini ko‘paytirish, raqamli xaritalar asosida yaratilgan va simulyatsiya qilingan jangovar vaziyatlarning xilma-xilligini oshirish orqali ekipajlarning jangovar tayyorgarligini oshirish, oddiy harbiy xizmatdan tortib mashg‘ulotlarda qatnashayotgan harbiy xizmatchilarning qamrovi kengligi ekipaj tarkibida, bo‘linmalarda, qurolli kuchlarning bo‘linmalari va qurolli kuchlarning tarmoqlari o‘rtasida o‘zaro aloqalarni rivojlantirish;

ekipajlarni haqiqiy texnologiyalardan foydalangan holda taqlid qilib bo‘lmaydigan sharoitlarda, masalan, ommaviy qirg‘in qurollaridan foydalanish sharoitida, shaharda texnika vositalaridan foydalanish, tinch aholi orasida;

harbiy texnika yoqilg‘isi va motor resurslarini tejash orqali o‘qitish xarajatlarini sezilarli darajada kamaytirish.

Kompyuter trenajorlaridan keng foydalanish zamonaviy kompyuterlarning ancha arzonlashib ketganligi, kompyuterlarning texnik tavsiflari real sharoitlarni yuqori darajadagi ishonchlilik bilan simulyatsiya qilishga imkon beradi, hatto eng qimmat - dinamik kompyuter majmualarining ham ketgan xarajatlarni qoplashi uchun foydalanish intensivligi olti oydan bir yilgacha oralig‘ida bo‘lib, mamlakatimiz harbiy xizmatchilarining jangovar tayyorgarligi tizimiga sezilarli darajada iqtisodiy foyda keltiradi.

XULOSALAR

1.Axborot-o‘quv trenajor (AO‘T) larini ishlab chiqishda asosiy qonuniyat - bu ularning didaktik va texnik imkoniyatlarining taktik tayyorgarlik tizimidagi mashg‘ulotlar vazifalariga muvofiqligi.

2.Istiqbolli trenajorlar, o‘quv majmualari va o‘quv metodik talablarni ishlab chiqishda kompyuterli o‘qitish dasturlarini yaratish to‘g‘risida o‘qitish pedagogikasi va psixologiyasi sohasidagi so‘nggi yutuqlarning hal qiluvchi va bevosita ta’siri bo‘lishi kerak.

3.AO‘T ni takomillashtirish yangi o‘quv uslublari, mashg‘ulotlar darajasini baholashning yangi usullari, harbiy xizmatchilar va qismlarning taktik tayyorgarligini tashkil etish, o‘tkazish va monitoringini olib borish

tartibini belgilaydigan hujjatlarning yaxshilanishi bilan chambarchas bog‘liq holda amalga oshirilishi kerak.

4.Harbiy trenajorlardan samarali foydalanish, ularga (kafolat va kafolatdan keyingi) texnik xizmat ko‘rsatish, ta’mirlash va modernizatsiya qilish tizimini takomillashtirmasdan ham mumkin emas. Shu nuqtai nazardan, rivojlanishning qonuniyatligini ta’kidlash kerak, chunki ularga texnik xizmat ko‘rsatish va ta’mirlash tizimini bir vaqtning o‘zida qo‘shinlarga taktik o‘quv mashg‘ulotlarining yangi tizimlarini kiritish kerak.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasi Qurolli Kuchlarining 25 yilligi munosabati bilan Vatan himoyachilariga yo‘llangan bayram tabrigi. / Sh. M. Mirziyayev. https://daryo.uz/2017/01/13/ (murojaat sanasi 10.12.2019).

2. A. I. Musulmanov. Kursantlarning harbiy - texnik va harbiy - maxsus fanlardan tayyorgarligini takomillashtirishning ayrim jihatlari.// O‘R QK Akademiyasi xabarlari, 2019. № 3 (31).

3. Комплексный тренажер экипажа боевой машины пехоты ПЖМ-2./ А. Н. Матвиевский, Н. А. Матвиевский, Т. Г. Бондаренко, Е. И. Казеев, И. А. Касян, В. И. Касян. https://docplaer.ru/71403002. 1919.(мурожаат санаси 10.12.2019).

4.Пономарев, А. Ю. Роль и место информационно-обучающих тренажеров в боевой подготовке подразделений воздушно-десантных войск / А. Ю. Пономарев. — Текст: непосредственный // Педагогика: традиции и инновации: материалы II Междунар. науч. конф. (г. Челябинск, октябрь 2012 г.). — Челябинск: Два комсомольца, 2012. — С. 204-208. — URL: https://moluch.ru/conf/ped/archive/63/2757/ (дата обращения: 06.01.2021).

5. А.В. Дмитрук. Методика подготовки и проведения занятий с использованием учебных тренировочных и тренажерных средств. http://ebooks.grsu.by/dmitruk/06.07.2021.

O‘ZBEKISTON RESPUBLIKASI MILLIY GVARDIYASI BO‘LINMALARI OBYEKTLARINI QO‘RIQLASHDA AXBOROT XAVFSIZLIGI TUSHUNCHASI VA UNING ASOSIY TAMOYILLARI

Ochilov I.N.
O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti Qo‘riqlashni muhandislik-texnik ta’minlash kafedrasi dotsenti, h.f.b.f.d. (PhD) dotsent

Tarixga nazar soladigan bo‘lsak, axborot xavfsizligini ta’minlash vosita va usullari, axborotni saqlash va uzatishning yangidan-yangi vositalari paydo bo‘lishiga qarab o‘zgarib, takomillashib kelgan.

Elektr va radio aloqa vositalari paydo bo‘lishi bilan axborotni yashirin jo‘natish uchun signallarni radio halaqitlarga turg‘un kodlar bilan uzatish ehtiyoji tug‘ilgan.

Elektron hisoblash mashinalarining paydo bo‘lishi, axborotni kodlashtirish bilan birga uni saqlash va qayta ishlash qurilmalaridan foydalanishni chegaralash usullari, simmetrik va nosimmetrik shifrlash algoritmlarini yaratish axborot xavfsizligining asosiy vazifasiga aylandi.

Kompyuter lokal va global tarmoqlari paydo bo‘lishi bilan unda saqlanayotgan va uzatilayotgan axborot davlat miqyosidagi resurslarga aylandi. Axborot xavfsizligini ta’minlash milliy xavfsizlik vazifalari tarkibiy qismi tarzida qaraladigan bo‘ldi.

Axborot xavfsizligi - fuqarolar, tashkilotlar va davlat manfaati yo‘lida jamiyat axborot muhitini shakllantirish, takomillashtirish hamda undan foydalanish jarayonida uning ichki va tashqi tahdidlardan himoyalanganligini ta’minlovchi holat.

Biror-bir obyektning axborot xavfsizligini ta’minlash uchun mazkur obyektning *axborot xavfsizligini ta’minlash tizimini* (AXTT) ishlab chiqish kerak. Buning uchun quyidagi vazifalarni bajarish lozim:

- obyekt xususiyatlaridan kelib chiqib, axborot himoyasi talablarini aniqlash;
- xalqaro va milliy qonunchilik talablariga rioya qilish;

- AXTTni qurish tajribalaridan (standartlar, uslublardan) foydalanish;
- AXTTni joriy qilish va ishlatish uchun mas'ul bo'linmalarni aniqlash va javobgarlikni taqsimlash;
- xavfsizlik risklari hisob-kitobi asosida himoya qilinuvchi obyektning axborot xavfsizligi siyosatini tashkil qiluvchi texnik va tashkiliy talablarni aniqlash;
- kerakli dasturiy-texnik usul va vositalarni joriy qilib, axborot xavfsizligi siyosatini ishlab chiqish;
- axborot xavfsizligi boshqaruv tizimini (AXBT) ishlab chiqish;
- AXBT vositasida, AXTT ish samaradorligini doimiy nazorat qilish.

Axborot xavfsizligi – axborotning konfidensialligi va yaxlitligini, vakolatli subyektlar tomonidan axborotdan oson foydalanishni ta'minlash jarayoni (1.).



1-rasm. Axborot xavfsizligining tarkibiy yo'nalishlari

Axborot xavfsizligi deganda, konfidensial hujjatlar, axborot tizimida ma'lumot konfidensialligini himoya qilish, tushuniladi. "Konfidensiallik" tushunchasi deyarli barcha sohalarda foydalaniladi. Tashkilot, idora, muassasalardagi konfidensiallik deganda, asosan, harbiy yoki davlat sirlari nazarda tutiladi.

Konfidensiallik – vakolatli subyektlarga axborotdan foydalanishga ruxsat berishni ta'minlashdir.

Konfidensial ma'lumotlarga quyidagilar kiradi:

- fuqaroning shaxsini identifikatsiya qilish imkonini beradigan, hodisalar, sharoitlar to‘g‘risidagi ma'lumotlar (qonunchilikda nazarda tutilgan yo‘l bilan ommaviy axborot vositalarida tarqatiladigan ma'lumotlar bundan mustasno);
- tergov va sud sirlari hamda himoyalanuvchilar to‘g‘risidagi ma'lumotlar;
- O‘zbekiston Respublikasi Fuqarolik kodeksiga ko‘ra foydalanilishi xizmat doirasida chegaralangan ma'lumotlar (xizmat siri);
- O‘zbekiston Respublikasi Konstitutsiyasi va qonunlariga ko‘ra professional faoliyat bilan bog‘liq ma'lumotlar (vrachlik, notarial va advokatlik sirlari, yozishma va telefon suhbatlari sirlari va h.k.);
- O‘zbekiston Respublikasi Fuqarolik kodeksiga ko‘ra chegaralangan, harbiy faoliyati bilan bog‘liq ma'lumotlar (harbiy sirlari);
- to ular haqida rasmiy xabar berilguncha, ilmiy tadqiqot mohiyati, modeli yoki ishlab chiqarish namunasi to‘g‘risidagi ma'lumotlar.

Harbiy sirni tashkil etuvchi konfidensial ma'lumotlar (ishlab chiqarish siri) – ishlab chiqarishga oid texnik, iqtisodiy, tashkiliy va boshqa ixtiyoriy xarakterdagi ma'lumotlar. Bular jumlasiga ilmiy-texnik sohadagi intellektual izlanishlar natijalari ham kiradi.

Axborot egasi tomonidan uning konfidensialligini himoya qilishga qaratilgan asosiy yo‘l-yo‘riqlar quyidagilardan iborat:

- harbiy sirlarini tashkil etadigan ma'lumotlar ro‘yxatini aniqlash;
- murojaat tartib-qoidalarini o‘rnatish orqali harbiy sirlarini tashkil etadigan axborotdan foydalanishni chegaralash;
- konfidensiallik tartib-qoidasiga rioya qilish nazoratini muntazam amalga oshirib borish;
- konfidensial axborotdan foydalanishga ruxsat berilgan yoki undan foydalangan shaxslar ro‘yxatini tuzib borish;

- konfidensial ma’lumot saqlanuvchi vositalar ustiga “xizmat doirasida foydalanish uchun” kabi grifni kerakli qo‘shimcha ma’lumotlari bilan birga yozib qo‘yish.

Yaxlitlik – axborotni saqlash, uzatish va unga ishlov berishda ishonchliligi va to‘liqligini ta’minlash.

Axborot yaxlitligi – informatika va telekommunikatsiya nazariyasi atamalariga ko‘ra, ma’lumotlar saqlanishi, uzatilishi, taqdim etilishi jarayonida o‘zgarmagan axborot. Axborot xavfsizligi, kriptografiya sohasida axborot yaxlitligi deganda ma’lumot qanday yaratilgan bo‘lsa, o‘sha holda o‘zgarmasdan turganligi tushuniladi.

Axborot yaxlitligi buzilishiga sabab bo‘ladigan holatlar:

- buzg‘unchi shaxs bank tranzaksiyalarida akkaunt nomerini o‘zgartirishi yoki hujjatni soxtalashtirishi.
- ma’lumotni uzatish yoki saqlashda texnik sabablarga ko‘ra uning o‘zgarib qolishi.
- ko‘pchilik fikrini boshqarish maqsadida ommaviy axborot vositalarida atayin faktlarni o‘zgartirib ko‘rsatish va h.k.

Kompyuter axborot tizimlarida, axborot yaxlitligini saqlash uchun quyidagi asosiy usullar qo‘llaniladi:

- ma’lumotlardan muntazam nusxa ko‘chirib saqlab borishni ta’minlash;
- ma’lumot saqlash vositalariga RAID-massiv yoki “Oyna aksi” (mirroring) kabi texnologiyalarni qo‘llab, to‘satdan buzilib qolishdan himoya;
- ma’lumotni elektron arxivlashtirish yordamida qayta tiklash;
- ma’lumot uzatishda uning yaxlitligini ta’minlash uchun kriptografik himoya (shifrlash, xesh funksiya, elektron raqamli imzo) usullaridan foydalanish va h.k.

Odatda, ixtiyoriy axborot tizimi muayyan axborot xizmatlarini ko‘rsatish uchun hosil qilinadi. Agar foydalanuvchilarga mazkur xizmat ko‘rsatilmasa, ma’lumot almashish subyektlariga zarar yetadi.

Axborot tizimi xavfsizligini ta’minlashda, nafaqat saqlanayotgan ma’lumotni o‘zgartirish, o‘g‘irlash, yo‘q qilishdan himoyasini ta’minlash,

balki kerak bo‘lganda, vakolatli foydalanuvchilar uchun ma’lumotdan foydalanish, tarqatish va ko‘paytirish imkoniyatlarini chegaralashdan himoyasini ham ta’minlash axborot xavfsizligi vazifalariga kiradi.

Axborotdan foydalanish *– vakolatli foydalanuvchilarga, hech qanday to‘siqsiz axborotdan osongina foydalanishni ta’minlash.*

Foydalanish huquqiga: ma’lumotni o‘qish, ko‘paytirish, o‘zgartirish, yo‘q qilish kiradi.

Axborot tizimlari ma’lumotlaridan foydalanishni ta’minlash uchun quyidagilarni amalga oshirish kerak:

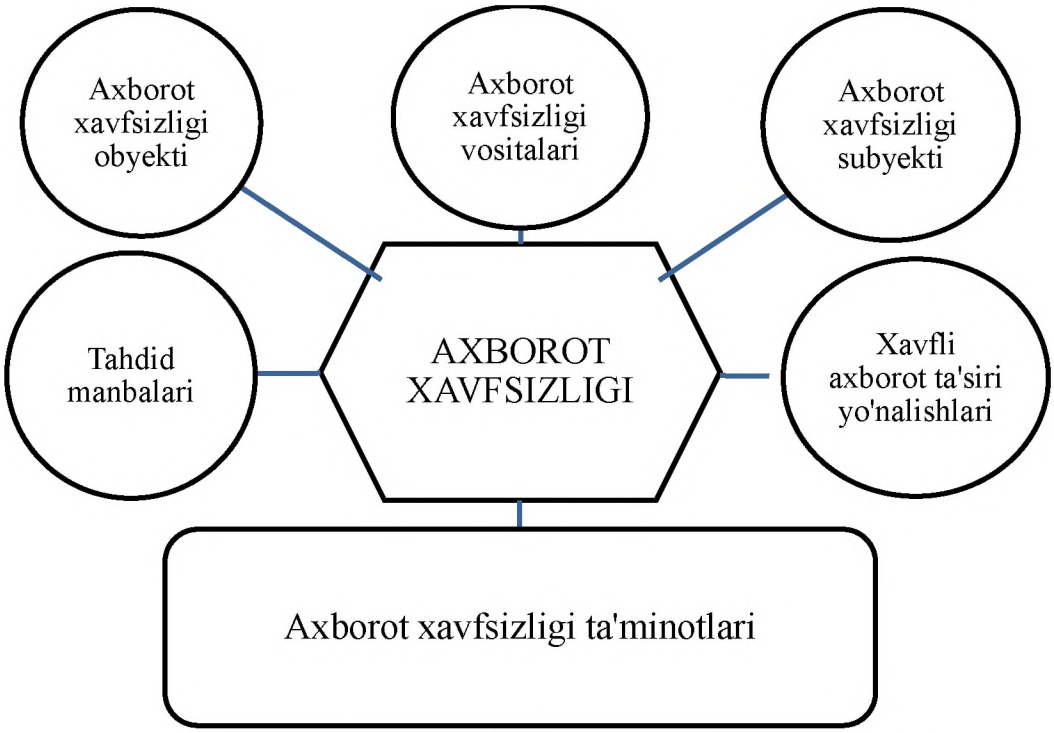
- ma’lumot saqlanayotgan tizimning elektr energiya bilan uzluksiz oziqlanishini ta’minlash tizimini ishlab chiqish;
- resurslarning zaxira nusxasi va dublikatlarini olib borish;
- axborot tizimi ma’lumotlarining dasturiy va texnik himoyasini ta’minlash.

Axborot xavfsizligiga tizimli yondashishda quyidagi tashkil qiluvchilarga alohida e’tibor qaratiladi:

- qonuniy asoslarni ishlab chiqish;
- axborot texnologiyalari xavfsizligini ta’minlovchi organlar (bo‘linmalar) strukturasi va vazifalarini aniqlash;
- tashkiliy-texnik qoida va usullarni (axborot xavfsizligi siyosatini) ishlab chiqish;
- axborot xavfsizligini ta’minlovchi dasturiy texnik usul va vositalarni joriy qilish.

Axborot tizimi subyektlarining axborot almashinuviga bo‘lgan munosabatlari tahlil qilinganda, muhimlik jihatidan axborotdan foydalanish (o‘qish, tanishib chiqish, nusxa ko‘paytirish) asosiy o‘rin tutishi ma’lum bo‘lgan. So‘ngra axborot yaxlitligini ta’minlash va konfidensiallik turadi.

Axborot xavfsizligiga tizimli yondashish uning subyektlari, vositalari, obyektlari, tahdid manbalari, xavfli axborot ta’sirining yo‘nalishi, axborot xavfsizligi ta’minotlarini aniqlashni talab qiladi (2).



2-rasm. Axborot xavfsizligining konseptual modeli

Axborot xavfsizligi obyektlari deb, tahdiddan himoya qilinishi lozim bo‘lgan axborot manbalariga aytiladi. Xavfli ta’sirga uchrashi mumkin bo‘lgan obyektlarga inson psixikasi, ongini ham kiritish mumkin. Bundan kelib chiqadiki, konfidensial axborot manbalariga odamlar, hujjatlar, nashrlar, axborot saqlash va uzatish texnik vositalari, ishlab chiqarish va mehnat faoliyatini ta’minlovchi texnik vositalar kiradi. Shuningdek, mahsulot hamda ishlab chiqarish chiqindilari ham kirishi mumkin.

Axborot xavfsizligi subyektlari sifatida xavfsizlikni ta’minlovchi tarkibiy bo‘linmalar, strukturalarni aytish mumkin.

Axborot xavfsizligini ta’minlovchi vositalar – axborot himoyasini ta’minlash choralarini amalga oshiruvchi boshqaruv tizimlari, aloqa, kompyuter tarmoqlari, axborot o‘g‘riligining oldini oluvchi tashkiliy, texnik, dasturiy vositalar. Axborot xavfsizligi vositalari sifatida apparat-dasturiy vositalar va kriptografik tizimlardan foydalaniladi. Kriptografik tizimlardan alohida apparat yoki dastur ko‘rinishida yoki ularni birgalikda qo‘llab foydalanish mumkin.

Axborotga tahdid deganda, uning konfidensialligi, butunligi, yaxlitligi va undan foydalanish qoidasi buzilishi tushuniladi. Axborot

xavfsizligiga tahdid manbalariga raqiblar, jinoyatchilar, korrupsiyachilar hamda ishga yangi kelgan xodimlar va boshqa buzuvchilar kirishi mumkin.

Konfidensial axborotga tahdidning yana bir ta'rifiga ko'ra, muhofaza qilinayotgan axborot resurslaridan ma'lumot olish bo'yicha amalga oshirilgan yoki amalga oshirilishi mumkin bo'lgan xatti-harakatlar tushuniladi.

Tahdidlar tabiiy, beixtiyor, tasodifan va qasddan qilingan bo'lishi mumkin.

Atayin, qasddan qilinmagan tahdid manbalariga: beixtiyor yo'l qo'yilgan xatoliklar, texnik nosozliklar, tasodifiy faktorlar, tabiiy falokatlar kirishi mumkin.

Qasddan qilingan tahdidlar ongli ravishda, ma'lum maqsadni ko'zlab amalga oshiriladi. Bunda axborot xavfsizligiga tahdid qiluvchi manbalarning ko'zlagan maqsadi quyidagicha bo'lishi mumkin: konfidensial ma'lumotlarni o'g'irlash, axborotni o'zgartirish yoki yo'qotish.

Huquqi bo'lmagan shaxslarning konfidensial axborotni qo'lga kiritishi – ma'lumotlarni axborot manbalari va texnik vositalar orqali chiqib ketishi hamda muhofaza qilinayotgan ma'lumotlarga sanksiyasiz kirish natijasida sodir etilishi mumkin.

Hozirgi kunda Internet tarmoqlari, ommaviy axborot vositalari orqali uyushtirilgan kuchli axborot hujumlari kishilar ongiga ta'sir o'tkazishi mumkinligi sir emas. *Xavfli axborot ta'sirini* ikki turga bo'lish mumkin.

1. Qimmatli ma'lumotni axborot tizimidan chiqib ketishi (yo'qotish) bilan bog'liq. Oqibatda, bunday yo'qotish axborot egasi ish faoliyati samarasining pasayishi yoki raqib tomon ish faoliyati samarasining oshishiga sabab bo'ladi.

Agar bunday xavfli axborot ta'sirining obyekti sifatida insonlarning ongi ko'zda tutiladigan bo'lsa, ularning xavfsizligi bilan senzura organlari, kontrrazvedka va boshqa axborot xavfsizligi subyektlari shug'ullanadi.

Agar axborot manbasi sifatida texnik tizimlar qaraladigan bo'lsa, telefon suhbatlarini eshitish, boshqa kommunikatsiya vositalari signallarini tutib olish kabi texnik razvedka yoki josuslik, kompyuter tarmoqlariga

kirish, ma'lumotlar bazasini buzish haqida so‘z ketadi. Texnik razvedkaga kontrrazvedka organlari hamda kompyuter vositalarining himoyasi bilan shug‘ullanadigan bo‘linma va strukturalar qarshi turadi.

2. Axborot ta'sirining ikkinchi ko‘rinishi soxta ma'lumotlarni axborot tizimiga joylashtirish bilan bog‘liq. Buning oqibatida qaror qabul qilishda xatoga yo‘l qo‘yish turli zararli xatti-harakatlarni yuzaga keltirishi mumkin. Bunday ko‘rinishdagi axborot ta'sirining himoyasini maxsus axborot-texnik bo‘linmalar ta'minlashi lozim. Ular dezinformatsiya tarqalishi oqimini zararsizlantiradilar, omma ongini boshqarishga bo‘lgan xatti-harakatlarning oldini oladilar, kompyuter hujumlari oqibatini yo‘qotadilar.

O‘zbekiston Respublikasi Milliy gvardiyasi bo‘linmalari obyektlarini qo‘riqlashda axborot xavfsizligi uni ta'minlash usullari, axborot xavfsizligi kundalik hayotda, xizmatga oid ma'lumotlarning tarqab ketishiga, raqib yoki dushmanning yolg‘on va zararli ma'lumotlarini tarqalishiga qarshi kurash zaruriyati tarzida tushuniladi.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasi Milliy gvardiyasi qo‘mondonining 2024-yil 6-maydagi “O‘zbekiston Respublikasi Milliy gvardiyasi bo‘linmalari obyektlarini qo‘riqlashning muhandislik va texnik vositalari bilan jihozlash va ulardan foydalanishni tashkillashtirish to‘g‘risida”gi 124-sonli buyrug‘i.

2. Achilov F.B. Qo‘riqlashning videokuzatuv tizimlari. Darslik. – T. HTI, 2019.

3. Владо Демьяновски. ССТВ. Библия охранного телевидения. Пер.с англ .-М.: ООО ИСС, 2002.

4. Магауенов Р.Г. Системы охранной сигнализации: основы теории и принципы построения. Учебное пособие – 2-е изд., перераб и доп. – М: Горячая линия – Телеком, 2008.

5. Movlonkoriyev K., Volxonskiy A. Qo‘riqlash tizimlarning signalizatsiya komplekslari – T., 2008.

6. Raximov B.N., Tadjitdinov G.B..Televidenie va telemexanika asoslari. O‘quv qo‘llanma. – T., 2018.

7. Tolibdjanov T.M., Tadjitdinov G.B. Videokuzatuv tizimlarini obyektlarni qo‘riqlashda qo‘llashning asoslari. O‘quv qo‘llanma – T., 2016.

8. Achilov F.B. Toifalangan obyektlarning kompleks qo‘riqlash tizimi texnik holatini baholash usullari. Monografiya – T., 2023.

9. Галатенко В. А. Основы информационной безопасности. Курс лекций Учебное пособие М: ИНТУИТРУ “Интернет-университет Информационных Технологий”, 2004.

HODISA JOYINI KO‘ZDAN KECHIRISHDA ILG‘OR TEXNOLOGIYALARDAN FOYDALANISHNING INNOVATSION YONDASHUVI

Xamidov G‘.S.
O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti, t.f.n., professor

Hodisa joyini ko‘zdan kechirish, dastlabki va eng muhim tergov harakati sifatida, yangi kriminalistika texnikasini yaratish va qo‘llash sharoitiga, shuningdek, interaktivlik sharoitiga moslashtirilishi lozim. Shu bilan birga, hodisa joyini ko‘zdan kechirishning mohiyati — ya’ni sodir bo‘lgan voqeani qayd etish va barcha holatlarni aniqlash uchun izlarni topish — o‘zgarishga uchramaydi [1].

Ahamiyatli jihati shundaki, zamonaviy texnika hamda axborot va axborot-kommunikatsiya texnologiyalarini [4, 5] qo‘llagan holda tergov harakatlarini amalga oshirishning yangi usullaridan foydalanish zarurligini asoslab berishdan iboratdir. Bu esa jinoyatlarni tergov qilish va fosh etishda zarur ma’lumotlarni sifatli va samarali to‘plash hamda izlarni aniq qayd etish imkonini beradi.

Hozirgi vaqtda hodisa joyini ko‘zdan kechirishning istiqbolli yo‘nalishlaridan biri — tasvir olish qurilmalaridan foydalanishdir. Bunda uchuvchisiz uchish qurilmalarida (dronlar) o‘rnatilgan qurilmalar ham qo‘llaniladi. Ushbu usulning afzalliklari quyidagilardan iborat:

to‘planadigan vizual ma’lumotning to‘liqligini sezilarli darajada oshirish;

ko‘zdan kechirish jarayonini tezkorlik bilan amalga oshirish;

mutaxassis uchun xavfli yoki kirish qiyin bo‘lgan hududlarni tasvirga olish imkoniyati.

Zamonaviy uchuvchisiz uchish qurilmalari yuqori ishonchlilikka, aniqlikka va xavfsizlikka ega. Ular yuqori aniqlikdagi raqamli kameralar, yuqori sezgirlikka ega sun’iy yo‘ldosh navigatsiya tizimlari hamda hududga bog‘lash funksiyalari bilan jihozlangan. Shu imkoniyatlar hodisa joyidagi vaziyatni tez va aniq vizual ma’lumotlar orqali qayd etish imkonini beradi.

Biroq, hozirgi vaqtda olingan tasvirlardan foydalanish asosan hodisa joyidagi vaziyatni tasvirlash va ifodalash bilan cheklanib qolmoqda. Zamonaviy qayd etish vositalari (uchuvchisiz uchish qurilmalari, fotoapparatlar, videokameralar va boshqalar) taqdim etadigan ma’lumotlar — masalan, hududning koordinatalari, obyektlarning o‘lcham xarakteristikalari — ko‘p holatlarda to‘liq ishlatilmay qolmoqda.

An’anaviy fototexnika va uchuvchisiz uchish qurilmalaridan foydalangan holda hodisa joyini ko‘zdan kechirish usuli muhim va ahamiyatli obyektlarni batafsil tasvirga olish maqsadida hodisa joyi ustida aylanib chiqishni nazarda tutadi.

Ushbu usulni kriminalist-mutaxassisning faoliyati xavfli yoki jismoniy jihatdan qiyin bo‘lgan holatlarda qo‘llanishi maqsadga muvofiq hisoblanadi.

Tasvirlar olingach, hodisa joyidagi vaziyatni o‘zgartirishi mumkin bo‘lgan harakatlar amalga oshirilishi mumkin. Masalan:

avariya-qutqaruv ishlari olib borilishi;

transport vositalarini ko‘chirish;

ashyoviy dalillarni tekshirish va olib chiqish va h.k. [2].

An’anaviy suratga olish jarayonida olingan ma’lumotlar, shuningdek uchuvchisiz uchish qurilmalaridan olingan ma’lumotlar 3D-modellar yaratishda qo‘llanilishi mumkin.

Virtual 3D-hudud, undagi obyektlar va hodisalarni ko‘rish imkoniyatiga ega 3D-modellarni yaratish jinoyatni tergov qilish jarayonida muhim va yuqori texnologiyali yo‘nalish hisoblanadi. Bunday modellar

koʻplab jinoyatlarning oldini olish uchun koʻrgazmali qoʻllanma sifatida xizmat qilishi mumkin.

Zamonaviy uch oʻlchamli modellar yaratish dasturiy vositalari ekspert tahlillari, tadqiqotlar va boshqa protsessual harakatlarni amalga oshirishda raqamli qayd etish vositalaridan foydalanish imkoniyatlarini sezilarli darajada kengaytiradi.

Olingan tasvirlar asosida hodisa joyining 3D-modeli yaratiladi va unda ayrim obyektlar zarur darajadagi detallashtirish bilan aks ettiriladi. Bu model istalgan vaqtda va istalgan joyda tahlil qilinishi mumkin, bu esa qoʻshimcha va takroriy koʻriklarni amalga oshirish imkoniyatlarini kengaytiradi hamda protsessual harakatlarning ishonchliligini oshirishga xizmat qiladi.

Zamonaviy dasturiy vositalar yordamida yaratilgan 3D-modellar oʻlchov oʻlchov olish imkoniyatlarini yaratadi, ya'ni ulardan faqat obyektlarning oʻzaro joylashuvini baholashda emas, balki ularning oʻlchamlarini va ular orasidagi masofani aniq oʻlchashda ham foydalanish mumkin [6].

Nazorat masshtabi sifatida metall lentalar, geodezik reykalar kabi obyektlaridan foydalanish oʻtkaziladigan oʻlchovlarning metrologik aniqligini ta'minlaydi. Tavsiflangan ushbu yondashuv hodisa joyi va ekspert obyektlarini qayd etishda yoʻl-transport hodisalarini koʻrikdan oʻtkazish, qurilish-texnik ekspertizalarda, portlash joylarini tekshirishda, texnogen avariya va falokatlarni oʻrganishda samarali qoʻllanilishi mumkin.

Soʻnggi yillarda soni tobora koʻpayib borayotgan holatli ekspertizalarda 3D-modellardan foydalanish juda istiqbolli yoʻnalish hisoblanadi.

Hodisa joyining aniq tasvirini olishning alternativ usuli sifatida lazerli 3D-skanerlash hisoblanadi. Bu usulning asosiy ustunligi — yaratilgan modellarning juda yuqori aniqligidadir.

Biroq mazkur usulda ayrim kamchiliklar ham mavjud boʻlib, ular hodisa joyini koʻrikdan oʻtkazishda lazerli skanerlardan foydalanishni qiyinlashtiradi yoki umuman imkonsiz qiladi. Asosiy kamchiliklardan biri

— skanerning ish vaqtining uzunligi va ma'lumotlarni asosan yer yuzasidan yoki kichik ko'tarilishlardan olish imkoniyati cheklanganligidir. Shuningdek, uskunaning yuqori narxi ham katta to'siq hisoblanadi.

Bundan tashqari, olingan ma'lumotlar aniqligi ko'p holatlarda ekspertlik vazifalarini hal qilish uchun ortiqcha bo'lishi mumkin.

Yuqoridagilardan kelib chiqib, xulosa qilish mumkinki, uchuvchisiz uchish qurilmalari (masalan, kvadrokopter), an'anaviy raqamli fotoapparatdan iborat fotokomplekt va maxsus dasturiy ta'minotdan foydalangan holda hodisa joyi va ekspert obyektlarining vizual va o'lchov xarakteristikalarini olish uchun yuqori samarador kompleks yaratish mumkin.

3D-modellashtirish texnologiyasi yordamida jinoyat manzarasini qayta tiklash hamda tergov-tezkor guruhi xodimlari oldida turgan ko'plab vazifalarni hal etish imkoniyati paydo bo'ladi. Bunday dasturiy ta'minotdan mohirona foydalanish jinoyat joyini ko'rikdan o'tkazish jarayonini ham real, ham virtual ko'rinishda ancha yengillashtirishi mumkin.

Hodisa joyini sifatli ko'rikdan o'tkazish uchun uning aniq chegaralarini belgilash, diqqat qaratilishi lozim bo'lgan joylar va obyektlarni aniqlash zarur. Har doim ham ayrim tergovchi, ekspert yoki mutaxassisning tajribasi bu vazifani yetarli darajada bajarishga imkon bermaydi. Shuningdek, turli holatlar sababli zarur mutaxassisning ko'rik jarayonida shaxsan ishtirok etishi hamisha ham mumkin bo'lavermaydi.

Ana shunday vaziyatda hodisa joyini ko'rikdan o'tkazishning an'anaviy usuliga alternativa sifatida *interaktiv ko'rik* tushunchasi paydo bo'ladi. Bu usul virtual ishtirokchilarni jalb qilgan holda, ularning tergov harakatida real vaqt rejimida ishtirok etish imkonini yaratadi.

Yangi texnologiyalar va interaktiv usullar qo'llanilishi bilan hodisa joyini ko'rikdan o'tkazishning shakli o'zgaradi, uning taktikasi qayta ko'rib chiqiladi, jarayonda yangi ishtirokchilar paydo bo'ladi. Ushbu mezonlar an'anaviy ko'rik bilan interaktiv ko'rikni farqlash imkonini beradi.

Klassik kriminalistika adabiyotida ***interaktiv hodisa joyini ko‘rikdan o‘tkazish*** tushunchasi yoritilmagan. Buning sababi shundaki, bunday ko‘rikni amalga oshirish imkoniyati faqat yaqin yillarda, yangi turdagi internet-texnologiyalar rivojlanishi bilan paydo bo‘ldi.

Interaktiv ko‘rikni amalga oshirish taktikasini belgilash masalalari hozirda qonunchilikda mustahkamlanmagan bo‘lib, ular faqat soha mutaxassislari orasidagi muhokamalardagina mavjud [3].

Shuning uchun an’anaviy ko‘rik va interaktiv ko‘rikni taqqoslash orqali yangi turdagi tergov harakatining ijobiy va salbiy tomonlarini aniqlash, shuningdek, uni amalga oshirishning dastlabki taktikasini belgilash zarur.

Interaktiv ko‘rikning asosiy belgilari:

Albatta onlayn muloqotni ta’minlaydigan texnik vositalardan foydalaniladi.

Jarayonda voqeani sifatli aks ettirish uchun zarur bilimga ega bo‘lgan ***virtual ishtirokchi*** qatnashadi.

Tergov harakatida masofaviy ishtirok etish — kelgusida tergov jarayonida ishtirok etishning yangi shakli sifatida rivojlanadi.

Interaktiv hodisa joyini ko‘rikdan o‘tkazishni qo‘llash zarur bo‘lgan holatlar

Interaktiv ko‘rikdan foydalanish ayrim holatlarda ayniqsa muhim ahamiyatga ega bo‘ladi. Bu usul an’anaviy ko‘rikni samarali ravishda to‘ldirib, tergov jarayonida aniqlik va tezkorlikni ta’minlaydi. Quyida uni qo‘llash zarur bo‘lgan asosiy vaziyatlar keltirilgan:

Katta jamoatchilik rezonansiga ega jinoyatlar:

tergov-operativ guruhi ishida joyda hozir bo‘lishi zarur bo‘lgan, lekin hodisa joyidan uzoqda joylashgan mutaxassislarning ishtirokini ta’minlash uchun;

ularning ko‘rikda shaxsan ishtirok etishi qisqa muddatda imkonsiz bo‘lgan holatlarda;

shuningdek, ekspertizalar va tadqiqotlar jarayonida ziddiyatlarni bartaraf etish maqsadida.

Jabrlanuvchining masofadan ishtirok etishi zarur bo‘lgan holatlar

agar jabrlanuvchi jinoyatdan keyin shoshilinch tarzda shifoxonaga yoki tibbiy punktga jo‘natilgan bo‘lsa, biroq hushyor holatda bo‘lsa;

jabrlanuvchi “onlayn” rejimda hodisa joyida jinoyat quroli yoki jinoyatchi izlari bo‘lishi mumkin bo‘lgan joylarni ko‘rsatib o‘tishi mumkin.

Yosh mutaxassislarni masofaviy maslahat bilan qo‘llab-quvvatlash:

yosh tergovchilar, tezkor vakolatli shaxslar va ekspertlarga rahbariyat tomonidan masofadan maslahat berish orqali ularni yo‘naltirish uchun;.

Nomuvofiq ob-havo sharoiti yoki uzoq masofalar sababli muammolar:

agar tergov-operativ guruhi a’zolaridan biri yomon ob-havo yoki hodisa joyi bilan orasidagi uzoq masofa sababli ko‘rikda shaxsan ishtirok eta olmasa;

xususan, aholi bir-biridan uzoqda joylashgan shimoliy hududlarda bu usul ayniqsa dolzarbdir.

Interaktiv ko‘rikning afzalliklari.

Interaktiv hodisa joyini ko‘rikdan o‘tkazish quyidagilarni ta’minlaydi:

Tergov harakatining sifatini oshirish,

Har bir ishtirokchining faolligini va samaradorligini kuchaytirish,

Yangi texnik va texnologiyalarni jamiyat hayotiga joriy etish jarayonida ulardan jinoyatlarni ochish va tergov qilishda samarali foydalanish.

Bu usul rivojlanib borgan sari jinoyatlarni ochishda va ularni to‘liq tergov qilishda tobora muhim va dolzarb ahamiyat kasb etadi.

Foydalanilgan adabiyotlar:

1. Аверянова Т. В., Белкин Р. С., Корухов Й. Г., Россинская Е. Р. Криминалистика: учебник // 3-е изд., перераб. и доп. М., 2010.

2. Дашко Л. В., Синюк В. Д., Пенков В. В. Возможности исползования беспилотних летателних аппаратов для фиксации обста-новки на месте пожара // Научний портал МВД России. 2017. № 4 (40).

3. Королева Д. В. Осмотр места происшествия с аутсенсуалними участниками следственного действия как новейшая криминалистическая технология современного периода // Законност и правопорядок в современном обществе. 2014. № 21.

4. Мартинов А. Н., Краветс Е. Г., Шувалов Н. В. Организатсионно-тактический модул дистанционних следственних действий // Труди Академии управления МВД России. 2017. № 4 (44).

5. Познанский Й. Н. Информационние технологии как средство повишения эффективности деятелности руководителей органов предварителного следствия в цистеме МВД России // Труди Академии управления МВД России. 2017. № 4 (44).

6. Прокофева Е. В., Баринова О. А., Прокофева О. Й. Применение метода 3Д-моделирования при осмотре места совершения кражи // Юридическая наука и правоохранителная практика. 2016. № 1 (35).

О РОЛИ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ИНЖЕНЕРНО-САПЕРНЫХ ПОДРАЗДЕЛЕНИЙ

Шайманов А.Т.

Д.ф.в.н. (PhD), подполковник, Университет военной безопасности и обороны Республики Узбекистан, начальник отделения планирования учебного процесса (магистратура)

Известно, что XXI век характеризуется широким применением средств информационно-коммуникационных технологий во всех сферах жизнедеятельности. Особое место в данном случае выделяется цифровым технологиям.

В данном контексте, бурное развитие средств цифровых технологий в области обучения кадров обеспечения общественной безопасности и выполнении специфических задач, способствуют эффективной подготовке высококвалифицированных специалистов.

Более того, доступность применения средств цифровых технологий при обучении военных кадров позволяет совершенствовать процесс их подготовки.

На современном этапе задачи качественной подготовки военных специалистов становятся особенно актуальными в связи с расширением спектра угроз общественной и национальной безопасности, в том числе повышением уровня информационной угрозы и необходимостью подготовки квалифицированных военных специалистов в области подготовки личного состава [1].

В настоящее время во всем мире, а также в высших военных образовательных учреждениях нашей республики имеется множество учебных тренажеров и симуляторов, которые охватывают широкий спектр задач и вопросов по обучению кадров общественной безопасности.

Одним из актуальных направлений в военной сфере, в части касающейся подготовке военных специалистов, является подготовка кадров в области инженерно-саперного дела.

С учетом изложенного возникают задачи расширения границ применения информационных и цифровых технологий в военном образовании, которые состоят в том, чтобы расширить и упростить доступ обучающихся к получению необходимых знаний, умений и получению первоначального профессионального опыта, что создаёт реальные предпосылки для повышения качества обучения и неизбежно приводит к изменению характера образовательной деятельности, появлению современных инструментов и технологий, позволяющих педагогу применять активные методы обучения, а так же строить диалог с обучающимися.

В то же время функционирование образовательного процесса с использованием информационных и цифровых систем требует соответствующей организации, создания обучающих электронных и моделирующих систем с содержанием вопросов инженерно-саперного дела.

Применение обучающей системы с использованием средств цифровых технологий даёт возможность уменьшить время на поиск учебного материала, даёт возможность расширения объема получаемой обучаемыми информации за счёт следующих факторов [1, 2]:

1. Обучающая система может включать основные сведения по произвольной, на первый взгляд, предметной области. Но, как показывает многовековая история вооруженных конфликтов, на войне информация любого рода лишней не бывает;

2. Средства вычислительной техники и используемая информация даёт возможность применять одну и ту же обучающую систему для всей категории обучающихся;

3. Использование компьютерной графики, анимации, видео, звука, других мультимедийных компонентов делает изучаемый материал максимально наглядным, интересным, понятным и запоминаемым. Это особенно необходимо в тех случаях, когда обучаемый должен усвоить большое количество информации, содержащей инструкции, технологические карты и схемы, нормативные документы и др.

Кроме того, информация в печатном варианте не всегда доступна для обучающихся, что неизбежно побуждает преподавателей к разнообразию работы с источниками информации в электронной форме. Возникает необходимость создания электронных учебников и обучающих программ, сочетающих в себе, как свойства обычного учебника, так и свойства справочника;

4. Информационные и цифровые технологии позволяют моделировать реальные условия оперативно-боевой и инженерной обстановки, дают возможность осуществлять тренировку не только в принятии необходимых управленческих решений, но и осуществлять профессиональную подготовку путем выполнения виртуальных задач по установке минно-взрывных устройств, разминированию взрывоопасных предметов, проведению инженерной разведки и т.д.

Уместно отметить, что развитие информационных и цифровых технологий позволяют массово и широко применять компьютерные средства обучения, с помощью которых доступно решать следующие немаловажные задачи [3]:

1. Обеспечить каждого обучающегося необходимым объёмом работы с изучаемым материалом, а также последовательность, состоящую в чередовании изучения теории, разбора примеров, отработки первоначальных профессиональных навыков, решения типовых компетентностно-ориентированных заданий;

2. Обеспечить возможность самоконтроля качества приобретённых знаний и умений, что в свою очередь необходимо для проведения практических занятий, особенно занятий с отработкой вопросов минно-подрывного дела;

3. Сократить время, необходимое для изучения материала. Необходимость внедрения новых информационных и цифровых технологий в образование вызывается и тем, что объем учебной информации постоянно возрастает, количество же учебных часов, отводимых на ее изучение, остается постоянным, а нередко и уменьшается. Современные коммуникационные технологии позволяют сделать взаимодействие руководителя занятия и обучающегося более активным, но это требует от преподавателя специальных дополнительных усилий.

Уместно отметить тот факт, что достижение в выполнении вышеперечисленных задач будет зависеть также от уровня освоения профессорско-преподавательским составом информационных и цифровых технологий, а также грамотному и эффективному их применению в ходе учебного процесса.

Таким образом, с одной стороны, в условиях развития современного мира информационным и цифровым технологиям в области подготовки военных кадров выделяется значительная роль, с другой стороны их применение требует высокий уровень профессионального и методического мастерства. Однако,

необходимо понимать, что применение данных технологий позволяют значительно повысить эффективность учебного процесса.

Использованной литературы:

1. Использование информационных компьютерных технологий в учебном процессе и проблемы его методического обеспечения // Интернет-журнал «Эйдос». – 2006.

2. Митяева А. М. Развитие индивидуальных стилей учебной деятельности студентов. Орел: Картуш, 2005. – 12с.

3. Коровин В. М. Технология профессионально-ориентированного обучения курсантов в высшем военно-учебном заведении / – Воронеж: МО РФ, 2001. – 271с.

KIBERXAVFSIZLIK: QUROLLI KUCHLARDA AXBOROT HIMOYASINI TA'MINLASH MUAMMOLARI VA CHORA-TADBIRLARI

Kamilov M.A.
Jamoat xavfsziligi universiteti Axborot texnologiyalari kafedrasi katta o'qituvchisi

Raqamli transformatsiya jarayonlari mudofaa sohasini tubdan o'zgartirmoqda: qo'mondonlik va boshqaruv (C2) tizimlari, aloqa va navigatsiya, razvedka-kuzatuv-ma'lumot yig'ish (ISR), logistik ta'minot hamda jangovar tayyorgarlik tobora ko'proq tarmoqlashtirilgan axborot-kommunikatsiya infratuzilmasiga tayanadi. Kiberfazodagi ustunlik esa an'anaviy qurolli to'qnashuvlardagi tashabbusga teng yoki undan ham muhim omilga aylanmoqda. Shunday sharoitda Qurolli Kuchlarda axborot himoyasini ta'minlash milliy xavfsizlikning ajralmas komponenti bo'lib, strategik barqarorlikni belgilovchi omil sifatida ko'riladi.

Hozirgi kunda tahdidlar spektri kengaymoqda: davlat va nodavlat subyektlar tomonidan uyushtiriladigan maqsadli kiberhujumlar (APT), xizmatdan mahrum etish (DDoS), ta'minot zanjiri orqali kirish (supply-chain), sanoat boshqaruv tizimlari (ICS/SCADA)ga aralashuv, xodimlar orqali ichki xavf (insider threat), shuningdek dezinformatsiya va

psixo-axboriy operatsiyalar bilan yo‘g‘rilgan gibrid urush elementlari. Harbiy segmentning sun’iy intellekt, dron va robototexnika, bulutli hisoblash, kvantga tayyor kriptografiya kabi texnologiyalarni joriy etishi yangi imkoniyatlar bilan birga yangi zaifliklarni ham keltirib chiqarmoqda.

Muammo shundaki, ko‘plab harbiy axborot tizimlari eskirgan komponentlarga, mozaik arxitekturaga va fragmentar me’yoriy-huquqiy bazaga ega; real vaqt monitoringi va hodisalarga javob berish (SOC/CSIRT) imkoniyatlari yetarli darajada integratsiyalashmagan; hamkor idoralar va pudratchilar bilan ma’lumot almashinuvida xavfsizlik siyosatlari bir xil emas. Natijada kichik ko‘lamli ekspluatatsiya ham zanjirsimon ta’sir bilan qo‘mondonlikni falaj qilishi, logistika uzilishlariga va operativ qaror qabul qilish sifatining pasayishiga olib kelishi mumkin.

Maqolaning maqsadi — Qurolli Kuchlarda kiberxavfsizlikni ta’minlashning hozirgi holatini tizimli tahlil qilish, asosiy muammolarni tipologik guruhlarga ajratish va ularni bartaraf etuvchi kompleks texnik, tashkiliy va huquqiy chora-tadbirlar majmuasini taklif etishdir. Ushbu maqsadga erishish uchun quyidagi ilmiy savollar qo‘yiladi: (1) harbiy axborot tizimlarining asosiy zaiflik sinflari nimalardan iborat? (2) tahdidlar modeli gibrid urush sharoitida qanday yangilanadi? (3) resurs cheklovlari sharoitida xavfni kamaytirishning eng yuqori samara beruvchi mexanizmlari qaysilar? (4) ichki tahdidlarni boshqarish va muvofiqlikni ta’minlash uchun qanday boshqaruv tizimi zarur?

Tadqiqot metodologiyasi sifatida normativ-huquqiy tahlil, xavf va yetkazilishi mumkin bo‘lgan zarar baholash (risk-impact assessment), arxitektura va jarayon auditi, ilg‘or amaliyotlar bilan taqqoslash (benchmarking), shuningdek ochiq manbalarda keng yoritilgan global voqealar (masalan, harbiy-sanoat infratuzilmasiga yo‘naltirilgan zararli dastur kampaniyalari, logistika tarmoqlariga ta’sir ko‘rsatgan kiberoperatsiyalar) bo‘yicha holat tadqiqi (case study) qo‘llanadi.

Ilmiy yangilik maqolaning Qurolli Kuchlar kontekstida uch qatlamli himoya konsepsiyasini (texnik-arxitektura qatlamida «zero-trust» tamoyili va segmentatsiya; tashkiliy qatlamda SOC-CSIRT-CTI uchligi; huquqiy qatlamda mas’uliyat va muvofiqlikni aniqlovchi standartlashtirilgan

jarayonlar) bir butun «mudofaa-in-depth» modeli ko‘rinishida taklif etishida namoyon bo‘ladi. Amaliy ahamiyati esa bosqichma-bosqich joriy etish xaritasi, metrikalar tizimi va kadrlar siyosati bo‘yicha aniq tavsiyalar bilan ta’minlanadi.

Tadqiqot doirasi Qurolli Kuchlarning boshqaruv, aloqa, razvedka, logistika va ta’lim segmentlarini qamrab oladi; yopiq va maxfiy ma’lumotlar ishlatilmaydi, xulosalar ochiq standartlar va umumlashtirilgan amaliy tajribalarga tayangan holda shakllantiriladi. Cheklovlar sifatida ayrim texnologik yechimlarning importga qaramligi va budjet-resurs cheklanishi ko‘rsatiladi.

Maqola quyidagicha tuzilgan: muammolar panoramasi va ularning tipologiyasi, so‘ng yechimlar majmuasi (texnik, tashkiliy, huquqiy), keyin esa joriy etish yo‘l xaritasi va kutilayotgan natijalar, yakunda xulosalar va tavsiyalar.

Qurolli Kuchlarda kiberxavfsizlikning dolzarbligi

Raqamli texnologiyalar harbiy boshqaruvning barcha qatlamlariga chuqur singib bormoqda: qo‘mondonlik va boshqaruv (C2), aloqa (C3), razvedka-kuzatuv-ma’lumot yig‘ish (ISR), otish boshqaruvi, logistika va tayyorgarlik jarayonlari tobora ko‘proq tarmoqlashtirilgan axborot-kommunikatsiya tizimlariga tayanadi. Shuning uchun kiberfazoda ustunlikka erishish, tarmoq va ma’lumotlarning yaxlitligi, maxfiyligi hamda mavjudligini (CIA) saqlash operativ qarorlar sifatiga bevosita ta’sir ko‘rsatadi va jangovar muvaffaqiyat shartlaridan biri sifatida namoyon bo‘ladi.

Dolzarblikni kuchaytiruvchi omillar:

1. **Gibrid urush va kiber-kinetik integratsiya.** Kiberoperatsiyalar endi alohida emas, balki radioelektron kurash, psixo-axboriy operatsiyalar va an’anaviy jangovar harakatlar bilan uyg‘un holda qo‘llanmoqda. Kiber zarba qo‘mondonlik zanjirini falaj qilib, qaror qabul qilish siklini (OODA) buzadi.

2. **C4ISR ga chuqur tayanish.** Sensor-effektor zanjiri, dron-rojlar, sun’iy yo‘ldosh aloqa va navigatsiya (GNSS)ga qaramlik

hujum sirtini kengaytiradi. Jamlagich tarmoqlarda bitta zaiflik butun operatsion rasmni buzishi mumkin.

3. **Logistikaning raqamlashtirilishi.** ERP/MES tizimlari, harbiy ta'minotning raqamli kuzatuvi (asset tracking) va yo'llash rejalari kiberhujumlar nishoni bo'lib, munosib himoya bo'lmasa, qo'shinlarning uzluksiz ta'minotini izdan chiqaradi.

4. **OT/ICS (sanoat boshqaruv tizimlari)ga bog'liqlik.** Harbiy bazalar, aerodromlar, yoqilg'i-energetika, suv-issiqlik ta'minoti, port va temiryo'l tugunlari SCADA orqali boshqariladi. Bu tizimlar tarixan IT xavfsizligi talablari bilan loyihalanmagan.

5. **Ichki tahdidlar va inson omili.** Maxfiy ma'lumotlarga kirish huquqi, spearfishing, parol gigiyenasi pastligi, BYOD va masofaviy ish amaliyoti xavfni oshiradi.

6. **Ta'minot zanjiri xatarlarining ortishi.** Pudratchilar, integratorlar va uchinchi tomon xizmatlariga qaramlik zararli kodlarning «orqa eshik» orqali kirishini yengillashtiradi.

7. **Yangi texnologiyalar va 5G/edge muhit.** Sun'iy intellekt, avtomatlashtirilgan boshqaruv, 5G va chekka hisoblash (edge) operativ ustunlik beradi, biroq avtorizatsiya va segmentatsiya to'g'ri qurilmasa, zaifliklar ham ko'payadi.

8. **Kosmik va elektromagnit muhitning o'zaro bog'liqligi.** GNSS spoofing/jamming, sun'iy yo'ldosh aloqasiga hujumlar va radioelektron qarshi choralar kiber va aloqa xavfsizligini bir vaqtda taqozo etadi.

Missiyaga ta'sir ssenariylari:

- **Situatsion rasmni buzish:** sensor ma'lumotlarini soxtalashtirish yoki kechiktirish natijasida noto'g'ri nishon tanlash.
- **Qo'mondonlik aloqasini uzish:** DDoS yoki marshrutlash manipulyatsiyasi sababli C2 uzilishi va bo'linmalar o'rtasida nomuvofiqlik.
- **Logistika falaji:** ombor/transport ERP tizimlariga zararli kod (ransomware/wiper) tushishi natijasida ta'minot uzilishi.

- **Kadrlar va safarbarlik tizimlariga ta’sir:** shaxsiy ma’lumotlar sizishi, ro‘yxatlar o‘zgartirilishi orqali ijtimoiy beqarorlik va boshqaruvga ishonchsizlikni kuchaytirish.
- **Ta’minot zanjiri buzilishi:** yangilanish paketlari orqali orqa eshik joriy etilishi va butun tarmoqqa «pastdan-yuqoriga» hujum.

Operativ ko‘rsatkichlar va boshqaruv metrikalari: dolzarblikni boshqarish uchun MTTD/MTTR (aniqlash va tiklash o‘rtacha vaqti), zaifliklarni yopiqlik vaqti (patch latency), segmentatsiya indeksi, foydalanuvchi xatti-harakatlari ko‘rsatkichlari (phishing click-rate), xizmatlarning mavjudlik darajasi (SLA) kabi metrikalar qo‘llanadi. Bu metrikalar resurslarni ustuvorlashtirish va riskni kamaytirish samarasini o‘lchashga yordam beradi.

Hamkorlik va interoperabellik zarurati: ittifoqchi va hamkor tuzilmalar bilan qo‘shma operatsiyalar kiberxavfsizlik siyosatlari, tasniflash darajalari va texnik standartlar bo‘yicha muvofiqlikni talab etadi. Aks holda, eng kuchli bo‘g‘in ham eng zaif tizim darajasiga tushib qoladi.

Kiberxavfsizlik Qurolli Kuchlar uchun yordamchi emas, balki jangovar imkoniyatlarni ko‘paytiruvchi va strategik barqarorlikni ta’minlovchi asosiy yo‘nalishdir. Dolzarblikning markazida missiyaga yo‘naltirilgan yondashuv, qatlamli himoya, real vaqt monitoringi va inson omilini boshqarish turadi. Shuning uchun siyosiy-strategik rejalashtirishda kiberxavfsizlikka ajratmalarni oshirish, doktrina va standartlarni yangilash, kadrlar tayyorlash hamda ta’minot zanjiri ustidan nazoratni kuchaytirish zarur.

Asosiy muammolar

Qurolli Kuchlarda kiberxavfsizlikni ta’minlashda duch kelinayotgan muammolar murakkab va ko‘p qatlamli bo‘lib, ularni quyidagi tipologik guruhlarga ajratish mumkin:

1. **Texnologik infratuzilmaning eskirishi va fragmentatsiyasi.** Ko‘plab harbiy axborot tizimlari eski apparat va dasturiy ta’minotga asoslangan. Yamoqlash (patch management) jarayoni muntazam emas, segmentatsiya va izolyatsiya mexanizmlari yetarli darajada yo‘lga

qo‘yilmagan. Bu esa ekspluatatsiya qilish oson bo‘lgan zaifliklarni ochiq qoldiradi.

2. **Zaif integratsiya va arxitektura mozaikligi.** Boshqaruv, aloqa va logistika tizimlari ko‘pincha turli davr va ishlab chiqaruvchilarga tegishli. Standartlarning bir xil emasligi interoperabellik muammolarini keltirib chiqaradi, natijada kiberhujumlarni aniqlash va bartaraf etish murakkablashadi.

3. **Malakali kadrlar yetishmovchiligi.** Yuqori darajadagi kiberxavfsizlik mutaxassislari soni cheklangan, mavjud kadrlar ko‘pincha umumiy IT bilimlariga ega, ammo harbiy kiberoperatsiyalar uchun zarur bo‘lgan chuqur tahliliy ko‘nikmalardan mahrum. Doimiy trening va sertifikatsiya tizimining sustligi muammoni kuchaytiradi.

4. **Ichki tahdidlar va inson omili.** Parol gigiyenasining pastligi, phishing xabarlariga berilish, maxfiy ma’lumotlarni himoya qilish madaniyatining sustligi, shuningdek qasddan xiyonat holatlari eng jiddiy xavf manbalaridan biri hisoblanadi. Statistik ma’lumotlarga ko‘ra, ko‘plab kiberinsidentlar bevosita xodimlarning xato yoki qasddan qilgan harakatlari natijasida yuz beradi.

5. **Axborot oqimining hajmi va monitoring cheklovlari.** Sensorlar, dronlar, razvedka vositalari va aloqa tarmoqlari juda katta hajmdagi ma’lumotlarni ishlab chiqaradi. Lekin real vaqt rejimida ularni tahlil qilish, korrelyatsiya qilish va anomaliyalarni aniqlash imkoniyatlari yetarli darajada rivojlanmagan.

6. **Huquqiy-me’yoriy bo‘shliqlar.** Harbiy kiberxavfsizlik bo‘yicha kompleks normativ-huquqiy baza to‘liq shakllanmagan. Masalan, kiberhujumlarni milliy xavfsizlikka qarshi jinoyat sifatida aniq tasniflovchi me’yorlarning yo‘qligi, pudratchilar bilan ishlashda huquqiy mas’uliyatning noaniqligi muammo tug‘diradi.

7. **Ta’minot zanjiri xatarlarining ortishi.** Qurolli Kuchlarda ishlatiladigan ko‘plab komponentlar import qilinadi. Uchinchi tomon ishlab chiqaruvchilar va integratorlar tomonidan zararli kod yoki orqa eshiklar joylashtirilishi ehtimoli yuqori. Bu holat ishonchlilikni keskin kamaytiradi.

8. **Sanoat boshqaruv tizimlarining (ICS/SCADA) zaifligi.** Harbiy bazalar, aerodromlar, portlar va logistika tugunlari boshqaruvida qo‘llaniladigan sanoat tizimlari ko‘pincha IT xavfsizlik tamoyillariga moslashtirilmagan. Ularning himoya darajasi pastligi sababli ular strategik zaif nuqtalarga aylanadi.

9. **Xalqaro hamkorlikdagi muvofiqlik yetishmasligi.** Qo‘shma operatsiyalar vaqtida turli davlatlarning kiberxavfsizlik standartlari va siyosatlari bir-biriga mos kelmasligi himoya samaradorligini pasaytiradi. Bu esa ittifoqchi kuchlarning eng zaif bo‘g‘in darajasida ishlashiga olib keladi.

Qurolli Kuchlarda kiberxavfsizlikni ta’minlash nafaqat texnik vazifa, balki strategik boshqaruv, tashkiliy mas’uliyat va huquqiy tartibga solish majmuasini o‘z ichiga oladi. Tadqiqot shuni ko‘rsatadiki, mavjud muammolar uch asosiy blokda jamlangan: (1) texnologik infratuzilmaning eskirishi va zaifligi; (2) kadrlar salohiyati va tashkiliy mexanizmlarning yetarli darajada integratsiyalanmagani; (3) normativ-huquqiy bazadagi bo‘shliqlar va muvofiqlikning pastligi. Bu omillar birgalikda harbiy axborot tizimlarini global va mintaqaviy kiberxavflar oldida himoyasiz qoldirishi mumkin.

Shu bilan birga, zamonaviy tajriba shuni ko‘rsatmoqdaki, qatlamli himoya (defence-in-depth) modeli, «zero-trust» arxitekturasi, SOC/CSIRT/CTI kabi operativ markazlarning uzviy ishlashi, kadrlar tayyorlash siyosatini modernizatsiya qilish va huquqiy tartibotni mustahkamlash Qurolli Kuchlar uchun samarali yechim bo‘la oladi. Xalqaro hamkorlik va qo‘shma mashg‘ulotlar esa tajriba almashish va real tahdidlarga birgalikda javob qaytarish imkonini beradi.

Ilmiy natijalar asosida quyidagi amaliy tavsiyalar beriladi:

- harbiy boshqaruv tizimlarida yagona kiberxavfsizlik siyosatini ishlab chiqish va qat’iy joriy etish;
- real vaqt monitoringi va insidentlarga tezkor javob berishni ta’minlovchi markazlashgan tarmoqni yaratish;
- axborot oqimlarini sun’iy intellekt asosida boshqarish va xodimlar uchun doimiy xavfsizlik treninglarini yo‘lga qo‘yish;

- milliy kriptografik standartlar va dasturiy mahsulotlarni keng qo‘llash;
- qonunchilik bazasini takomillashtirish va kiberhujumlarni milliy xavfsizlikka qarshi jinoyat sifatida huquqiy baholash.

Shunday qilib, Qurolli Kuchlarda kiberxavfsizlikni mustahkamlash kompleks yondashuvni talab etadi. Bu nafaqat texnik barqarorlikni, balki milliy mudofaa tizimining uzluksiz ishlashini, strategik qarorlarning ishonchliligini va davlat suverenitetining mustahkamligini kafolatlaydi.

Foydalanilgan adabiyotlar:

1. Axmedov SH. «Kiberxavfsizlik va milliy xavfsizlik muammolari». Toshkent: Akademnashr, 2021.
2. Clarke R., Knake R. «Cyber War: The Next Threat to National Security and What to Do About It». HarperCollins, 2010.
3. Nurmatov O. «Harbiy sohada axborot xavfsizligini ta’minlash masalalari». O‘zbekiston Mudofaa Vazirligi ilmiy jurnali, №3, 2022.
4. Nye J. «The Future of Power». PublicAffairs, 2011.
5. O‘zbekiston Respublikasi Prezidentining “Kiberxavfsizlikni ta’minlash tizimini takomillashtirish chora-tadbirlari to‘g‘risida”gi qarori, 2022.
6. Singer P.W., Friedman A. «Cybersecurity and Cyberwar: What Everyone Needs to Know». Oxford University Press, 2014.
7. Zetter K. «Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon». Crown, 2014.
8. Begmatov A., Xidirova D. «Informatsionnaya bezopasnost i yeyo pravovoye regulirovaniye v Respublike Uzbekistan». Toshkent: Yuristlar nashriyoti, 2020.
9. Rid T. «Cyber War Will Not Take Place». Oxford University Press, 2013.
10. Kasimov F. «Milliy xavfsizlik va axborot siyosati». Toshkent: Ma’naviyat, 2019.
11. Cavelty M. «Cybersecurity and Threat Politics: US Efforts to Secure the Information Age». Routledge, 2007.

СЕТЕЦЕНТРИЧЕСКИЕ ВОЙНЫ: РОЛЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ В УПРАВЛЕНИИ БОЕВЫМИ ДЕЙСТВИЯМИ

Хатамов Б.Б.
Университет общественной безопасности Республики Узбекистан
Заместитель начальника кафедры, д.ф.т.н. (PhD)

В XXI веке цифровизация охватила практически все сферы деятельности человека, включая военную область. Одним из наиболее перспективных направлений в военном строительстве стала концепция сетецентрических войн (Network-Centric Warfare, NCW), впервые сформулированная в США в конце 1990-х годов [1]. Её сущность заключается в объединении разведывательных систем, средств связи, вооружений, командных пунктов и солдат в единую сеть, что обеспечивает более высокую скорость передачи информации и принятия решений. Впервые термин *«сетецентрическая война»* был введён в США в конце 1990-х годов (Alberts, Garstka, Stein, 1999), и с тех пор стал основой военной доктрины ведущих держав.

В 1991 году в операции «Буря в пустыне» США впервые использовали элементы сетево-центрического управления, когда спутниковая разведка, GPS-навигация и системы связи позволили поддерживать высокий уровень ситуационной осведомлённости на всём театре военных действий. Применение систем C4ISR в Ираке (2003 год) обеспечило координацию действий сухопутных, авиационных и морских сил. Интеграция разведданных в режиме реального времени позволила значительно ускорить захват стратегических объектов. В миссиях в Афганистане активно применялись БПЛА, сенсорные сети и системы анализа данных, что позволяло прогнозировать передвижение противника и минимизировать риски для войск коалиции.

Концепция сетецентрических войн (NCW) – это современный военный подход, основанный на использовании цифровых технологий, позволяющих объединять все элементы вооружённых

сил в единую информационно-коммуникационную сеть [1]. Её суть заключается в том, что «информация становится главным ресурсом войны». Если в традиционных войнах решающим фактором были численность армии и огневая мощь, то в сетецентрической парадигме определяющим становится скорость получения, обработки и передачи данных.

Основные положения концепции, следующие:

- Единое информационное пространство. Все подразделения армии – от солдат и техники до командных пунктов и разведывательных систем – объединяются в цифровую сеть;

- Ситуационная осведомлённость. Командование и бойцы в реальном времени получают данные о положении войск, ресурсах и действиях противника;

- Сокращение цикла «обнаружение – решение – действие». Чем быстрее информация превращается в решение и действие, тем выше эффективность боевых операций;

- Интеграция разных родов войск. Армия, авиация, флот, кибервойска и беспилотные системы действуют как единый организм;

- Использование цифровых технологий. IoT, искусственный интеллект (ИИ), большие данные, облачные вычисления и кибероперации становятся ключевыми инструментами.

К преимуществам NCW относятся высокая скорость и точность принятия решений, возможность гибко реагировать на изменения обстановки, уменьшение ошибок за счёт объективных данных, а также более эффективная координация между подразделениями.

Внедрение цифровых технологий позволяет достичь повышения скорости и качества принятия решений, гибкости управления в быстро меняющихся условиях, снижения нагрузки на командиров за счёт автоматизации анализа данных, более эффективного взаимодействия между различными подразделениями, создания адаптивных боевых стратегий.

К основным рискам NCW относятся уязвимость к кибератакам и радиоэлектронному подавлению, зависимость от спутников и цифровой инфраструктуры, сложность обеспечения киберзащиты.

Современная сетецентрическая война сопряжена со следующими угрозами:

– уязвимость к кибератакам, которые могут парализовать сеть управления;

– зависимость от спутниковых и облачных технологий, подверженных перехвату и глушению;

– риск утечки информации через IoT-устройства;

– сложность координации различных стандартов и технологий в единой системе [5].

Сегодня с развитием цифровых технологий современная сетецентрическая война может базироваться на следующих основных принципах:

1. Единое информационное пространство. Единое информационное пространство (ЕИП) в рамках концепции сетецентрической войны – это ключевой элемент, который обеспечивает интеграцию всех участников боевых действий в общую цифровую сеть. Все участники боевых действий подключены к единой цифровой сети, что исключает задержки и искажения информации.

Суть ЕИП заключается в объединение разведывательных систем (спутники, БПЛА, радиолокационные станции, киберразведка), связи с командными пунктами и центрами принятия решений, интеграции боевых подразделений (сухопутные войска, авиация, флот, кибервойска), а также включение логистических и технических структур (снабжение, ремонт, медицинское обеспечение). Все участники операции получают актуальные данные о противнике, союзных силах и обстановке на поле боя. Информация моментально превращается в команду и боевое действие («сенсор – сеть – огонь»). Разнородные источники информации (радиолокация, видео, спутниковая разведка, киберданные) объединяются в единую

систему. Решения могут приниматься как на стратегическом, так и на тактическом уровне благодаря общей базе данных.

Преимущества ЕИП заключается в минимизации «тумана войны», повышении точности огневых ударов, сокращении времени реакции, а также в возможности многодоменных операций (суша, море, воздух, киберпространство, космос).

Вместе с тем, к основным рискам и уязвимостям ЕИП можно отнести зависимость от каналов связи и цифровых технологий, угрозу кибератак и радиоэлектронного подавления, перегрузку информацией, если не используется ИИ для фильтрации данных.

2. Ситуационная осведомлённость. Ситуационная осведомлённость – это способность командования и всех участников боевых действий получать, интегрировать и понимать актуальную информацию о противнике, союзных войсках и внешней среде в режиме реального времени. Командиры в реальном времени получают точные данные о позициях своих войск и противника [2].

Сегодня к технологиям, обеспечивающим ситуационную осведомлённость можно отнести Системы C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance), ГИС и цифровые карты для отображения данных, ИИ для анализа больших данных, IoT и сенсорные сети для мониторинга в реальном времени, киберсистемы для защиты и фильтрации информации.

Таким образом, ситуационная осведомлённость определяется как степень понимания текущего состояния операционной среды, положения противника, союзных сил и нейтральных акторов с целью эффективного управления боевыми действиями.

3. Сокращение цикла «обнаружение – решение – действие». Информация быстро преобразуется в боевые решения и немедленные действия.

Одним из ключевых преимуществ сетецентрической войны является ускорение цикла OODA (Observe – Orient – Decide – Act), предложенного американским военным теоретиком Джоном Бойдом. Этот цикл описывает процесс:

• Обнаружение (Observe) – сбор данных о противнике и обстановке;

• Ориентирование (Orient) – интерпретация полученной информации;

• Принятие решения (Decide) – выбор варианта действий;

• Действие (Act) – реализация выбранного решения.

• Сетецентрическая война позволяет максимально сократить время между этапами за счёт цифровых технологий и интегрированных информационных систем [6].

К преимуществам сокращённого цикла OODA относятся минимизация времени реакции на действия противника, снижение вероятности ошибок за счёт объективных данных, повышение эффективности боевых операций, создание эффекта «опережающего удара» – когда противник не успевает адаптироваться к действиям.

4. Интеграция различных родов войск. Армия, флот, авиация и кибервойска действуют в единой системе управления.

Роль цифровых технологий в управлении боевыми действиями.

Современные цифровые технологии формируют основу сетецентрической войны. Ключевыми направлениями являются:

• Интернет вещей (IoT). Использование датчиков, GPS-модулей и беспилотных аппаратов позволяет в реальном времени отслеживать передвижение техники, состояние вооружений и логистические цепочки [3].

• Искусственный интеллект (AI). Алгоритмы машинного обучения обеспечивают автоматическую обработку разведывательных данных, прогнозирование поведения противника и оптимизацию маршрутов снабжения.

• Большие данные (Big Data). Сбор и анализ огромных массивов информации позволяют выявлять закономерности и моделировать развитие боевой обстановки [4].

• Киберпространство. Кибервойска становятся неотъемлемой частью армии, обеспечивая как защиту своих систем, так и проведение наступательных операций.

• Спутниковые и облачные технологии. Обеспечивают непрерывный обмен данными даже в условиях радиоэлектронного противодействия.

Роль цифровых технологий в ускорении OODA.

1. Интеграция разведывательных данных. Использование C4ISR-систем и сенсорных сетей обеспечивает мгновенный сбор информации с различных источников (БПЛА, спутники, радиолокация).

2. Автоматизированная обработка. Искусственный интеллект и системы машинного обучения анализируют данные в реальном времени, исключая необходимость длительной аналитической работы человека.

3. Единое информационное пространство. Все уровни командования получают доступ к единой базе данных, что исключает задержки при передаче информации.

4. Автоматизация принятия решений. Алгоритмы поддержки принятия решений формируют оптимальные варианты манёвров, маршрутов или распределения ресурсов.

5. Высокоскоростные коммуникации. Спутниковая и защищённая радиосвязь минимизируют время передачи данных.

Заключение. Сетецентрические войны представляют собой новую парадигму ведения боевых действий, где решающую роль играет информация и скорость её обработки. ЕИП является фундаментом сетецентрической войны. Без него невозможно обеспечить быстрый обмен данными и интеграцию действий разных родов войск. Ситуационная осведомлённость – это сердце сетецентрической войны, обеспечивающее информационное превосходство, без которого невозможно достичь успеха в современных конфликтах. Одним словом, ситуационная осведомлённость позволяет превратить данные в знание, а знание – в военное преимущество. Примеры США и НАТО показывают, что

именно высокий уровень информационной интеграции обеспечивает эффективность современных боевых действий. В будущем роль ситуационной осведомлённости будет только возрастать, а её ключевым инструментом станут ИИ и автономные системы.

Сокращение цикла «обнаружение – решение – действие» является одной из ключевых задач сетецентрической войны. За счёт интеграции цифровых технологий, ИИ и систем C4ISR современные армии получают способность действовать быстрее и точнее, чем противник. В условиях высокоманёвренной войны именно скорость информационного цикла определяет победителя.

Цифровые технологии становятся не только средством поддержки военных операций, но и их ключевым элементом. Однако успешная реализация концепции требует создания устойчивой системы киберзащиты, развития собственных цифровых стандартов и интеграции искусственного интеллекта в систему командования.

Использованной литературы:

1. Alberts D., Garstka J., Stein F. Network Centric Warfare: Developing and Leveraging Information Superiority. Washington, DC: CCRP, 1999.

2. Нургалиев И. Сетецентрическая война и перспективы её развития. – Военная мысль, 2020.

3. Ганиев А. Интернет вещей и военное управление: перспективы применения. – Национальная безопасность, 2021.

4. Chen M., Mao S., Liu Y. Big Data: A Survey. – Mobile Networks and Applications, 2014.

5. Шевченко В. Киберугрозы в военной сфере: проблемы и пути решения. – Информационная безопасность, 2022.

6. Alberts D. S., Garstka J. J., Stein F. Network Centric Warfare: Developing and Leveraging Information Superiority. CCRP, 1999.

АНАЛИЗ ПРОЦЕССА ФОРМИРОВАНИЯ ПРОФЕССИОНАЛЬНОЙ КОММУНИКАТИВНОЙ КОМПЕТЕНЦИИ НА ОСНОВЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ (ИКТ)

Убайдуллаева А.А.

Независимый соискатель РУ МО АКТ и Военный Институт Связи ВС РУ центр ПВМ

Формирование образовательного процесса с использованием информационно-коммуникационных технологий через изучение профессионально ориентированных тем на английском языке способствует развитию профессиональной коммуникативной компетенции слушателей военного образования. Кроме того, с целью формирования у слушателей знаний по специальности в процессе профессиональной деятельности в учебный процесс внедрены специальные курсы английского языка, предусмотрено использование интернет-ресурсов, а также организация онлайн-видеоуроков.

Для обеспечения обучения применяются сертифицированные программы, электронные учебники и электронные переводчики (Yandex Translate, Google Translate, Voice Translator, Duolingo). Внедрение информационно-коммуникационных технологий в учебный процесс предусматривает использование таких программ, как Quizlet, где в начале каждого занятия проводится тест на знание лексики. Для установления соответствия между терминами и выражениями составляются три вида лексических упражнений:

1. Jig Word — выбор соответствия из списка (перемещение элементов мышью);

2. Match Word — ввод перевода предложенного слова на экране;

3. Speed Word — выбор соответствия в закрытых карточках (скрытые пары).

В традиционном образовательном процессе, адаптированном под использование информационно-коммуникационных технологий,

применяются нормативные документы. На основе профессионально ориентированных тем создаются комплексы программ для проведения практических занятий по английскому языку. Данные программы обеспечивают организацию учебного процесса на английском языке по специальным дисциплинам, а также позволяют максимально удовлетворить потребности преподавателя в эффективном формировании навыков обучающихся. Особое внимание уделяется разработке рабочих программ, интерактивных презентаций для совершенствования произношения и самостоятельного контроля.

Для повышения эффективности учебного процесса предусматривается работа над грамматическими упражнениями, подготовка профессионально ориентированных презентаций, тестов, заданий на аудирование, развитие речевой деятельности через видеоматериалы и монологи, использование документальных фильмов (с субтитрами и без них), поиск информации в интернет-ресурсах, а также проведение сюжетно-ролевых игр.

Проведение сюжетно-ролевых игр на английском языке по профессионально ориентированным темам с использованием информационно-коммуникационных технологий является одним из наиболее распространённых методов обучения и диагностики знаний.

По мнению У. Машарипова, внедрение ИКТ в учебный процесс обеспечивает реализацию профессиональной коммуникативной компетенции студентов в любой деятельности [1; 45–46]. Следует отметить, что данный процесс также способствует развитию инновационной культуры, так как требует высокого уровня информационной грамотности для самостоятельного поиска необходимой информации. Внедрение ИКТ в образовательный процесс способствует быстрому анализу и корректной интерпретации информации, повышая готовность слушателей военного образования к профессиональной деятельности.

И.Б. Султонов в своих исследованиях подчёркивает, что использование ИКТ в образовательном процессе является одним из

наиболее эффективных средств формирования профессиональной коммуникативной компетенции студентов [2; 78].

Процесс преподавания профессионально ориентированных тем на английском языке совершенствует способность обучающихся использовать информационные технологии для решения задач и достижения профессиональных целей. При этом компьютеры и программы выступают в роли посредников, позволяя студентам планировать действия для достижения результата, обрабатывать и систематизировать информацию, а также представлять её в доступной форме [3; 77–81].

В.В. Шишканова отмечает, что внедрение инновационных технологий в образовательный процесс при обучении иностранным языкам способствует развитию профессиональной коммуникативной компетенции, разделению студентов на малые группы и повышению уровня владения языком [4; 160–165]. Кроме того, эффективными средствами обучения являются иллюстративные материалы, тексты и другие наглядные пособия.

Важнейшие средства формирования профессиональной коммуникативной компетенции в военном образовании включают:

- ориентацию учебного процесса на практические примеры из профессиональной деятельности и выполнение заданий преимущественно индивидуально;

- восприятие и применение инновационных технологий для развития коммуникативных навыков в процессе научных исследований и повседневной деятельности.

В то же время, в некоторых высших военных учебных заведениях имеются проблемы: недостаток учебных часов по английскому языку и определённые трудности в использовании инновационных технологий в образовательном процессе.

По мнению В.В. Лихановой, для эффективного применения ИКТ в формировании профессиональных знаний студентов необходимо использовать мультимедийные программы, организовывать дискуссии по профессиональным темам, привлекать студентов к

дополнительным занятиям, а также развивать навыки самостоятельной работы [5; 48]. Использование мультимедийных средств повышает эффективность преподавания английского языка по специальности, способствует самостоятельной исследовательской деятельности студентов, формированию навыков устного высказывания, созданию комфортной образовательной среды и экономии времени.

Основное направление	Содержание Мероприятия	Цель / Результат
Использование ИКТ в обучении	Онлайн-курсы, электронные учебники, переводчики, программы (Quizlet, Duolingo)	Формирование профессиональной коммуникативной компетенции
Лексические упражнения	Jig Word, Match Word, Speed Word	Закрепление терминологии и лексики по специальности
Традиционный процесс + ИКТ	Создание программ, нормативные документы, интерактивные презентации	Эффективная организация учебного процесса, развитие произношения и самоконтроля
Учебная деятельность	Грамматические упражнения, презентации, тесты,	Развитие речи, навыков анализа, самостоятельного общения
Ролевые игры	Сюжетно-ролевые занятия по профессиональным темам	Диагностика знаний и формирование практических навыков

Использование мультимедийных средств в учебном процессе способствует повышению эффективности преподавания профессионально-ориентированных дисциплин на немецком языке и является удобным инструментом для формирования профессиональной коммуникативной компетенции студентов. Это расширяет возможности самостоятельных исследований, повышает результативность изучения профессиональных знаний на немецком языке, развивает умение студентов излагать свои мысли на немецком

языке, формирует основу для самостоятельной работы, экономит личное время обучающихся и, прежде всего, обеспечивает создание комфортной образовательной среды. Достигается это посредством знакомства студентов с усовершенствованной, максимально естественной и интерактивной информационно-технологической средой.

Согласно утверждению В.В. Шишкановой, использование инновационных технологий реализуется посредством применения электронных тестовых систем, что позволяет усвоить более высокий уровень информации и знаний, а также эффективно реализовать все положительные стороны образовательного процесса [6; 128–135].

По утверждению Й.С. Полата, для развития профессиональной коммуникативной компетенции студентов необходимо внедрение в учебный процесс мультимедийных и гипертекстовых технологий, а также использование компьютерных обучающих курсов.

Поскольку большинство таких учебных курсов предназначено для дистанционного обучения, они должны соответствовать следующим требованиям:

- интеграция самостоятельной учебной деятельности студентов с различными источниками информации, а также с учебными материалами, специально разработанными для данного курса;

- обеспечение оперативного и регулярного взаимодействия с преподавателем курса и координирующими консультантами

А.Б. Гусева в процессе анализа своих научных исследований отмечает, что внедрение специфических особенностей преподавания иностранного языка в учебный процесс для студентов нефилологических направлений является одной из ключевых основ развития их профессиональной деятельности [8; 60–70].

Проведённый анализ показал, что интеграция информационно-коммуникационных технологий в образовательный процесс военных учебных заведений способствует более эффективному формированию профессиональной коммуникативной компетенции слушателей. Использование электронных ресурсов, мультимедийных программ и сюжетно-ролевых технологий не только повышает

качество обучения английскому языку по профессиональной направленности, но и формирует навыки самостоятельного поиска, анализа и систематизации информации. Внедрение инновационных технологий создаёт условия для повышения готовности будущих военных специалистов к профессиональной деятельности, ориентированной на современную информационную среду.

Использованной литературы:

1. Машарипов У.А. Методика формирования речевой культуры студентов, изучающих иностранные языки в условиях инновационного образования: дис. канд. пед. наук (PhD). – Ташкент, 2021. – 139 с.

2. Султанова И.Б. Формирование иноязычной социокультурной компетенции у студентов-психологов (на материале английского языка): дис. канд. пед. наук: 13.00.02. – Волгоград, 2007. – 238 с.

3. Низамов Г.М. Важные факторы и эффективность использования коммуникативной методики в процессе преподавания иностранного языка в сочетании с критериями профессиональной коммуникативной компетентности // Научный вестник Ташкентского государственного педагогического университета. – 2022. – №12. – С. 800.

4. Шишканова В.В. Формирование социокультурной компетенции у студентов неязыкового вуза (бакалавриат, немецкий язык): дис. … канд. пед. наук. – Москва, 2015. – 160 с.

5. Лиханова В.В. Формирование межкультурной компетентности студентов неязыковых вузов средствами краеведческого материала: дис.канд. пед. наук: 13.00.01. – Улан-Удэ: Бурятский государственный университет, 2010. – 217.

6. Полат Е.С. Новые педагогические и информационные технологии в системе образования: учебное пособие для студентов педагогических вузов и системы повышения квалификации педагогических кадров. – М.: Издательский центр «Академия», 2003. – 272 с.

7. Гусева Л.В. Принципы создания ситуаций межкультурного общения для формирования межкультурной компетенции студентов по направлению «Туризм» // Высшее образование сегодня. – 2015. – №1. – С. 83–90.

RAQAMLI XAVFSIZLIK VA SHAXSIY MA'LUMOTLAR HIMOYA QILISH

Saidbayev B.Dj.
Texnika fanlari bo'yicha falsafa doktori (PhD), podpolkovnik
"Axborot texnologiyalari" kafedrasi dotsenti

Siz bu so'zlarni internet orqali o'qiyapsiz. Katta ehtimol bilan musiqa eshitish yoki video ko'rish uchun fayllarni internetdan yuklab olasiz. Plastik kartadan plastik kartaga pul o'tkazish uchun onlayn dasturlardan foydalanasiz. Yaqinlaringiz bilan Telegram kabi messenjerlarda shaxsiy mavzularda gaplashasiz. Ko'chaga chiqmasdan kommunal to'lovlarni qilishingiz, uyga taksi chaqirishingiz yoki ovqat buyurtma berishingiz ham mumkin. Hattoki, o'zingiz internetda ishlashingiz ham mumkin. Umuman olganda, odamlarning hayoti raqamlashib bormoqda. Raqamli hisoblanadigan smartfonlar, dasturlar va internet zamonaviy hayotning bir qismiga aylanib bo'ldi.

Odamlar odatda uyining, borayotgan manzilining, yashayotgan mamlakatining xavfsizligiga alohida e'tibor qaratishadi. Gaplashayotgan suhbatdoshlariga, sotuvchilarga va har xil va'dalarga qanchalik ishonish mumkinligini o'ylab ko'rishadi. Lekin xuddi shu narsalar raqamli ko'rinishga o'tganda odamlar tez aldanib qolishlari mumkin. Shuning uchun ham yangiliklarda kiberfiribgarlarning qurbonlari haqidagi xabarlar ko'paymoqda.

Raqamli xavfsizlik — bu raqamli ma'lumotlaringiz, qurilmalaringiz va resurslaringizni himoya qilish amaliyoti. Bunga shaxsiy ma'lumotlaringiz, akkauntlaringiz, fayllaringiz, fotosuratlaringiz va hattoki plastik kartangizdagi pulingiz ham kiradi.

Zamonaviy media muhitda xavfsiz va qo'rquvsiz yashash uchun birinchi zaruriy qadam shaxsiy ma'lumotlarni muhofazalash ko'nikmasini

orttirishdan boshlanadi. Shaxsiy ma'lumotlar o'z nomi bilan sizning shaxsiyatingizni aniqlab berishda ishtirok etuvchi barcha zaruriy ma'lumotlarni o'z ichiga oladi. Bunday ma'lumotlarning sizib chiqishi sizning jamiyatda kasb etgan qiyofangizga, siz haqingizdagi atrofingizdagilarning fikrlari va tasavvurlarga ta'sir qilgani bois, shuningdek, sizga moddiy, ma'naviy, psixologik zarar keltirish, yomon maqsadlarda qo'llanilish va obro'sizlantirish riskini saqlagani tufayli atrofdagilardan muhofazalanishi zarur. Quyidagi maqolada ana shunday muhim ma'lumotlarni asrash uchun zaruriy bo'lgan bilimlarni siz bilan bo'lishamiz.

Maxfiyligingiz va xavfsizligingizni himoya qilish uchun o'zgalar tomonidan ruxsatsiz olish, kirish va foydalanishdan himoya qilinishi zarur bo'lgan shaxsiy ma'lumotlar quyidagilardir:

- To'liq ism-sharif
- Uy manzili
- Telefon raqamlar (uy, ish, mobil)
- Elektron pochta manzillari
- Identifikatsiya raqamlari (shaxsni tasdiqlatuvchi hujjatlardagi raqamlar, shaxs guvohnomasi (ID card) raqami, pasport raqami, ijtimoiy sug'urta raqami, haydovchilik guvohnomasi raqami va boshqalar)
- Tug'ilgan sana, yosh va tug'ilgan joy
- Moliyaviy ma'lumotlar (bank hisob raqamlari, kredit karta raqamlari, moliyaviy hisoblarni boshqaruvchi mobil va desktop ilovalar, PIN-kodlar, parollar)
- Salomatlik va tibbiy ma'lumotlar (shaxsga oid tibbiy tarix, shifokor tomonidan berilgan ko'rsatmalar, retseptlar, sug'urta ma'lumotlari)
- Ish faoliyati tarixi, ma'lumoti va kasbiy malakasi haqidagi ma'lumotlar
- Biometrik ma'lumotlar (barmoq izlari, yuz tanish moslamalari uchun yuz tuzilishiga oid ma'lumotlar, retinal skanerlar)
- Raqamli va onlayn identifikatorlar (tarmoqdagi foydalanuvchi nomlari, parollar, xavfsizlik savollari, IP manzillar, cookie-fayllar)

- Ijtimoiy tarmoq profillari va hisob qaydnomalari
- Shaxsiy fotosuratlar va videolar
- Joylashuv (geolokatsiya) ma'lumotlari (GPS koordinatalari, tez-tez tashrif buyuriladigan joylar)
- Soliq va daromad haqida ma'lumotlar
- Huquqiy hujjatlar (vasiyatnomalar, shartnomalar, nikoh guvohnomalari, ajrim hujjatlari)

Yuqoridagi ma'lumotlarning aksar qismi bugun media qurilmalarda saqlanadi va boshqariladi. Ularni to‘g‘ri ehtiyotlash uchun esa ushbu texnologiyalarning tabiati, ular bilan to‘g‘ri muloqot qilish haqida atroflicha bilib olish zarur.

Online platformalarda to‘liq ism-sharifdan foydalangan ma'qulmi?

Ijtimoiy tarmoqlar, messenjerlar, bloglar, saytlar va boshqa onlayn platformalarda haqiqiy ismingizdan foydalanishingizning holatiga qarab, ijobiy va salbiy tomonlari bor.

Agar onlayn platforma ishonchli bo‘lmasa, unga to‘liq ism-sharifingizni kiritmaganingiz ma'qul. Sababi maxfiylik va xavfsizlik darajasi u platformalarda yaxshi bo‘lmasa, kiberfiribgarlar kamida to‘liq ism-sharifingiz yozilgan akkauntlarning nomidan noqonuniy yoki obro‘ngizga ta'sir qiluvchi harakatlar qilishi mumkin. Akkauntingizga qanday ruxsatlar berilganiga qarab, sizning shaxsiy bo‘lgan fotolaringiz, videolaringiz va hujjatlaringizni o‘g‘irlashi mumkin.

Agar ijtimoiy tarmoqlarda shaxsingizning ko‘pchilikka bildirish niyatingiz yo‘q bo‘lsa ham haqiqiy ismingizni yozmaganingiz ma'qul. Sababi to‘liq ism-sharifingiz yozilgan akkaunt bo‘lsa, birinchidan, hakerlar uchun akkauntingizni topish osonlashadi, ikkinchidan, sizga nisbatan kiberbulling qilish mumkin, trolling qurboniga ham aylanishingiz mumkin. Uchinchidan, haqiqiy ismingiz nomiga ochilgan akkauntga qo‘ygan post va fikrlaringizni vaqti kelganda sizga qarshi ishlatishlari ehtimoli ham bor. Bundan tashqari, qilgan har bir harakatingiz, misol uchun, ko‘rgan kontentlaringiz, bosgan layklaringiz o‘sha platformaning serverlarida umrbod saqlanib qolishi mumkin.

my.gov.uz kabi davlat xizmatlari saytlaridan foydalanmoqchi bo‘lsangiz, to‘liq ism-sharifingizni kiritishingiz kerak. Sababi davlat sizga xizmat ko‘rsatishi uchun foydalanuvchi aynan siz ekanligingizga amin bo‘lishi kerak.

Lekin davlat nomidan ochilgan soxta platformalarga, to‘liq ism-sharifingizni kiritishingiz evaziga yutuq berishni va’da qiladigan feyk saytlarga ishonmaganingiz ma’qul. Shuning uchun aldanib qolishni xohlamasangiz, har safar haqiqiy ismingizni kiritayotganingizda platformaning domeniga alohida e’tibor bering.

Shaxsiy brendingizni rivojlantirmoqchi bo‘lsangiz, ishonchli bo‘lgan LinkedIn, Facebook va Instagram kabi ijtimoiy tarmoqlarda haqiqiy ismingizdan foydalangan holda ro‘yxatdan o‘tsangiz ham bo‘ladi.

O‘zingiz bilmagan holda uy manzilingizni ulashib qo‘ymang!

Siz shu kungacha bilmasdan turib uy manzilingizni internetga ko‘p tarqatgan bo‘lishingiz ham mumkin.

Misol uchun geotegging tufayli ko‘pchilik bilmasdan uy manzilini ulashib qo‘yadi. Hozirgi kamera va smartfonlar rasm yoki video olib bo‘lib, faylni saqlayotganida uning ichiga joylashuv ma’lumotlarini ham qo‘shib ketadi. Shu funksiya geotegging deyiladi. Aslida bu funksiya kerakli vaziyatlarda yoki kerakli odamlarga qayerda suratga olganingizni ko‘rsatishga yordam beradi. Lekin, masalan, uyda tushgan suratingizni internetga yuklaydigan bo‘lsangiz, internetdagi har qanday odam qiynalmasdan uy manzilingizni bilib olishi mumkin. Buning oldini olish uchun qurilmangiz sozlamalarida geoteggingni o‘chirib qo‘yishingiz yoki faylni internetga yuklashdan oldin joylashuv ma’lumotlarini olib tashlashingiz mumkin.

Metama’lumotlar ham uy manzilingizni bilmasdan internetga tarqatishingizga sababchi bo‘lishi mumkin. Metama’lumotlar — ma’lumotlar haqidagi ma’lumotlardir. Ya’ni sizning suratlaringizni ma’lumot deydigan bo‘lsak, metama’lumotlar shu surat qayerda, qachon, qaysi vaqtda va qaysi qurilma tomonidan olinganini, o‘zgartirilganini va boshqa ma’lumotlarni o‘z ichida saqlaydi. Metama’lumotlari bor fayllaringizni internetga ulashadigan bo‘lsangiz, bitta uy manzilingizni

emas, qaysi telefondan foydalanishingizni ham ulashib qo‘yishingiz mumkin. Buning oldini olish uchun faylni internetga yuklashdan oldin unda metama’lumotlari bor yoki yo‘qligini aniqlang, agar bor bo‘lsa, verexif.com kabi saytlar yordamida metama’lumotlarni olib tashlang.

Ma’lumotlaringizni yashirib turib, o‘zingiz uy manzilingizni o‘z qo‘llaringiz bilan kiberfiribgarlarga berib qo‘yishingiz mumkin. Onlayn so‘rovnomalarda qatnashadigan bo‘lsangiz, unda sizdan manzilingizni so‘rashlari mumkin, agar siz manzilni kiritadigan bo‘lsangiz, ular sizning uy manzilingizni bilib olishadi. Shuning uchun qayerlarga uy manzilingizni kiritayotganingizga doim e’tibor qarating, hattoki evaziga qandaydir yutuq taklif etilsa ham.

Telefon raqamingizni ehtiyot qilish nima uchun muhim?

Sizning telefon raqamingiz faqatgina siz bilan bog‘lanish uchun kerak bo‘ladigan vosita emas. Chunki u sizning ismingiz, manzilingiz, joylashuvingiz, ijtimoiy tarmoqlardagi akkauntlaringiz va hattoki bankdagi ma’lumotlaringiz kabi ko‘plab shaxsiy ma’lumotlarni ochib berishi mumkin. Shuning uchun telefon raqamingizni kim bilan baham ko‘rayotganingizga e’tiborli bo‘lishingiz kerak, ayniqsa saytlar va ijtimoiy tarmoqlarda.

Telefon raqamingizni ijtimoiy tarmoqlarda yoki saytlarda hammaga ko‘rinadigan qilib qo‘ysangiz, ko‘plab muammolarga duch kelishingiz mumkin.

Eng beozori bu — spam qo‘ng‘iroqlar va SMSlar. Firibgarlar yoki prankchilar sizga qo‘ng‘iroq qilib, nimanidir sotmoqchi bo‘lishi yoki shunchaki jig‘ingizga tegmoqchi bo‘lishi mumkin. Bu ham sizga noqulaylik olib keladi, ham vaqtingizni behuda sarflaydi.

Telefon raqamingizni bilib olib, shaxsingizni o‘g‘irlashlari mumkin. Bunda telefon raqamingiz orqali nomingizdan elektron pochta, ijtimoiy tarmoqda akkaunt yoki bankda hisob ochishlari mumkin. Undan ham yomonrog‘i o‘zingizning akkauntlaringizga o‘rningizdan kirishlari mumkin. Bu esa obro‘ngizning to‘kilishiga va katta miqdorda pul yo‘qotishingizga olib keladi.

Kimdir sizning telefon raqamingizdan joylashuvingizni bilib olib, doimiy kuzatib borishi mumkin. Turli tahdidlar esa sizni xavf ostiga qo‘yib, ruhiy salomatligingizga yomon ta’sir qilishi mumkin.

Telefon raqamingiz ortidan muammolarga duch kelmaslik uchun birinchi navbatda telefon raqamingizni saytlarga va ijtimoiy tarmoqlarga ochiq joylashtirmang. Raqamingizni faqat o‘zingiz ishonadigan va shaxsan biladigan odamlar bilan baham ko‘ring. Xizmatlar yoki ilovalarga ro‘yxatdan o‘tish kabi tekshirishni talab qiladigan onlayn harakatlar uchun ikkinchi darajali yoki bir martalik telefon raqamlaridan foydalaning. Vaqtinchalik yoki muqobil raqamni olish uchun Google Voice yoki Burner kabi xizmatlardan foydalanishingiz mumkin. Qurilmangiz sozlamalariga kirib, spamlardan himoya qilish funksiyasini yoqib qo‘ying yoki Truecaller yoki Hiya kabi ilovalardan foydalaning. Saytlar va ijtimoiy tarmoqlarda maxfiylik sozlamalarini tekshiring. Telefon raqamingizni va boshqa shaxsiy ma’lumotlaringizni kim ko‘rishini nazorat qilayotganingizga ishonch hosil qiling. Xavfsizligiga ishonchingiz komil bo‘lmasa, so‘rovnomalarda telefon raqamingizni qoldirmang.

Google o‘zida qanday shaxsiy axborotlaringizni saqlaydi?

Agar siz internetdan foydalansangiz, katta ehtimol bilan sizda Google akkaunti bor. Google akkauntingiz Gmail elektron pochta manzilingiz, YouTube profilingiz, Google Play hisobingiz yoki Google Photos dasturi orqali ochilgan bo‘lishi mumkin. Google akkaunt hayotingizni yanada qulay va qiziqarli qilib beradigan ko‘plab xizmatlar va ilovalardan foydalanish imkonini beradi. Ammo Google siz haqingizda qanday shaxsiy ma’lumotlarni saqlashini bilasizmi? Google sizning shaxsiy ma’lumotlaringizni nima qilishini-chi?

Google

— ismingiz,

— elektron pochta manzilingiz,

— telefon raqamingiz,

— tug‘ilgan kuningiz,

— jinsingiz,

— yashayotgan mamlakatingiz,

— qurilmangiz modeli,
— sizdagi operatsion tizim,
— o‘rnatilgan brauzerlar,
— IP manzilingiz,
— identifikatorlar kabi qurilmangiz ma’lumotlari,
— GPS koordinatalaringiz,
— uyali aloqa tarmoqlari va Bluetooth signallari kabi ma’lumotlaringiz,
— siz tashrif buyurgan veb-sahifalar,
— tomosha qilgan videolaringiz,
— foydalanadigan ilovalaringiz,
— qilgan qidiruvlaringiz,
— bosgan layklaringiz,
— ko‘rgan reklamalaringiz,
— siz yuborgan va qabul qilgan elektron pochta xabarlari,
— fotosuratlaringiz,
— videolaringiz,
— qaysi tilda gapirishingiz,
— sizga qanday bildirishnomalar kelishi,
— qaysi kanallarga obuna bo‘lganingiz haqidagi va yana boshqa ma’lumotlaringizni o‘zida saqlaydi.

Google shuncha shaxsiy ma’lumotingizni yig‘ib, sizga yanada yaxshiroq xizmatlar ko‘rsatishni, YouTubeda qiziqarliroq videolarni taklif qilishni, foto va videolaringizni yanada yaxshiroq tahrir qilib berishini boshlaydi, deyishadi. Bu rost. Lekin Google sizni bilib olib, reklamachilarga shaxsiy ma’lumotlaringizni sotadi va siz o‘zingiz yaqinda izlagan narsalaringizni reklamalarda ko‘rasiz. Bundan tashqari, shaxsiy ma’lumotlaringiz uchinchi shaxslar tomonidan har doim ham sizning manfaatingiz uchun emas, balki turli maqsadlarda ishlatilishi mumkin. Bu bitta sizga tegishli emas, Googledan foydalanadigan milliardlab odamlarga tegishli.

Google siz haqingizda qanday ma’lumotlarni yig‘ganini bilish uchun myaccount.google.com saytiga kirishingiz kerak. U yerdan siz shaxsiy

ma’lumotlaringizni ko‘rib chiqib, Google bilishi kerak emas deb hisoblagan ma’lumotlarni o‘chirib yuborishingiz va kelajakda shu ma’lumotlarni yig‘ishda davom etishini to‘xtatishingiz mumkin. Shaxsiylashtirilgan reklamalardan voz kechishingiz mumkin, shunda sizning ma’lumotlaringizga asoslanib reklama ko‘rsatishni to‘xtaydi. Google Takeout dasturi orqali esa Google siz haqingizda yig‘gan ma’lumotlarni yuklab olishingiz mumkin.

Shaxsiy ma’lumotlaringizni himoyalashda elektron pochtangiz ham muhim rol o‘ynaydi. Uni ham ochiq internetga qo‘ymagan yaxshi. Chunki pochtangiz bundan keyin spamlarga to‘lib ketishi mumkin. Pochtangizga keladigan maxfiy raqam va belgilarni hech kimga aytmaslikni ham unutmang. “Siz mukofot yutdingiz” qabilidagi, davlat va banklar nomidan yozadigan soxta xabarlardagi havolalarga kira ko‘rmang. Google akkauntingizni kiberfiribgarlar egallab olishi mumkin.

Eng muhimi, shaxsiy ma’lumotlaringizni himoyalashda internetda har bir ulashayotgan ma’lumotlaringizga, kirayotgan havolalaringizga va internetda o‘tirganingizda o‘zingizdan qanday raqamli iz qoldirayotganingizga e’tiborli bo‘ling.

Foydalanilgan adabiyotlar:

1. https://www.simplilearn.com/what-is-digital-security-article

2. https://www.nytimes.com/guides/privacy-project/how-to - protect -your-digital-privacy

3. https://www.security.org/digital-safety/

HARBIY OBYEKTLAR VIDEOKAMERALARIDAN MA’LUMOTLARNI UZATISH PROTOKOLLARINING TAHLILI

Mambetsharipov Y.R.
O‘R JXU kafedra dotsenti

Zamonaviy harbiy infratuzilmalar xavfsizligini ta’minlashda kuzatuv va monitoring tizimlari muhim ahamiyat kasb etadi. Ayniqsa, strategik ahamiyatga ega obyektlar — qo‘mondonlik markazlari, qurol-aslaha omborlari, chegara postlari va aerodromlar kabi joylarda videokuzatuv

tizimlari orqali real vaqt rejimida axborot olish, tahlil qilish va tezkor qarorlar qabul qilish zaruriyati ortib bormoqda.

Bunday tizimlarning samarali ishlashi, avvalo, videokameralardan olingan ma'lumotlarni ishonchli va tezkor tarzda uzatish protokollariga bog'liq. Harbiy tarmoqlarda qo'llaniladigan ma'lumot uzatish kanallari yuqori darajadagi himoya, shifrlash, kechikishlarga bardoshlilik hamda uzluksiz aloqa talablariga javob berishi lozim.

Joriy vaqt masshtabida videoni yetkazib berish uchun o'zaro bog'langan protokollar to'plami mavjud:

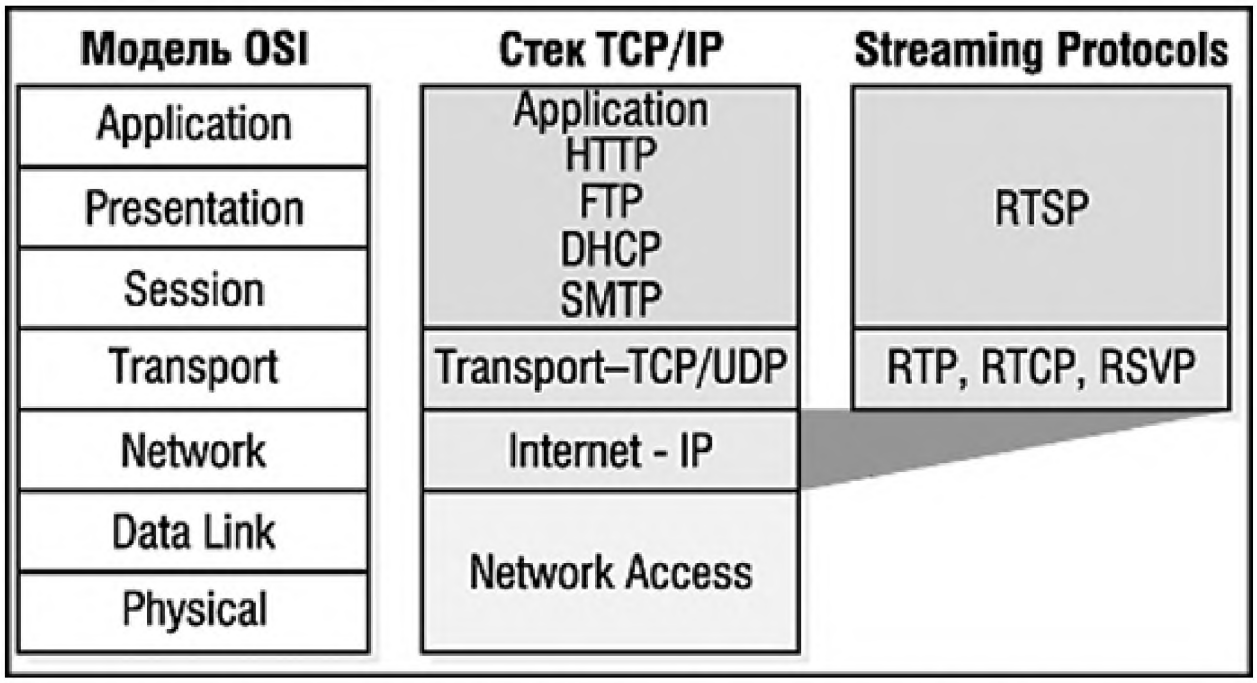
- RTP (Real-Time Transport Protocol);
- RTCP (Real-Time Control Protocol);
- RSVP (Resurslarni zaxiralash protokoli);
- RTSP (Real-time Streaming Protocol).

Bu protokollarning har biri videotrafikni yetkazib berishga o'z ulushini qo'shadi. OSI etalon modelining steki va qatlamlariga nisbatan oqim protokollarining holati 1-rasmda aks ettirilgan.

RTP IP protokoliga asoslangan transport protokoli bo'lib, video ma'lumotlarini paketlar kommutatsiyalanadigan tarmoqlar, xususan, Internet orqali uzatish uchun ishlatiladi. RTCP va RSVP protokollari birgalikda multimedia fayllari uchun uchdan-uchga yetkazib berishni va zarur QoS darajasini ta'minlay oladi. RTP marshrutlashtirish funksiyasini o'z ichiga olmaydi, chunki buning uchun TCP/IP protokoli stekidagi UDP (User Datagram Protocol) deytagrammalar xizmatidan foydalaniladi. RTP foydali yuklama turini aniqlash, paketlar ketma-ketligini raqamlash va vaqt belgilarini tayinlash kabi funksiyalarni bajaradi.

RTP transport qatlami protokoli bo'lsa-da, u ilovalar qatlamiga xos bo'lgan qator funksiyalarini bajaradi. Ular sirasiga paketlarni vaqt bo'yicha tartiblash, rekonstruksiyalash va sinxronlashtirish kiradi. Buni amalga oshirishga imkon beradigan ma'lumotlar RTP sarlavhasiga joylashtirilgan. Shuningdek, bu yerda foydali yuklamani shifrlash usuli haqida ma'lumotlar mavjud, bu muhim, chunki shifrlash usuli tarmoq yuklamasiga bog'liq ravishda o'zgarishi mumkin. RTCP uzatishni boshqarish protokoli hisoblanadi. Boshqaruv funksiyalarini bajaradi va

diagnostika va unumdorlikni optimallashtirish uchun RTP boshqaruv ma'lumotlarini taqdim etadi. Bundan tashqari, u ma'lumotlarni yetkazib berish sifatini nazorat qilishni amalga oshiradi. Protokolning asosiy funksiyalari quyidagilardan iborat:



1-rasm. OSI etalon modelining steki va qatlamlariga nisbatan oqim protokollarining holati

- QoS monitoringi va kanalning o'ta yuklanishini boshqarish;
- manbani identifikatsiyalash (aniqlash);
- masshtablashtirishni boshqarish.

Qabul qilish tugunida RTCP protokoli generatsiyalagan teskari aloqa paketlari asosida jo'natuvchi ma'lumotlarni uzatish tezligini sozlashi mumkin. Bu paketlardan tarmoq ma'muri tarmoqning unumdorligini baholash uchun ham foydalanishi mumkin. Manbani aniqlash uchun RTCP mos sarlavha maydonining 32-bitli qiymatini istalgan sessiya ishtirokchilarini identifikatsiyalaydigan noyob global nomlarga o'zgartiradi.

RSVP videoma'lumotlarni o'z vaqtida va samarali tashish uchun butun marshrut bo'ylab resurslarni zaxiralaydigan protokol hisoblanadi. Shu maqsadda u kommutatorlarga, marshrutizatorlarga va boshqa tarmoq qurilmalariga kerakli o'tkazish polosasiga so'rovlarni uzatadi. RTSP

protokolini ma'lumotlarni uzatish bilan hech qanday aloqasi yo'q. Bu amaliy qatlam protokoli va uning vazifasi oxirgi foydalanuvchiga oqimni boshqarishni ta'minlashdan iborat. RTSP orqaga aylantirish, pauza va to'xtatish kabi operatsiyalarni bajarishga imkon beradigan interfeysni ta'minlaydi.

RTSP protokoli RTP, RSVP, IP va TCP/UDP kabi quyi qatlam protokollar bilan birgalikda ishlaydi. RTSP masshtablanuvchanlik va o'zaro ta'sirlashish xususiyatlariga ega. RTSP protokolida holat yoki aloqani boshqarishni server bajarishini ko'zda tutadi. RTSP protokolida ma'lumotlar asosiy polosadan tashqari (out-of-band) boshqa protokollar, masalan, RTP orqali uzatilishi mumkin. RTSP xizmati server va mijoz o'rtasida almashinadigan ko'rsatmalar to'plami bilan qo'llanadi. Ular oqim uchun o'rnatish parametrlarini o'z ichiga olgan RTSP paketlari ko'rinishida uzatiladi.

Joriy vaqtda ishlash uchun veb-ilovalar bilan bog'liq eng keng tarqalgan muammo ilovalar qatlamining HTTP protokoli hisoblanadi. Bu so'rov-javob protokoli bo'lib, unda faqat mijoz so'rov uzatishi mumkin va faqat server mijozning oldingi uzatilgan so'roviga javob uzatishi mumkin. Odatda, HTTP transport qatlami protokoli sifatida TCP protokolidan foydalanadi. TCP-bog'lanish so'rov uzatilgandan va javob olinganidan keyin yopiladi. Agar mijoz takroran server bilan aloqani xohlasa, TCP-bog'lanish mijoz tomonidan takroran ishga tushirilishi kerak. HTTP-polling kabi boshqa yechimlar ham mavjud, ammo bu yondashuv bilan faqat joriy vaqt rejimiga yaqin sxemaga erishish mumkin, chunki mijoz ma'lum bir chastotada yangi yangilanishlar uchun serverdan so'rashi kerak.

Shuningdek, so'rovlar tezligini juda past o'rnatish mumkin, ammo bu holda ilova yaxshi ishlamaydi. Odatda, HTTP-bog'lanish bilan TCP protokoli har bir so'rov-javob bosqichidan keyin yopiladi. Mijoz va server doimiy bir-birlariga ulanganda yana bir muammo yuzaga keladi, bu esa har bir mijoz uchun barcha ulanishlar ochiq bo'lganligi sababli server resurslari bilan bog'liq muammolarni keltirib chiqarishi mumkin.

Foydalanilgan adabiyotlar:

1. Павлов М.С. Реализация сервера для установления соединения и непрерывного обмена между парами компьютер-мобильное устройство // Молодежный научно-технический вестник. 2014. № 10. С. 18.

2. Ричардсон Ян. Видеокодирование. H. 264 и MPEG-4 – стандарты нового поколения // Техносфера. Москва– 2005 С. – 368.

3. Mambetsharipov Y.R., Saidboyev B.Dj., Kamilov M.A. Videokuzatuv tizimining mijoz va server qismlari orasidagi o‘zaro ta’sirlashish algoritmlari // «Harbiy aloqa va AKT xabarlari» jurnali, №2(10)/2022. –44-50 b.

MILLIY GVARDIYASI BO‘LINMALARIDA AXBOROT XAVFSIZLIGI HAMDA OBYEKTLAR XAVFSIZLIGINI TA’MINLASHDA AXBOROT TEXNOLOGIYALARI VA TEXNIK QO‘RIQLASH VOSITALARINING O‘RNI

Ochilov I.N.

O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti Qo‘riqlashni muhandislik-texnik ta’minlash kafedrasi dotsenti, h.f.b.f.d. (PhD) dotsent

Ma’lumki, har qanday davlatning axborot resurslari uning iqtisodiy va harbiy salohiyatini belgilovchi omillardan biri hisoblanadi. Ushbu resursdan samarali foydalanish mamlakat xavfsizligini va demokratik axborotlashgan jamiyatni muvaffaqiyatli shakllantirilishini ta’minlaydi. Bunday jamiyatda axborot almashinuv tezligi yuksaladi, axborotlarni yig‘ish, saqlash, qayta ishlash va ulardan foydalanish bo‘yicha ilg‘or axborot-kommunikatsiyalar texnologiyalarini qo‘llash keng ko‘lamda amalga oshiriladi.

2021-yilning 14-dekabr kuni bo‘lib o‘tgan Oliy Majlis palatalarining qo‘shma majlisida O‘zbekiston Respublikasi Prezidenti Shavkat Mirziyoyev “Axborot-kommunikatsiya texnologiyalari sohasi qanchalik rivoj topgani sari, uning afzalligi va qulayliklaridan foydalanish bilan bir qatorda, butun mamlakatimizda axborot xavfsizligini ta’minlash eng

dolzarb masalaga aylanib bormoqda.” deb, deputatlarning e’tiborini ushbu masalaga qaratdi.

Davlatning axborot xavfsizligini ta’minlash muammosi milliy xavfsizlikni ta’minlashning asosiy va ajralmas qismi bo‘lib, axborotni muhofaza qilish esa davlatning birlamchi masalalariga, davlat siyosati darajasiga aylanganligi barchamizga ma’lum.

Umumjahon axborot globallashuvi jarayonlari axborot-kommunikatsiya texnologiyalarini nafaqat mamlakatlar iqtisodiyoti va boshqa sohalariga joriy etish, balki axborot tizimlari xavfsizligini ta’minlashni ham taqozo etayotir. O‘zbekiston axborot va kommunikatsiya texnologiyalari sohasidagi xalqaro xavfsizlik tizimiga Markaziy Osiyoda birinchilardan bo‘lib qo‘shildi.

Axborot xavfsizligini ta’minlash bo‘yicha Aloqa, axborotlashtirish va telekommunikatsiya texnologiyalari davlat qo‘mitasi tomonidan quyidagi chora-tadbirlar amalga oshiriladi:

- ma’lumotlar uzatish, telekommunikatsiya tarmoqlari, teleradioefir hamda axborot tizimlarida axborot xavfsizligini ta’minlashni takomillashtirish va rivojlantirish bo‘yicha davlat siyosatini yuritish;

- axborot xavfsizligiga oid qonunchilik va me‘yoriy-huquqiy hujjatlarining yaratilishini tashkil qilish va bunda ishtirok etish;

- axborot tizimlari komplekslari, resurslari va ma’lumotlar bazalarining axborot xavfsizligini ta’minlash;

- davlat organlarining axborot tizimlari va resurslari axborot xavfsizligi siyosatini ishlab chiqish va amalga oshirishga ko‘maklashish;

- davlat axborot tizimlari va resurslarining axborot xavfsizligini ta’minlash yuzasidan monitoring natijalari to‘g‘risidagi statistik ma’lumotlarni O‘zbekiston Respublikasi Aloqa, axborotlashtirish va telekommunikatsiya texnologiyalari davlat qo‘mitasiga belgilangan tartibda taqdim etish;

- telekommunikatsiyalar tarmoqlarining operatorlari va provayderlari bilan hamkorlik qilish, davlat organlarining kompyuter va axborot texnologiyalaridan foydalanish sohasidagi qonun buzilishlarining oldini

olish masalalari bo‘yicha birgalikdagi ishlarini tashkil etish va ularning faoliyatini muvofiqlashtirish;

- internetning milliy foydalanuvchilarini Internet tarmog‘i milliy segmentida axborot xavfsizligiga paydo bo‘layotgan tahdidlar to‘g‘risida o‘z vaqtida xabardor qilish, shuningdek axborotlarni muhofaza qilish bo‘yicha konsultatsiya xizmatlari ko‘rsatish;

- qonun buzuvchilarni tahlil qilish, identifikatsiyalashda, axborotlar makonidagi ruxsatsiz yoxud buzuvchi harakatlarni amalga oshirishda foydalaniladigan metodlar va vositalarni tahlil qilishda huquqni muhofaza qilish organlari bilan hamkorlik qilish;

- internet tarmog‘i milliy segmentida axborot xavfsizligi hodisalarining oldini olish bo‘yicha o‘zaro amaliy ishlarni tashkil etish maqsadida axborot xavfsizligi sohasidagi xalqaro hamkorlikni rivojlantirish.

O‘zbekiston Respublikasi Aloqa, axborotlashtirish va telekommunikatsiya texnologiyalari davlat qo‘mitasi huzuridagi Axborot xavfsizligini ta’minlash markazi tashkil etilgan bo‘lib, mazkur Markazning asosiy maqsadi etib, “Elektron hukumat” tizimining axborot tizimlari, resurslari va ma’lumotlar bazalarining, shuningdek Internet tarmog‘i milliy segmentining axborot xavfsizligini ta’minlash sohasidagi normativ-huquqiy bazani takomillashtirish bo‘yicha takliflar ishlab chiqish, davlat organlari tizimlari va axborot resurslarida axborot xavfsizligini ta’minlash belgilangan.

Markaz xodimlari axborot xavfsizligiga hozirgi vaqtdagi tahdidlar to‘g‘risidagi ma’lumotlarni yig‘ish, tahlil qilish va to‘plash bilan shug‘ullanadilar, “Elektron hukumat” tizimi axborot tizimi, resurslari va ma’lumotlar bazalariga noqonuniy kirib olish holatlarining oldini olishni ta’minlaydigan tashkiliy va dasturiy-texnik yechimlarni samarali qabul qilish bo‘yicha tavsiyalar va takliflar ishlab chiqishda ishtirok etadilar.

“Elektron hukumat” tizimi axborot xavfsizligini ta’minlashning me‘yoriy-huquqiy asoslarini takomillashtirish bo‘yicha takliflarini ishlab chiqish ham Markazning maqsad-vazifalari hisoblanadi.

Shuningdek, Prezident Shavkat Mirziyoyev joriy yilning 27-avgust kuni Toshkent viloyati va poytaxtimizdagi shunday majmualar bilan tanishdi.

Ulardan biri - Zangiota tumanida qurilgan “Elektron hukumat” tizimi ma’lumotlarini saqlash va qayta ishlash yagona markazi hisoblanadi.

Mamlakatimizda barcha sohalarni raqamlashtirish, xizmatlarni odamlarga qulaylashtirish choralari ko‘rilmoqda. Shuningdek, yurtimiz masofaviy xizmatlar eksporti bo‘yicha o‘ziga xos mintaqaviy xabga aylanib bormoqda. Bu xalqaro talablarga mos Datamarkaz tashkil qilishni zaruratga aylantirdi.

Shu bois “Raqamli O‘zbekiston - 2030” strategiyasi doirasida O‘zbekistonda ilk bor katta hajmdagi ma’lumotlarni saqlash va qayta ishlash markazi barpo etildi. Davlatimiz rahbari bu erda yaratilgan sharoitlarni ko‘zdan kechirdi.

Markazda Xitoyning Huawei kompaniyasi bilan hamkorlikda 20 peta bayt xotiraga ega tizim tashkil etilgan. 580 ta server, umumiy elektr quvvati 5 megavattli dizel generatorlar tizimning uzluksiz ishlashini ta’minlaydi. Binoni sovutish, yong‘in xavfsizligini ta’minlash tarmoqlari ham barcha talablarga javob beradi. Umuman, Ma’lumotlar markazi xalqaro “Uptime” instituti tomonidan beriladigan TIER III sertifikatiga ega.

- Bu markaz raqamlashtirishning “yuragi”, “Elektron hukumat”ning zamini, - dedi Prezident. Mazkur markaz ishga tushishi natijasida davlat idoralarining ma’lumotlarni saqlash va texnik qo‘llab-quvvatlashga sarflaydigan milliardlab xarajatlari tejaladi, aholi va tadbirkorlarga ko‘rsatilayotgan xizmatlar sifati yaxshilanadi. Eng asosiysi, kiberhujumlardan ishonchli himoya ta’minlanadi.

O‘zbekiston Respublikasining 2022-yil 15-iyun kungi “Qo‘riqlash faoliyati to‘g‘risida”gi O‘RQ 778-sonli Qonuniga muvofiq, Milliy gvardiyaga qo‘riqlash faoliyati sohasida davlat siyosatini amalga oshirish, o‘zining qo‘riqlash xizmatlari tariflarini tasdiqlash, davlat, ayniqsa o‘ta muhim, toifalangan va boshqa obyektlarni, jismoniy va yuridik shaxslarning mol-mulkini, xorijiy davlatlar hamda xalqaro tashkilotlarning diplomatik, konsullik va boshqa vakolatxonalarini qo‘riqlashni amalga

oshirish vakolatlari berildi. Qolaversa, so‘nggi yillarda respublikada davlat obyektlari, o‘ta muhim, toifalangan va boshqa obyektlarni samarali qo‘riqlashni tashkil etish, jismoniy va yuridik shaxslarning mol-mulkini ishonchli himoya qilish yuzasidan qator chora-tadbirlar amalga oshirildi.

Obyektlarining xavfsizlik tizimida muhandislik-texnik qo‘riqlash vositalari asosiy o‘rinni egallaydi. Muhandislik-texnik qo‘riqlash vositalarisiz xavfsizlik tizimi oqsaydi va qo‘riqlash xizmatini tashkil etish uchun juda katta kuch talab etiladi. Boshqa tomondan olib qaraydigan bo‘lsak ortiqcha va qiyinlashtirilgan muhandislik-texnik qo‘riqlash vositalari inson omiliga qo‘llashga to‘liq o‘z ta’sirini ko‘rsata olmaydi. Bundan tashqari murakkab tizimlarni ta’mirlash uchun yuqori malakali mutaxassislarni jalb etishga to‘g‘ri keladi.

Xavfsizlikni ta’minlashda qo‘riqlash texnikalariga video kuzatuv vositalari va signalizatsiyalar kiradi. Ular ham o‘z qatorida bir qator turlarga bo‘linadi.

Xavfsizlik, yong‘in signalizatsiya tizimlari, datchiklar, detektorlar, xabargichlar, bildirgichlar, signalizatsiyalar va boshqa xavfsizlik tizimlari kiradi. Masalan, trevogali signalizatsiya, harakat datchiklari, infraqizil detektorlar, tutun datchiklari, shisha sindiruvchi datchiklar, radioto‘lqin detektorlar, metall detektorlar, yong‘in datchiklari, vibratsion detektorlar, issiqlik detektorlari va h.klardan iborat.

Video kuzatuv vositalari va signalizatsiyalardan foydalanishning afzalliklari va kamchiliklari ham mavjud.

Avzalliklari: video kuzatuv vositalari va signalizatsiyalar obyektlarga o‘rnatilishidan maqsad inson omillarini kamaytirishdan iboratdir. Ya’ni toifalangan obyektlarda, davlat idoralarida, harbiy va davlat obyektlarida xavfsizlikni ta’minlashda qo‘riqlash texnikalari juda katta ko‘lamli ishni amalga oshiradi. Ya’ni har xil turdagi jinoyatlarni oldini olish va sodir etilgan jinoyatlarni aniqlashga yordam beradi.

Kamchiliklari: video kuzatuv vositalari va signalizatsiyalar elektr energiyasi bilan ishlashida, issiq va sovuqda, qor va yomg‘irda nuqsonlar paydo bo‘lishida.

Obyektlar himoyasi mustahkamligini oshirish va qorovullar shaxsiy tarkibi sonini kamaytirish maqsadida texnik qo‘riqlash vositalari qo‘llaniladi. Bularga quyidagilar kiradi: perimetrik topish vositalari, obyektni qo‘riqlash signalizatsiyasi, ogohlantiruvchi va ta’sir etuvchi texnik vosita, yong‘in signalizatsiyasi, texnik qo‘riqlash vositalari signallarini qabul qiluvchi apparat va radiotarmoq signalizatsiyasi.

Quyidagi hollarda texnik qo‘riqlash vositalarini qo‘llash bilan mustahkam himoyaga erishish mumkin: texnik qo‘riqlash vositalari to‘g‘ri tanlanganda va ulardan muhandislik to‘siqlari bilan kompleks holda foydalanilganda; himoya vositalarini o‘rnatish ishlari sir saqlangan holda olib borilganda; ular o‘z joyiga sifatli o‘rnatilganda; holidan xabar olib turganda va nazorat qilib turilganda; texnik qo‘riqlash vositalari ishlagan chog‘da qorovul shaxsiy tarkibi xushyor va o‘z vaqtida harakat qilganda.

Ilg‘or xorijiy tajriba asosida qo‘riqlash faoliyatiga zamonaviy axborot-kommunikatsiya tizimlari joriy qilinishi natijasida O‘zbekiston Respublikasi Milliy gvardiyasi qo‘riqlash xizmati tomonidan jismoniy va yuridik shaxslarning qo‘riqlashga olingan obyektlari soni so‘nggi ikki yilda 15 foizga oshdi.

Obyektlarga o‘rnatiladigan texnik qo‘riqlash vositalarining turi va miqdori qo‘riqlanayotgan obyektning ahamiyatiga (muhimligiga) bog‘liq: birinchi kategoriyali obyektlarga - ikki yoki undan ortiq chiziqli perimetrik topish vositasi, obyekt qo‘riqlash signalizatsiyasi va boshqa vositalar; ikkinchi kategoriyali obyektlarga - bir chiziqli perimetrik topish vositasi va obyekt qo‘riqlash signalizatsiyasi; uchinchi kategoriyali obyektlarga - obyekt qo‘riqlash signalizatsiyasi o‘rnatiladi.

Xulosa qilib aytganda, Milliy gvardiyasi bo‘linmalarida axborot xavfsizligi hamda obyektlar xavfsizligini ta’minlashda axborot texnologiyalari va texnik qo‘riqlash vositalari bilan jihozlangan qurol-aslaxa, o‘q-dori omborlari va doimiy nazorat, mustahkam himoya talab qiladigan boshqa obyektlar soqchi qo‘yish bilan qo‘riqlanadi. Texnik qo‘riqlash vositalarining signallarini qabul qiladigan apparatni qorovul boshlig‘i yoki uning yordamchisi (tarqatuvchi) nazorat qiladi.

Nazorat qo‘riqlash guruhining navbatchiligi operator tomonidan texnik qo‘riqlash vositalari signallarini qabul qiladigan apparatlarni muntazam nazorat qilish, texnik qo‘riqlash vositalari o‘z-o‘zidan ishlab ketganda nazorat qo‘riqlash guruhi postlari va ularning doimiy tayyorgarligini kundalik tekshiruvdan o‘tkazishdan iboratdir.

Foydalanilgan adabiyotlar:

1. Achilov F.B.va boshqalar. Texnik qo‘riqlash vositalariga texnik xizmat ko‘rsatish: – T.: O‘zbekiston Respublikasi MG HTI, 2019.

2. U.A.Yoqubov, A.N.Dadaboyev. Obyektlar xavfsizligini tizimli ta’minlash konsepsiyasi. -T.: O‘zR MG HTI, 2018.

3. Lex.uz -normativ huquqiy hujjatlar portal

4. Fayllar.org – internet portal

5. Infocom.uz- internet portal

6. www.ictnews.uz sayti.

OMMAVIY TARTIBSIZLIKLARNING OLDINI OLISHDA PROFILAKTIK CHORA-TADBIRLARNING AHAMIYATI

Jalolov A.A.
O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti
Axborot texnologiyalari kafedrasi o‘qituvchisi

Ayrim xorijiy davlatlarda vujudga kelayotgan murakkab siyosatlar ommaviy tartibsizliklarning kelib chiqishiga sabab bo‘lmoqda. Gap shundaki, jamiyatda yuz berayotgan demokratik o‘zgarishlar davrida ommaviy xarakterga ega bo‘lgan mitinglar, yurishlar, demonstratsiyalar, aksiyalar va noroziliklar juda ommaviylashib ketmoqda.

Ushbu sharoitlarda negativ xarakterga ega bo‘lgan ommaviy xodisalar, xususan, ommaviy tartibsizliklarning jamiyatda keng tarqalishi kuzatilmoqda. Prezidentimiz ta’biri bilan aytganda, “...aholining tinch va osoyishta hayotini ta’minlash, jinoyatchilik va huquqbuzarliklarga qarshi kurashish, jamoat tartibini saqlash – hozirgi kunda eng muhim vazifadir” [1].

Hozirda dunyoning qit’a va mintaqalarida, olis va yaqin atrofimizdagi ba’zi davlatlarda qarama-qarshilik, ziddiyatlar tobora

kuchayib borayotganligining guvohi bo‘layapmiz. Ayrim mintaqalarda qon to‘kilayotgani, nizo va adovatlar avj olayotgani, millatchilik, shovinizm, kabi xavfli ofatlar maydonga chiqayotgani, bir so‘z bilan aytganda, vaziyat tobora keskinlashib, xavf-xatarlar ortib borayotgani barchamizni tashvishga solmasdan qo‘ymaydi. Dunyoga xavf solayotgan tahdidlar bugungi kunda juda serqirra bo‘lib, endilikda u biror-bir davlat yoki mintaqa bilan chegaralanib qolayotgani yo‘q. Chunonchi, bugungi kunda tahdid xalqaro terrorizm, radikalizm, siyosiy va diniy ekstremizm, millatchilik, etnik hamda millatlararo nizolar, transmilliy jinoyatlar, shuningdek, fitna va bo‘xtonlar uyushtirish orqali keng ommani huquqbuzarliklar va jinoyatlar sodir etishga undash, olomon yordamida “urush bilan bog‘liq bo‘lmagan usullar”ni qo‘llab, hokimiyat tepasiga chiqish kabi muammolarni o‘z ichiga oladi.

Ommaviy tartibsizliklarga qarshi kurash fuqarolarimiz va shu qatorda huquqni muhofaza qiluvchi idoralarning qat’iy burchidir. Huquqni muhofaza qilish organlari davlat manfaatlari, fuqarolarning hayoti va insoniy qadr-qimmati, konstitutsiyaviy huquqlari va erkinliklarini ommaviy tartibsizlik kabi jinoiy tajovuzlardan himoya qilishga doimo shay turishlari darkor.

Vatanimiz rivojlanishi, gullab-yashnashi va ravnaqi uchun, albatta, hech qanday yovuz kuch raxna solmasligi kerak. Buning uchun barcha huquqni muhofaza qiluvchi organlar, ayniqsa, O‘zbekiston respublikasi Milliy gvardiyasi va IIV xodimlari aholi bilan profilaktik tadbirlarni olib borishlari va, albatta, noqonuniy ommaviy tadbirlar davomida tartibsizlik keltirib chiqarish yomon oqibatlarga olib kelishi bo‘yicha tushuntirish ishlarini muntazam olib borishlari hamda bu borada aholining huquqiy bilimlarini oshirib borishlari zarur.

Ommaviy tartibsizliklarning kelib chiqish sabablari va ularni oldini olishda profilaktik chora tadbirlarni ahamiyatiga to‘xtalishdan oldin ommaviy tartibsizliklar tushunchasiga ta’rif berib o‘tish maqsadga muvofiqdir.

Ommaviy tartibsizliklar deganda, davlatning suvereniteti, jamoat tartibi va xavfsizligi, fuqarolarning shaxsiy xavfsizligiga ta’sir qiluvchi

ommaviy jinoyat sifatida, zo‘rlash, o‘t qo‘yish, buzg‘unchilik, davlat va shaxsiy mulkni o‘g‘irlash, talash va yo‘q qilish, tinch aholi va hukumat kuchlariga nisbatan sovuq (o‘q otar) qurol, portlovchi yoki tez alanga oluvchi moddalarni tayyorlash va qo‘llash, qarshilik ko‘rsatish, davlat, jamoat tashkilotlari va muassasalari, transport vositalari faoliyatini izdan chiqarish va bu vaziyatda ularni bartaraf etish uchun keskin chora-tadbirlarni qo‘llashga majbur qiluvchi hodisalar tushuniladi [2].

Respublikamiz qonunchiligida ommaviy tartibsizliklar hokimiyat, boshqaruv va jamoat birlashmalari organlarining faoliyat tartibiga qarshi jinoyatlar turkumiga kiritilgan bo‘lib, bu jinoyat turi qattiq qoralanadi va Jinoyat kodeksining 244-moddasida* o‘z aksini topgan.

O‘zbekiston Respublikasi Jinoyat kodeksining 244-moddasiga asosan, qurol yoki qurol sifatida foydalanadigan boshqa narsalarni ishlatib yoxud ishlatish bilan qo‘rqitib shaxsga nisbatan zo‘rlik ishlatish, qirg‘in solish, o‘t qo‘yish, mulkka shikast yetkazish yoki nobud qilish, hokimiyat vakiliga qarshilik ko‘rsatish orqali ommaviy tartibsizliklar tashkil qilish, shuningdek, ommaviy tartibsizliklarda faol qatnashish - o‘n yildan o‘n besh yillargacha ozodlikdan mahrum qilish bilan jazolanadi.

Ommaviy tartibsizliklar hukumat boshqaruvi organlari faoliyatini izdan chiqarish, jamoat tartibini keng qamrovli buzish, jamoat xavfsizligini tahdid ostida qoldirish, insonlar qurbon bo‘lishi, davlat (jamiyat, shaxs)ga jiddiy iqtisodiy zarar keltirishi bilan ijtimoiy xavflidir. Ommaviy tartibsizliklarning tahlillari shuni ko‘rsatadiki, bu xavfli jinoyat jamiyat asosini yemiradi, vaziyat barqarorligi, fuqarolarning normal hayotini, korxona, muassasa va tashkilotlarning ishini buzadi.

Ko‘p sonli olomonning kriminal harakati odatga ko‘ra, tajovuzkorlik, o‘zaro ta’sirchanlikning kuchliligi, ehtiroslarning jo‘shqinligi bilan kuzatiladi.

Ma’lumki, ommaviy tartibsizliklarning ishtirokchilari, ularning noqonuniy xatti-harakatlarining ko‘lami, moddiy oqibatlari haqidagi aniq ma’lumotlar hamma vaqt mavjud bo‘lavermaydi, bu esa ushbu jinoyatga qarshi kurash imkoniyatlarini qisman cheklab qo‘yadi. Yuqoridagilarni inobatga olgan holda ommaviy tartibsizliklarni turli zo‘ravonlikda

ifodalangan, jamiyatga va fuqarolarning shaxsiy xavfsizligiga real xavf soluvchi ommaning harakatlari deb tushunish mumkin.

Ommaviy tartibsizliklarning sinflanishi va psixologiyasi

Biror-bir hodisa yoki jarayonni chuqur o‘rganish uchun, avvalambor, uning o‘ziga xosligi, alomatlari va mexanizmini keng tadqiqot qilish zarur bo‘ladi.

Ommaviy tartibsizliklarni ham uning tabiatini to‘liq tahlil qilish orqali bilib olish mumkin. Tahlilni ommaviy tartibsizliklarning sinflanishini o‘rganishdan boshlash maqsadga muvofiqdir.

Ommaviy tartibsizliklarning sinflanishining asosiy mezonlarini, uning vujudga kelish alomatlari va oqibatlari tashkil etadi.

Ommaviy tartibsizliklar davomidagi jinoiy xatti-harakatlar ikki turga bo‘linadi: umumiy; o‘zgacha. Muassasalar, do‘konlarni vayron qilishga qaratilgan buzg‘unchiliklar, transport vositalarini yo‘q qilish, o‘t qo‘yish va boshqa shunga o‘xshash harakatlar ommaviy tartibsizliklarning umumiy alomatlarini belgilab beradi. O‘zgacha ommaviy tartibsizliklar esa fuqarolarning xonadonlariga bosqinchilik qilishda ifodalanadi.

Yuqoridagilarni hisobga olgan holda ommaviy tartibsizliklarni quyidagi sinflarga bo‘lish asosli:

1. Vujudga kelish sabablariga ko‘ra: a) siyosiy; b) jtimoiy-iqtisodiy; v) milliy (irqiy); g) diniy; d) ekologik.

2. Xarakteriga ko‘ra: a) umumiy (davlat idoralari, muassasalari, tashkilotlarini vayron qilish); b) fuqarolarning shaxsiy mulkiga tajovuz qilish (xonadonlarni vayron qilish)

3. Kelib chiqish oqibatining og‘irligiga ko‘ra: a) odamlarga har xil turdagi tan jarohati yetkazilishi; b) insonlarning o‘limiga olib kelishi; v) katta moddiy zarar yetkazilishi.

4. Vujudga kelish joyiga ko‘ra: a) aholi yashash punktlarida; b) davlat korxonalari va tashkilotlarida; g) ijtimoiy-siyosiy, madaniy, ommaviy sport, ko‘ngilochar-tomosha, umumxalq, diniy, kasbiy va boshqa tadbirlarni o‘tkazish joylarida; d) ozodlikdan mahrum qilish turidagi jazoni ijro etish muassasalarida.

5. Davomiyligiga ko‘ra: a) uzoq muddatli, b) qisqa muddatli.

6. Qatnashuvchilar soniga koʻra: a) 100 kishigacha, b) 1000 kishigacha, v) 10000 kishigacha, g) 10000 kishidan ortiq.

Ommaviy tartibsizliklar sodir etilishi mumkin:

– davlat boshqaruvi (huquqni muhofaza qilish) organlari obyektlari, xorijiy davlatlar elchixonalari yonida;

– aholi punktlari (koʻchalar, sayilgohlar, maydonlar, bozorlar)da;

– davlat, madaniy, ommaviy sport tadbirlarini oʻtkazish davomida;

– yirik sanoat obyektlari (zavodlar, fabrikalar)da;

– jazoni ijro etish muassasalari (turmalar, koloniyalar, tergov xibsxonalari va qamoqxonalar)da va h.k.

Miting – biror-bir muhim voqea, siyosiy, ijtimoiy-iqtisodiy masalalarni hal etish uchun oʻtkaziladigan yigʻilish. Miting deyilganda, odatda, bayramona kayfiyatda yoki davlat hokimiyat organlaridan norozi boʻlgan ma'lum bir siyosiy guruhning yoki ommaviy harakat yoxud ishlab chiqarish tashkilotlarining shahar markazlariga chiqib, oʻz fikr va talablarini bildirishi tushuniladi [3].

Yigʻilishlar erkinligi – fuqarolarning asosiy siyosiy huquqlaridan biri, yopiq binolarda toʻplanishning cheklanmagan imkoniyatlarini ifodalaydi, unga kirish aslida uni tashkil etganlar tomonidan cheklanishi mumkin. Qonunchilik yigʻilishlar oʻtkazishning oshkor qilish tartibini nazarda tutishi mumkin, bunda vakolatli organlar boʻlajak yigʻilish, uning oʻtkazilish vaqti, joyi va mavzusi toʻgʻrisida oldindan xabardor qilinadi, ammo hech qanday xabar berish talab etilmasligi ham mumkin [4].

Namoyish – fuqarolar guruhlarining plakatlar, transparant va b. koʻrgazmali tashviqot vositalaridan foydalangan holda jamoaviy kayfiyatni tashkiliy-ommaviy bildirish. Ommaviy tadbirlarning bir koʻrinishi hisoblanadi. Namoyishlar erkinligi fuqarolarning asosiy konstitutsiyaviy siyosiy erkinliklaridan biridir [5].

Ammo, shu oʻrinda, ushbu ommaviy toʻplanishlar koʻcha tartibsizliklariga aylanib ketayotganligi ham kuzatilmoqda. Ma'lum darajada bu ommaviy tartibsizliklarning bir koʻrinishidir.

Bosh qomusimizda fuqarolarimizning oʻz ijtimoiy faolliklarini Oʻzbekiston Respublikasi qonunlariga muvofiq mitinglar, yigʻilishlar va

namoyishlar shaklida amalga oshirish huquqiga ega ekanligi, bunda hokimiyat organlari faqat xavfsizlik nuqtai nazaridangina bunday tadbirlar o‘tkazilishini to‘xtatish yoki taqiqlash huquqiga egaligi mustahkamlangan [6].

Ommaviy tartibsizliklarni va guruhiy tartibbuzarliklarning oldini olish deganda bevosita ommaviy tartibsizliklarni keltirib chiqaruvchi ziddiyatli holatlarni o‘z vaqtida bartaraf etishni tushunamiz.

Ichki ishlar organlari va ularning boshliqlari ommaviy tartibsizliklarni oldini olish bo‘yicha quyidagi tadbirlarni amalga oshirishlari lozim:

1. Dastlabki profilaktika.

2. Yolg‘on va ig‘vo mish-mishlar paydo bo‘layotgan vaqtda ularning oldini olish.

3. Ommaviy tartibsizliklarda olomon paydo bo‘lishi, sababchilarini zo‘rlab ishlatishga chorlovlari va alohida huquqbuzarlar hamda qonunni himoya qiluvchi kuchlar o‘rtasida paydo bo‘lgan kichik ziddiyatlarni vaqtida bartaraf etish.

4. Ommaviy tartibsizliklarning faol a’zolarini maxsus tadbirlar o‘tkazib qo‘lga olish va ommaviy tartibsizliklarni bartaraf etish.

5. Bo‘lib o‘tgan ommaviy tartibsizliklarning sabab va sharoitlarini aniqlash hamda qayta sodir bo‘lishini oldini olish.

Ommaviy tartibsizliklarni oldini olishning bosh omili bo‘lib, profilaktik xarakterdagi maxsus tadbirlarni ishlab chiqish va amalga oshirishi hisoblanadi. Ularni ishlab chiqish va amalga oshirish hududdagi operativ vaziyatning tahlili, jamoatchilikning Ichki ishlar organlari faoliyati to‘g‘risidagi va vujudga kelgan vaziyat, ya’ni ziddiyatli ommaviy tartibsizliklarga sabab bo‘luvchi vaziyat haqidagi fikrini chuqur o‘rganish asosida amalga oshiriladi.

Ichki ishlar organlarining rahbarlari amalga oshiradigan zaruriy profilaktika tadbirlarini ikki guruhga yig‘ib ishlab chiqadi:

– yuqori turuvchi organlar tomonidan amalga oshiriladigan tadbirlar;

– boshqa davlat boshqaruv organlari, korxona, muassasalar tomonidan amalga oshiriladigan va bevosita bajariladigan tadbirlar.

Birinchi guruh tadbirlari bo‘yicha. Ichki ishlar organlari tegishli yuqori turuvchi organlarni axborot bilan ta’minlab, tegishli aniq takliflarni kiritishlari lozim. Masalan, hokimiyat boshqaruv organlariga jinoyatchilik va jamoat tartibini holati, jinoiy va ma’muriy javobgarlikka tortilgan shaxslar, ichkilikbozlik, giyohvandlik va voyaga yetmagan shaxslar orasidagi jinoyatchilik holati to‘g‘risidagi ma’lumotlarni taqdim qilishlari lozim. Shu bilan birga, Ichki ishlar organlarining rahbarlari tuman, shahar, viloyat deputatlari kengashlariga hududdagi profilaktika ishlarining tashkil qilinganligi to‘g‘risida ma’lumot berishlari va uni takomillashtirish bo‘yicha aniq takliflarni ishlab chiqib taqdim etadilar.

Ikkinchi guruh tadbirlari bo‘yicha:

– jinoyatchilikka qarshi kurash va jamoat tartibini saqlash bo‘yicha faoliyatni kuchaytirish, shu jumladan, voyaga yetmagan shaxslar orasida profilaktika ishlarini olib borish, “ko‘cha”da sodir etiladigan jinoyatlarga qarshi kurashni kuchaytirish, operativ pozitsiyalarni mustahkamlash, yoshlar to‘planadigan jamoat joylarida tungi klublar, diskotekalar, billiardxonalar, sport markazlari doimiy ravishda agentura ma’lumotlarini o‘rganishni tashkil qilish, ya’ni vujudga kelishi mumkin bo‘lgan ziddiyatlar xususidagi ma’lumotlarni tahlil qilish, ushbu masalalar bo‘yicha doimiy ravishda agentura so‘rovini o‘tkazib turish, agentura va ishonchli shaxslar orqali bunday salbiy ziddiyatlarni tashkil qiluvchi shaxslarni aniqlash bo‘yicha tadbirlar o‘tkazish, PPX xodimlari faoliyatini samaradorligini oshirish, ularni fuqarolarning arizalariga munosabatini nazorat qilish, og‘ir jinoyatlarni o‘z vaqtida ochish.

– jamoatchilik va davlat organlari o‘rtasida aloqani mustahkamlash, operativ vaziyatni barqarorlashtirishda ommaviy axborot vositalari orqali Ichki ishlar organlarining jinoyatchilikka qarshi kurash faoliyatini aks ettiruvchi ko‘rsatuv, eshittirish, maqolalarni tayyorlash va jamoatchilikka namoyon etish, Ichki ishlar organlarining rahbarlari, jamoatchilik o‘rtasida davra suhbatlarini o‘tkazish kabilardir.

Ommaviy tartibsizliklar vaqtida shaxsiy tarkibni doimiy tayyorgarligini ta’minlash (guruhiy tartibbuzarliklar va ommaviy tartibsizliklar vaqtida harakat qilish uchun maxsus rejalarni ishlab chiqish, kuch va vositalarni hisobga olish, operativ shtablar tuzish va ularning ish

faoliyatini tashkil qilish, trevoga signali bo‘yicha shaxsiy tarkib tayyorgarlik tizimini va ular bilan aloqani tekshirish, qo‘l ostidagi xodimlarni ommaviy tartibsizliklar vaqtida o‘tkaziladigan harakatlarga o‘rgatish, ommaviy tartibsizliklarga xodimlarni psixologik jihatdan tayyorlash, xodimlar orasida g‘oyaviy-siyosiy targ‘ibot ishlarini va ularning jangovar tayyorgarligini oshirish, ya’ni boshqa huquqni muhofaza qiluvchi organlar bilan hamkorlikni ishlab chiqish).

Ichki ishlar organlarining moddiy-texnik bazasini mustahkamlash (Ichki ishlar organlari xizmat xonalari va binolarining muhofazalanganligini tekshirish, shu jumladan, oynalarga panjaralar o‘rnatilganligi, eshiklarga himoya bloklarini qo‘yilganligi, qurol-yaroq va texnik vositalarni saqlash xonalari va hokazolarni tekshirish, yuqori turuvchi organlari oldiga qurol-yaroq va texnik vositalar bilan ta’minlash bo‘yicha hisobotlar va takliflar tayyorlash).

Ichki ishlar organlari rahbarlari yuqoridagi tadbirlarni ishlab chiqishda va ular orasidan zarurlarini amalga oshirishda bevosita qatnashadilar.

Agarda dastlabki profilaktika bosqichida kerakli natijaga erishish imkoniyati bo‘lmasa, ommaviy tartibsizliklarni bartaraf etish profilaktikasini amalga oshirish bo‘yicha keyingi tadbirlar ishlab chiqiladi.

O‘z vaqtida bartaraf etilmagan siyosiy yo‘sindagi ommaviy tartibsizliklar:

• qurolli to‘qnashuvlarga;

• fuqarolar urushiga;

• davlatda o‘rnatilgan konstitutsion tuzumni ag‘darilishi va boshqa holatlarni keltirib chiqarishi mumkin.

Ijtimoiy-siyosiy beqarorlik, notinchlik belgilariga quyidagilar kiradi: tajovuzkorlik, aqidaparastlik, diniy ekstremizm, islom fundamentalizmi, davlat shovinizmi, millatchilik, agressiv millatchilik, korrupsiya va jinoyatchilik, mahalliychilik va urug‘-aymoqchilik, shuningdek, o‘z siyosatini, ta’sirini o‘tkazish va hukmronlik qilishga urinayotgan kuchlar, terrorizm va hokazo.

Qonunchiligimizda kabi dinimizda ham haddan oshish, tajovuzkorlik, zo‘ravonlik qattiq qoralanadi. Islom ta’limoti buzg‘unchilikni, odamlar qalbiga vahima, dushmanlik va fitna urug‘larini sochishni qattiq qoralaydi. Ma’lumki, so‘nggi yillarda dinni o‘zlariga niqob qilib olgan oqimlar, toifalar paydo bo‘ldi. Ular g‘arazli maqsadlari yo‘lida jamiyatda buzg‘unchilik, begunoh odamlarning qonini nohaq

to‘kish kabi jinoyatlarni avj oldirib, fuqarolar tinchligini buzib, xalq orasida nizo chiqarishga harakat qilishmoqda.

Ommaviy tartibsizliklarning tahlili shuni ko‘rsatadiki, bu og‘ir jinoyat turi hisoblanib, jamiyat asoslarini izdan chiqaradi, vaziyatni beqarorlashtiradi, xavf-xatar tug‘diradi, fuqarolar, korxonalar, tashkilotlar va muassasalarning faoliyatini ishdan chiqaradi. Ommaviy tartibsizliklarga qarshi kurashish masalalarida davlat idoralari va huquq-tartibot organlari harakatsizlik va sovuqqonlikka yo‘l qo‘ymasligi talab qilinadi.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasi Prezidenti Shavkat Mirziyoyevning xalq deputatlari Xorazm viloyati Kengashining navbatdan tashqari sessiyasidagi nutqi // “Xalq so‘zi”. – 2017. – 15 okt.
2. Багмет, Анатолий Михайлович. “Массовие беспорядки как уголовноправовое понятие”. Власт и управление на Востоке России 3 (2012): 124–126.
3. Хохрин С.А. Массовие беспорядки: проблема определения понятия // Вестник Владимирского юридического института. – 2009. – №. 4. – С. 160–161.
4. O‘zbekiston yuridik ensiklopediyasi / Nashr uchun mas’ul R.A. Muhitdinov va boshq.; mas’ul muharrir N. Toychiyev. – T.: Adolat, 2010. – B. 704, 234.
5. Xoxrin S.A. Массовие беспорядки, совершаемие осужденними в исправителних учреждениях (уголовно-правовой и криминологический аспекти) // Уголовно-правовой и криминологический аспекти): дис... канд. юрид. наук. – 2011. – Т. 12. – № 08.
6. O‘zbekiston Respublikasi Konstitutsiyasi, 33-modda. Toshkent Adolat 2019 yil.
7. 12.https://www.researchgate.net/publication/360280222_Ommavij_tartibsizliklarning_oldini_olisda_profilaktik_cora-tadbirlarning_aamiati
8. 13. www.press-service.uz.
9. 14. “Xalq so‘zi” gazetasi – www.ihfo.xs.uz.
10. http://akadmvd.uz (O‘zbekiston Respublikasi IIV Akademiyasi).
11. http://www.tsul.uz (Toshkent davlat yuridik universiteti).
12. http://www.ziyonet.uz (Axborot ta’lim tarmog‘i).
13. www.bilim.uz.

UCHUVCHISIZ UCHISH APPARATLARIDA VIDEOAXBOROT UZATISH TEXNOLOGIYALARINING RIVOJLANISH TENDENSIYALARI.

Ziyayev B.N.
O‘R JXU magistratura tinglovchisi

Bugungi kunda uchuvchisiz uchish apparatlari (UUA) turli sohalarda – harbiy, qutqaruv, geodeziya, qishloq xo‘jaligi va fuqarolik sohalarida keng qo‘llanilmoqda. Ayniqsa, joriy vaqt rejimida videoaxborotlarni uzatish imkoniyati ularning samaradorligini yanada oshirmoqda. Video ma’lumotlarni uzatishda yuqori sifat, tezkorlik, xavfsizlik va ishonchlilik asosiy talablardan biri hisoblanadi. Shu bois, bu yo‘nalishda zamonaviy kommunikatsiya texnologiyalari (4G/5G tarmoqlari, IoT, Wi-Fi 6), sun’iy intellekt algoritmlari va ma’lumotlarni shifrlash usullari keng tadbiq etilmoqda.

Ushbu tezisda UUAda videoaxborot uzatish texnologiyalarining rivojlanish tendensiyalari, mavjud muammolar va ularning yechimlari tahlil qilinadi. Shuningdek, kelgusida ushbu sohada qo‘llanilishi mumkin bo‘lgan yangi yechimlar haqida ham fikr yuritiladi.

Asosiy rivojlanish yo‘nalishlari

1. Tezlik va sifatning oshishi.

Ilgarigi analog tizimlar o‘rnini raqamli uzatish texnologiyalari egalladi. Hozirda HD va 4K sifatdagi videolar uzatilishi mumkin. 5G tarmoqlari latensiyani (kechikishni) juda kamaytirib, joriy vaqtda uzatish imkoniyatini oshirmoqda.

2. Sun’iy intellektdan foydalanish.

Neyron tarmoqlar orqali videoda shovqinni yo‘qotish, sifatni oshirish, obyektlarni aniqlash va kuzatish mumkin. Shu bilan operatorga tezkor va aniq axborot yetib boradi.

3. Xavfsizlikni ta’minlash.

Video ma’lumotlar shifrlash orqali uzatiladi. AES va RSA kabi kriptografik usullardan foydalanish dron ma’lumotlarini begona shaxslardan himoya qiladi.

4.Ko‘pkanalli uzatish.

Video ma’lumotlarni bir vaqtning o‘zida Wi-Fi, LTE, 5G va sun’iy yo‘ldosh orqali uzatish mumkin. Bu usul uzilishlarni kamaytiradi va uzatishning barqarorligini ta’minlaydi.

5. Qo‘llanish sohalarining kengayishi:

harbiy razvedka va chegara nazoratida;
tabiiy ofatlar paytida qutqaruv ishlarida;
obyektlarni qo‘riqlashda xavfsizlik monitoringida;
qishloq xo‘jaligida yer maydonlari va hosil holatini nazorat qilishda.

XULOSA

Uchuvchisiz uchish apparatlarida videoaxborot uzatish texnologiyalari jadal rivojlanmoqda. Yuqori tezlikdagi tarmoqlar, sun’iy intellekt va xavfsizlik mexanizmlari dronlardan foydalanish samaradorligini oshirmoqda. Kelajakda 6G va yanada kuchli sun’iy intellekt yordamida real vaqtda yuqori sifatli, xavfsiz va uzluksiz videouzatish imkoniyatlari yanada takomillashishi kutilmoqda.

Foydalanilgan adabiyotlar:

1. 3GPP TS 22.261. Service requirements for next generation new services and markets – 5G tizimlarining imkoniyatlari haqida hujjat.
2. ITU-R. IMT-2020 requirements for 5G networks. Xalqaro telekommunikatsiya uyushmasi tavsiyalari.
3. Stallings W. Cryptography and Network Security: Principles and Practice. Pearson, 2017.
4. Szeliski R. Computer Vision: Algorithms and Applications. Springer, 2022.
5. Redmon J., Farhadi A. Yolov3: An Incremental Improvement. arxiv:1804.02767,

QUROLLI KUCHLAR TIZIMIDA RAQAMLI TEXNOLOGIYALAR

Uzakov E.O.
Yusupov U.A.
Jamoat xavfsizligi universiteti kursanti
Jamoat xavfsizligi universiteti AT kafedrasi katta o‘qituvchisi

XXI asrda insoniyat taraqqiyotining eng muhim belgilaridan biri bu raqamli texnologiyalarning keng joriy etilishidir. Axborot-kommunikatsiya vositalarining rivojlanishi nafaqat kundalik hayot, balki davlat boshqaruvi, iqtisodiyot, ta’lim va tibbiyot sohalarini tubdan o‘zgartirib yubordi. Shu bilan birga, harbiy sohada ham raqamli texnologiyalar strategik ahamiyat kasb etmoqda. Zamonaviy urushlar tobora “axborot urushi” ko‘rinishini olmoqda, bunda kim tezroq va aniqroq

axborotga ega bo‘lsa, kim boshqaruvni samarali amalga oshira olsa, o‘sha tomon ustunlikka erishadi.

Qurolli kuchlar tizimida raqamli texnologiyalarni joriy etishning ahamiyati beqiyosdir. Avvalo, ular boshqaruv tizimini tezkor va samarali qiladi. Masalan, qo‘mondonlik markazlari elektron boshqaruv vositalari yordamida butun armiyani yagona tizim sifatida nazorat qila oladi. Ikkinchidan, razvedka va kuzatuv jarayonlari raqamli texnologiyalar orqali real vaqt rejimida amalga oshiriladi. Uchinchidan, logistika va ta’minot tizimlarida raqamli monitoring resurslarning aniq hisobini yuritishga yordam beradi. Shuningdek, kibermudofaa sohasida ham raqamli texnologiyalar dushman hujumlarini qaytarishning muhim kafolatidir.





Ammo imkoniyatlar bilan bir qatorda qator muammolar ham mavjud. Birinchidan, kiberxavfsizlik masalasi. Harbiy tarmoqlar raqamlashtirilgan sari ularga hujum qilish xavfi ortadi. Ikkinchidan, xorijiy texnologiyalarga qaramlik masalasi bor. Uskunalar va dasturiy ta’minotning katta qismi

import qilinadi, bu esa strategik jihatdan xavf tug‘dirishi mumkin. Uchinchidan, malakali kadrlar yetishmovchiligi seziladi. Zamonaviy raqamli tizimlar bilan ishlash uchun yuqori malakali mutaxassislar tayyorlash zarur.

Harbiy boshqaruv tizimlarida raqamli texnologiyalar

Qurolli kuchlarning samarali faoliyati, avvalo, boshqaruv tizimining to‘g‘ri tashkil etilishiga bog‘liq. Harbiy boshqaruv — bu qo‘mondonlikdan boshlab quyi bo‘g‘ingacha bo‘lgan jarayonlarni yagona markazdan muvofiqlashtirish, qarorlarni tezkor qabul qilish va ularni qisqa vaqt ichida ijroga yo‘naltirish tizimidir. Zamonaviy sharoitda ushbu jarayonni samarali amalga oshirish raqamli texnologiyalarsiz deyarli imkonsiz hisoblanadi.

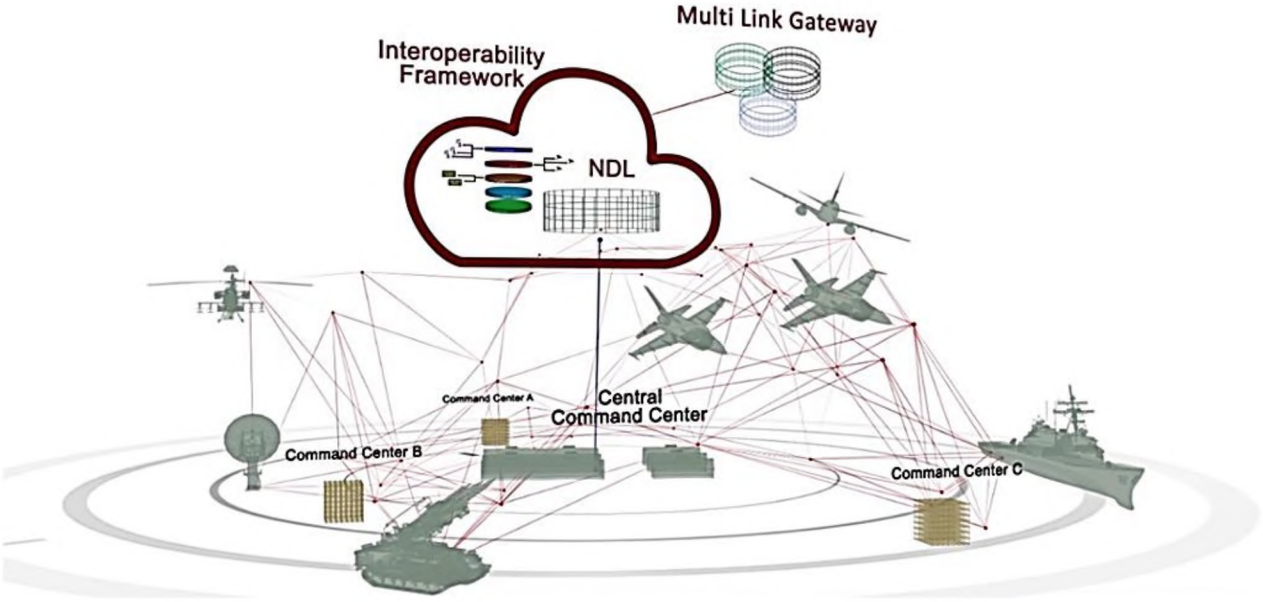




Raqamli texnologiyalar harbiy boshqaruvda uchta asosiy vazifani bajaradi. Birinchidan, tezkorlikni ta’minlaydi. Masalan, elektron boshqaruv tizimlari yordamida qo‘mondonning buyruqlari bir necha soniya ichida butun bo‘linmalarga yetkazilishi mumkin. Bu jangovar sharoitda ustunlikni qo‘lga kiritishda hal qiluvchi ahamiyat kasb etadi.

Ikkinchidan, aniqlik va ishonchlilikni kafolatlaydi. Axborot texnologiyalari orqali resurslar, qo‘shinlarning joylashuvi va vaziyat haqidagi ma’lumotlar avtomatik tarzda qayd etilib, inson omilidan kelib chiqadigan xatoliklarni kamaytiradi. Uchinchidan, muvofiqlashtirishni kuchaytiradi. Quruqlik, havo va dengiz kuchlari yagona elektron tizimda faoliyat yuritib, murakkab operatsiyalarni birgalikda olib borishi mumkin.

Raqamli boshqaruv tizimlarining yana bir afzalligi bu simulyatsiya va modellashtirish imkoniyatlaridir. Maxsus dasturiy ta’minotlar yordamida turli jangovar vaziyatlar oldindan tahlil qilinadi va qo‘mondonlar optimal qarorlarni ishlab chiqishi mumkin. Bu urush va mojarolarda talafotlarni kamaytirishga yordam beradi.



Shu bilan birga, raqamli boshqaruv tizimlari bilan bog‘liq muammolar ham yo‘q emas. Eng asosiy xavf bu kiberhujumlardir. Agar boshqaruv tarmog‘i dushman tomonidan buzilsa, butun qo‘shinlarning harakati izdan chiqishi mumkin. Shuningdek, xorijiy dasturiy ta’minotga qaramlik strategik xavfni oshiradi. Shu sababli milliy platformalarni ishlab chiqish va kuchli kiberxavfsizlik choralarini ko‘rish zarur.

Razvedka va kuzatuv tizimlarida raqamli texnologiyalar

Bugungi qurolli kuchlar tizimida razvedka va kuzatuv (intellegens va surveillans) faoliyatining samaradorligi raqamli texnologiyalar bilan

chambarchas bog‘liq. Shu asosda sun’iy yo‘ldoshlar, dronlar (uchuvchisiz uchish apparatlari), videokuzatuv kameralar va turli sensor tizimlari muhim rol o‘ynaydi. Ularning barchasi real vaqt rejimida ma’lumot yig‘ish va tahlil qilish imkonini beradi, bu esa qo‘mondonlikka tez va aniq qarorlar qabul qilishga katta yordam beradi.

Sun’iy yo‘ldoshlar. Sun’iy yo‘ldoshlar razvedka faoliyatida uzun masofali kuzatuv va global qamrovdagi nazorat uchun ishlatiladi. Masalan, 2023-yilda AQSh orbitada 247 harbiy sun’iy yo‘ldoshga ega bo‘lganligi ma’lum: ularning tamomiga razvedka va aloqa maqsadlarida ishlatiladi.



Rossiya ham 160 ga yaqin harbiy sun’iy yo‘ldoshga ega ekani aytiladi.

Sun’iy yo‘ldoshlar yuqori aniqlikdagi tasvirlar, radarlarga asoslangan kuzatuv, elektron kashfiyot vositalari bilan jihozlanadi. Ular geografik joylashuv, dushman kuchlari harakati, strategik obyektlar holati haqida ma’lumot bera oladi. Bu ma’lumotlar yer yuzida joylashgan qo‘shinlar va uchuvchisiz tizimlarga taqdim qilinadi.

Uchuvchisiz uchish apparatlari (dronlar) — razvedka va kuzatuv sohasida eng keng tarqalgan vositalardan biridir. Joriy bozor ma’lumotlariga ko‘ra, harbiy dronlar bozorining qiymati 2024-yilda taxminan USD 15,23 milliard bo‘lgan va 2030-yilgacha USD 22,81

milliardgacha o‘sishi kutilmoqda (yillik o‘sish sur’ati ~7,6 %) Boshqa bir hisobot bo‘yicha esa 2023-yilda bu bozor USD 14,14 milliard sifatida baholangan va 2032-yilgacha USD 47,16 milliardgacha ko‘tarilishi prognoz qilingan. Ushbu statistikalar shuni ko‘rsatadiki, harbiy dronlar va ular bilan bog‘liq razvedka vositalari tez sur’atda rivojlanmoqda va davlatlar tomonidan katta resurslar ajratilmoqda.

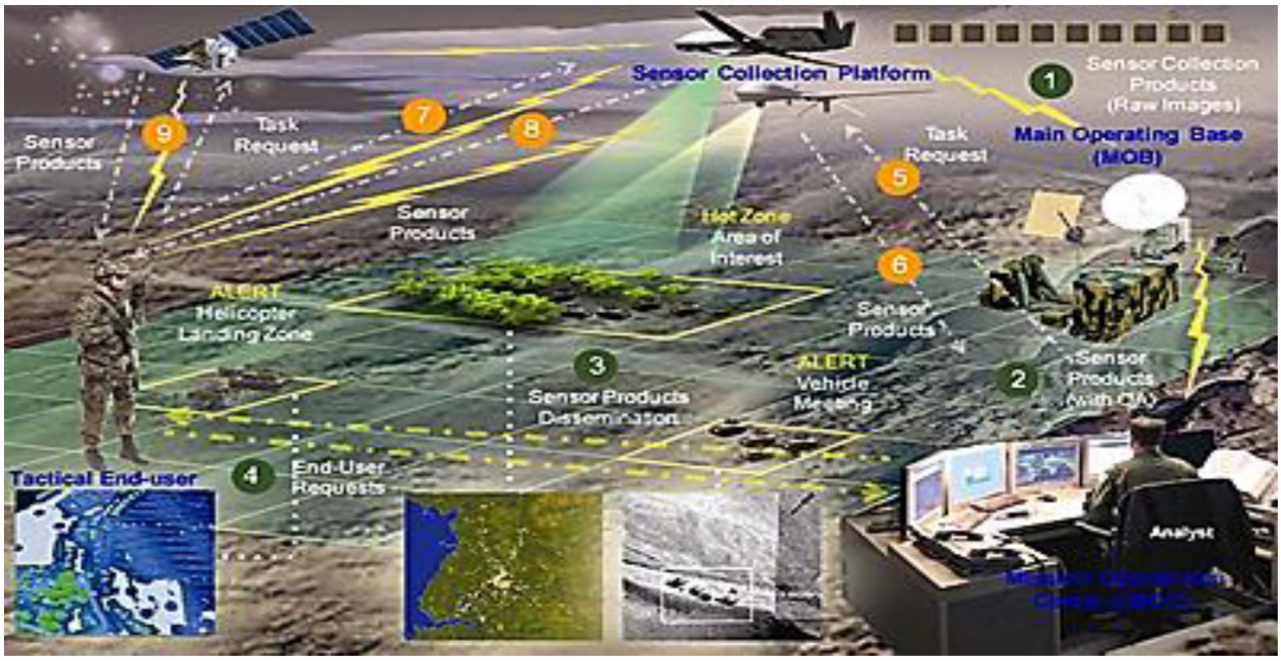


Dronlar har xil tipda bo‘lishi mumkin: kichik taktik dronlar (qo‘shin bo‘linmalari darajasida), o‘rta va uzoq masofali dronlar, shuningdek, qurolga ega bo‘lgan dronlar (UCAV – Unmanned Combat Aerial Vehicles). Ular kameralar, infraqizil sensörlar, radarlarga ega bo‘lishi mumkin.

Videokuzatuv va sensor texnologiyalari. Razvedka va kuzatuv ishlarida videokuzatuv sistemalari va turli sensorlar (masalan, infraqizil, termal, akustik sensorlar) muhim rol o‘ynaydi. Ular dushman pozitsiyalari, yo‘nalishlar, harakatlanuvchi obyektlar haqida ma’lumot beradi.

Sensorlar, masalan, harorat, titrash, akustik signallarni aniqlashga mo‘ljallangan bo‘lishi mumkin va ularning ma’lumotlari algoritmlar orqali tahlil qilinadi. Misol uchun, dronda o‘rnatilgan infraqizil kamera kechasi yoki ob-havo sharoitida ham harakatdagi obyektlarni aniqlay oladi. Yoki yer ustiga joylashtirilgan akustik sensor tarmoqlari dushman bomba

harakatlarini ovoz orqali aniqlashga qodir. Bunday sensor tarmoqlari tomosha maydonini bevosita qamrab oladi va jonli ma'lumot uzatadi. Videokuzatuv tizimlari ayniqsa shahar hududlari, chegara zonalari va muhim obyektlar atrofi uchun muhimdir. Ular doimiy monitoring va aniqlangan ogohlantirishlar berish imkonini beradi.



Real vaqt rejimida axborot yig'ish. Razvedka tizimlarida eng muhim jihat — axborotni kechikmasdan olish va tez tahlil qilish. Raqamli platformalar orqali sensorlar, dronlar, sun'iy yo'ldoshlar ma'lumotni real vaqt rejimida qo'mondonlik markazlariga yetkazadi. Bu esa strategik va taktik qarorlar qabul qilish jarayonini sezilarli darajada tezlashtiradi. Misol sifatida Ukraina—Rossiya mojarosida dronlar juda keng qo'llanilmoqda. Ba'zi manbalarda aytilishicha, FPV (First Person View) dronlar orqali urush maydonida 60–70 % gacha bo'lgan zarar yetkazish holatlari dronlar bilan bog'liq bo'ladi. Shuningdek, 2023-yilda dunyo bo'ylab dron hujumlari natijasida 4 957 holat qayd etilgan, bu 2018-yilga nisbatan keskin o'sishni anglatadi. (2018-yilda faqat 421 holat) Bu statistika dronlar va razvedka texnologiyalarining urushlarda qanday tez kirib borganini ko'rsatadi.

Bundan tashqari, ma'lumotning tezligi nafaqat harakatlanish tomoniga, balki axborotni tahlil qilish vositalariga ham bog'liq. Sun'iy

intellekt, mashinaviy o‘rganish modullari va real vaqtda ma’lumotni filtrlaydigan algoritmlar qo‘mondonlikka zarur ma’lumotlarni darhol uzatadi. Shu yo‘l bilan ma’lumot zaxiralaridan xabardor bo‘lmagan komandirlar vaqtni yo‘qotmay, aniqlik bilan qarorlar qabul qilishi mumkin.

Kibermudofaa va axborot xavfsizligi

Raqamli texnologiyalar kuchayib borayotgani sayin, qurolli kuchlar tizimlarining axborot infratuzilmasi ham katta xavf ostida qoladi. Kiberxavf yurituvchilar, razvedka idoralari, qurol-yarog‘ nazorati, kommunikatsiya tarmoqlari kabi muhim bo‘g‘inlar hujumga uchrashi mumkin. Shu bois, kibermudofaa va axborot xavfsizligi qurolli kuchlarning strategik ustuvor yo‘nalishlaridan biri hisoblanadi.

Harbiy tarmoqlarni himoyalash

Harbiy tarmoqlar – bu komandirlik, razvedka, logistika va harbiy texnikaning boshqaruvlari o‘rtasidagi aloqalarni ta’minlovchi yo‘lakchalar. Ularning buzilishi urush rejimida jiddiy oqibatlarga olib kelishi mumkin; buyruqlar uzilishi, ma’lumot yo‘qolishi yoki chalkashlik yuzaga kelishi ehtimoli bor. Masalan, global miqyosda harbiy kibermudofaa bozori 2025-yilda taxminan USD 17 milliardni tashkil etadi va 2035-yilgacha USD 31.9 milliardgacha yetishi kutilmoqda. CAGR (yillik o‘sish sur’ati) taxminan 6.5 % atrofida.

North America (Shimoliy Amerika) hududi harbiy kiberxavfsizlik bozorida eng katta ulushga ega bo‘lib, 2023/2024 yillarda bu bozorning ~45-50 % qismini tashkil etgan.

Asia-Pacific mintaqasi esa eng yuqori CAGR mendan biri bo‘lgan hududlardan bo‘lib, taxminan 13-14 % yillik o‘sish sur’ati bilan rivojlanishi prognoz qilinmoqda.

Harbiy tarmoqlarni himoyalash doirasida quyidagi jihatlar muhim: tarmoq xavfsizligi (network security), endpoint (oxirgi qurilmalar) himoyasi, operatsion texnologiyalar (OT/ICS), aloqa kanallarining himoyasi. Masalan, Mordor Intelligence ma’lumotlariga ko‘ra, 2024-yilda tarmoq xavfsizligi segmenti harbiy kiberxavfsizlik bozorining taxminan 38.45 % ulushini tashkil qilgan.

Shifrlash va maxsus dasturiy ta'minotlar

Qurolli kuchlarda maxfiylik va ma'lumotlar yaxlitligi (integrity) juda muhim. Buyruklar, xususiy strategik ma'lumotlar va razvedka natijalari shifrlash, autentifikatsiya va maxsus dasturiy ta'minotlar yordamida himoyalanishi lozim. Maxsus programmiy ta'minotlar odatda quyidagilarni o'z ichiga oladi:

Yagona ma'lumot uzatish kanallari (secure communication channels) – VPN, TLS/SSL, maxsus cipher-algoritmlar;

Ma'lumot saqlash (data at rest) va uzatish (data in transit) shifrlanishi;

Kodeks auditlari, open source komponentlar bo'yicha xavfsizlik testlari;

Zero Trust arxitekturasi – ya'ni tarmoq yoki qurilma joylashuviga qaramay, har bir kirish nuqtasi tekshiriladi. Mordor Intelligence hisobotida aytilishicha, ko'plab davlatlar endi Zero Trust tizimlarini joriy etishni rejalashtirmoqda.

Maxsus dasturiy ta'minotlar shuningdek threat intelligence platformalari, SIEM (Security Information and Event Management), IDS/IPS (Intrusion Detection/Prevention Systems) kabi vositalarni o'z ichiga oladi. Statistika shuni ko'rsatadiki, threat intelligence va response segmentlari harbiy kiberxavfsizlik bozorining ~28–30 % qismini tashkil qiladi.

Kiberhujumlarga qarshi kurashish usullari

Kiberhujumlarga qarshi kurashish strategiyalari bir necha darajalarda amalga oshiriladi:

Oldini olish (Prevention):

Tarmoq segmentatsiyasi, tarmoqdan tashqari bo'lmagan aloqalar, faqat kerakli portlar va xizmatlar ochiq bo'lishi;

Yuqori darajadagi autentifikatsiya, ikki faktorli identifikatsiya (2FA), biometrik uslublar;

Doimiy yangilanish va patch boshqaruvi: operatsion tizimlar, ilovalar, firmwareda zaifliklarni bartaraf etish;

Xodimlar orasida kiberxavfsizlik bo‘yicha treninglar, xavf-xatarni anglatish.

Aniqlash (Detection) va monitoring:

Real vaqtli tarmoq monitoringi, intrusion detection tizimlari;

Loglarni yig‘ish, analiz qilish (audit logs, SIEM, EDR – Endpoint Detection & Response);

Threat intelligence va tahdidlar haqidagi ma’lumot almashuvi; davlatlararo hamkorlik qilish;

Sun’iy intellekt va mashinaviy o‘rganish yordamida anomal holatlarni aniqlash.

Reaksiya (Response) va tiklash (Recovery):

Hodisa yuz berganda favqulodda choralar (incident response plan), zarur mutaxassislar va resurslar bilan ishlash;

Ma’lumotlar zaxirasini (backup) saqlash va tez qayta tiklash;

Kompromit qilingan tizimlarni izolyatsiya qilish; zarar yetkazilgan qismi va ta’sirini baholash;

Post-mortem tahlil, sabablari aniqlanishi va kelgusida takrorlanmasligi uchun chora ko‘rilishi.

Global harbiy kiberxavfsizlik bozori (Military Cybersecurity Market) 2025-yilda USD 17 milliardga teng bo‘lishi taxmin qilinadi va 2035-yilgacha USD 31.9 milliardga yetishi prognoz qilinmoqda. CAGR ~6.5 % dan.

Mordor Intelligence ma’lumotiga ko‘ra, harbiy kiberxavfsizlik bozorining tarmoq xavfsizligi segmenti 2024-yilda taxminan 38.45 % ulushga ega bo‘lgan.

Threat intelligence va reaction (javob) segmentlari bozor tarkibining ~28-30% qismini tashkil qiladi.

Geografik taqsimotda: Shimoliy Amerika bozorning eng katta qismini egallab turibdi (~45-50 %), Asia-Pacific hududi esa eng tez rivojlanayotgan mintaqalardan biri, 2023-2025 yillarda ~13-14 % CAGR.

Hukumat sohasida ma’lumot buzilishi (data breach) narxi: misol uchun, hukumat sektori uchun ma’lumotlar buzilishi o‘rtacha xarajat 2021-yilda USD 1.93 million, 2022-yilda esa USD 2.07 millionga ko‘tarilgan.

XXI asrda qurolli kuchlar tizimida raqamli texnologiyalarni keng ko‘lamda qo‘llash davlat xavfsizligini mustahkamlashda, zamonaviy harbiy amaliyotlarni samarali tashkil etishda va milliy mudofaa salohiyatini oshirishda asosiy omilga aylandi. Harbiy boshqaruv tizimlarida raqamli platformalardan foydalanish tezkor qaror qabul qilish, qo‘mondonlikning barcha bo‘g‘inlarini yagona axborot tarmog‘ida birlashtirish imkonini bermoqda. Bu esa operativ vaziyatga moslashuvchanlikni ta’minlab, har qanday tahdidga qisqa fursatda javob berish imkonini beradi.

Razvedka va kuzatuv tizimlarida raqamli texnologiyalar qo‘llanishi qurolli kuchlarning “ko‘z va quloqlarini” sezilarli darajada kuchaytirdi. Sun’iy yo‘ldoshlar, uchuvchisiz uchish apparatlari, videokuzatuv va sensor texnologiyalari real vaqt rejimida axborot yig‘ib, strategik qarorlar qabul qilishda beqiyos yordam bermoqda. Statistik ma’lumotlar ham shuni ko‘rsatadiki, jahon bo‘yicha razvedka va kuzatuv texnologiyalariga ajratilayotgan mablag‘ yildan-yilga oshib bormoqda. Logistika va ta’minot tizimlarida raqamli yechimlar resurslarni aniq hisobga olish, ta’minot zanjirida shaffoflik yaratish va harbiy harakatlarning uzluksizligini ta’minlashga xizmat qilmoqda. Bu esa jangovar sharoitda qo‘shinlarning imkoniyatlarini oshiradi va resurslardan oqilona foydalanishga zamin yaratadi.

Kibermudofaa va axborot xavfsizligi esa raqamlashtirilgan qurolli kuchlar tizimining eng zaif, lekin eng muhim qismi hisoblanadi. Kiberxavfning kuchayishi, maxfiy ma’lumotlarning oshkor bo‘lish xavfi, dushman tomonidan hujumga uchrashi ehtimoli davlatlar oldida jiddiy vazifalarni qo‘ymoqda. Shuning uchun ham milliy dasturiy ta’minot ishlab chiqish, kuchli shifrlash algoritmlarini joriy etish, kiberhujumlarga qarshi samarali strategiyalarni ishlab chiqish va malakali mutaxassislarni tayyorlash zarur.

Foydalanilgan adabiyotlar:

1. To‘xtayev, A. (2022). Axborot texnologiyalari va ularning milliy xavfsizlikdagi o‘rni. Toshkent: “Fan va texnologiya” nashriyoti.

2. Abdullayev, M. (2021). Raqamli transformatsiya va mudofaa tizimlari. Toshkent: O‘zbekiston Milliy Mudofaa universiteti matbuoti.

3. Military Cybersecurity Market Report (2024–2035). Future Market Insights. https://www.futuremarketinsights.com

4. Military Cybersecurity Market Size & Trends (2024). Mordor Intelligence. https://www.mordorintelligence.com

5. Singer, P.W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.

6. Nye, J.S. (2017). The Future of Power in the Digital Age. Harvard University Press.

7. The Cost of Data Breach Report 2022. IBM Security. https://www.ibm.com/reports/data-breach

8. Krepinevich, A. (2019). The Military-Technical Revolution: A Preliminary Assessment. Center for Strategic and Budgetary Assessments, Washington.

9. United Nations Office for Disarmament Affairs (2020). Cybersecurity and International Security. Nyu-York.

10. Raqamli O‘zbekiston – 2030 strategiyasi. (2020). Toshkent: O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi.

O‘ZBEKISTON RESPUBLIKASINING QUROLLI KUCHLARIDA YANGI TEXNOLOGIYALAR VA YANGLIKLAR KIRITISH

Qilichov B
Jamoat Xavfsizligi Universiteti kursanti
Jalolov A.A.
O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti
Axborot texnologiyalari kafedrasi o‘qituvchisi

Zamonaviy dunyoda qurolli kuchlar davlat xavfsizligi va barqarorligini ta’minlashda muhim rol o‘ynaydi. Texnologiyalar tez sur’atlar bilan rivojlanib borayotgan hozirgi davrda, qurolli kuchlarga yangi innovatsion texnologiyalarni joriy etish ularning samaradorligini

oshirishda muhim ahamiyat kasb etadi. Zamonaviy asbob-uskunalar, axborot tizimlari va raqamli texnologiyalar harbiy operatsiyalarni yanada aniq, tezkor va samarali amalga oshirishga imkon beradi. Ushbu maqolada qurolli kuchlarga kiritilayotgan yangi texnologiyalar va yangiliklarning ahamiyati, shuningdek, ularning harbiy kuchlar faoliyatiga ta'siri tahlil qilinadi.

Bugungi kunda harbiy sohada texnologiyalar tez rivojlanib bormoqda va qurolli kuchlarning samaradorligini oshirishda muhim omilga aylangan. Yangi texnologiyalarni joriy etish orqali harbiy kuchlar yanada ilg'or, tezkor va aniq harakat qilish imkoniyatiga ega bo'ladi. Innovatsion yechimlar, raqamli tizimlar va avtomatlashtirilgan qurilmalar harbiy xizmatchilarning vazifalarini yengillashtirib, mudofaa salohiyatini oshiradi. Ushbu maqolada qurolli kuchlarga kiritilayotgan yangi texnologiyalar va ularning harbiy sohadagi o'rni haqida so'z boradi.

1.Dunyo davlatlarida ishlatilayotgan texnologiyalar va inovatsion qurilmalar.

1. Dronlar va Kamikadze Dronlar

Ukraina "Brave1" nomli yangi kamikadze dronini ishlab chiqdi. Bu dron 50 kilometrgacha aniq zarba bera oladi va elektron urush tizimlariga qarshi chidamli. Ya'ni, signalni to'sib qo'yish yoki aralashtirish orqali uni to'xtatib bo'lmaydi.

Shimoliy Koreya esa "Saebyeol-4" deb nomlangan razvedka dronini ishlab chiqdi. Bu dron tashqi ko'rinishi bo'yicha AQShning "RQ-4 Global Hawk" droniga o'xshaydi va qilish imkonini beradi.

2. Giper Ovozli Qurollar

Xitoy "YJ-19" nomli giper ovozli raketasini taqdim etdi. Bu raketa havo nafas olish tizimi orqali Mach 10 tezlikda (tovush tezligidan 10 baravar tez) ucha oladi. Uni suv osti kemalaridan uchirish mumkin.

Hindiston esa "LRAShM" deb nomlangan giper ovozli raketani ishlab chiqmoqda. U 1500 kilometrgacha aniq zarba bera oladi va hozirda Hindiston harbiy kuchlari tomonidan sinovdan o'tkazilmoqda.

3. Sun'iy Intellekt va Avtonom Harbiy Texnologiyalar

AQSh harbiylari Reaper dronlari uchun sun’iy intellekt tizimini ishlab chiqmoqda. Bu tizim dronning zaif joylarini aniqlaydi, shuningdek, lazer nurlarini aniq yo‘naltirishda yordam beradi.

Hindistonda "Bharat Electronics Limited" kompaniyasi tomonidan sun’iy intellekt asosida ishlovchi texnologiyalar yaratilmoqda. Ular orasida virtual yordamchilar, til tarjimonlari va ovozli tahlil tizimlari mavjud bo‘lib, bu texnologiyalar harbiy sohada keng qo‘llaniladi.

4. Lazer Qurollari

Buyuk Britaniya armiyasi lazer quroli yordamida dronlarni havoda yo‘q qilishni muvaffaqiyatli sinovdan o‘tkazdi. Ushbu qurol 1 kilometr masofadagi dronlarni yo‘q qilish imkoniyatiga ega.

Xitoy esa "Silent Hunter" nomli lazer qurolini ishlab chiqdi. Bu qurol 30 kVt dan ortiq energiyaga ega bo‘lib, dronlarga qarshi kurashda juda samarali hisoblanadi.

2.Dunyo bo‘yicha yangi texnologiya va qurilmalarga ega bo‘lgan davlatlar.



3.O‘zbekiston harbiy sohasiga innovatsion yangilik va qurilmalar kiritish bo‘yicha maslahatlar.

1. Texnologik innovatsiyalarni joriy etish

Zamonaviy raqamli va sun’iy intellekt texnologiyalarini harbiy tizimlarga integratsiya qilish muhim ahamiyatga ega. Bu harbiy boshqaruv,

razvedka va ma'lumotlarni tahlil qilish jarayonlarini sezilarli darajada yaxshilaydi.

Masofadan boshqariladigan dronlar, kiberxavfsizlik tizimlari, lazer qurollari va giper ovozli raketalar kabi ilg'or qurollarni o'rganish va ishlab chiqishga alohida e'tibor qaratish lozim.

2. Kadrlar tayyorlash va ilmiy tadqiqotlarni rivojlantirish

Harbiy texnologiyalar sohasida malakali mutaxassislarni tayyorlash uchun oliy o'quv yurtlari va ilmiy markazlarni rivojlantirish zarur.

Innovatsion g'oyalarni qo'llab-quvvatlash uchun ilmiy-tadqiqot institutlari va harbiy sanoat korxonalari o'rtasida yaqindan hamkorlik o'rnatilishi kerak.

3. Xalqaro hamkorlikni kengaytirish

Innovatsion harbiy texnologiyalarni rivojlantirish uchun ilg'or davlatlar bilan hamkorlik qilish muhim. Bu orqali yangi texnologiyalarni o'rganish va ularni mamlakatga olib kirish imkoniyatlari kengayadi.

Xalqaro forum va ko'rgazmalarda qatnashish orqali dunyodagi yangi tendensiyalarni kuzatib borish mumkin.

4. Mahalliy harbiy sanoatni rivojlantirish

Mahalliy korxonalarni yuqori texnologiyali harbiy mahsulotlar ishlab chiqarishga jalb qilish kerak.

Innovatsion startaplarni qo'llab-quvvatlash, harbiy sanoat uchun maxsus grantlar va imtiyozlar yaratish orqali milliy harbiy sanoatni mustahkamlash mumkin.

5. Axborot xavfsizligini mustahkamlash

Kiberxavfsizlik sohasida kuchli tizimlar yaratish va axborot hujumlariga qarshi himoyani ta'minlash dolzarb masala hisoblanadi.

Harbiy infratuzilmani raqamli tahdidlardan himoya qilish orqali umumiy milliy xavfsizlikni kuchaytirish mumkin.

O'zbekiston uchun eng muhim jihat — bu ilm-fan va texnologiyalarga sarmoya kiritish, shuningdek, yosh mutaxassislarni qo'llab-quvvatlashdan iborat. Bunday yo'nalishlar bo'yicha konkret loyihalar va texnologik yechimlar ishlab chiqish orqali real natijalarga erishish mumkin.

Zamonaviy harbiy sohada muvaffaqiyatga erishish uchun texnologik taraqqiyot muhim omilga aylanmoqda. O‘zbekiston Qurolli Kuchlarini kuchaytirish, milliy xavfsizlikni mustahkamlash va harbiy salohiyatni oshirish uchun innovatsion texnologiyalarni joriy etish dolzarb vazifadir.

Sun’iy intellekt, dronlar, kiberxavfsizlik tizimlari, giper ovozli qurollar va raqamli boshqaruv kabi sohalarga e’tibor qaratish zarur.

Buning uchun:

- mahalliy harbiy sanoatni rivojlantirish,
- ilmiy-tadqiqot ishlarini kuchaytirish,
- yosh kadrlarni tayyorlash,
- ilg‘or davlatlar bilan hamkorlik qilish katta ahamiyatga ega.

O‘zbekiston o‘z salohiyatini to‘liq ishga solsagina, yaqin kelajakda harbiy texnologiyalar sohasida mintaqada yetakchi o‘rinlardan birini egallashi mumkin.

Foydalanilgan adabiyotlar:

1.World of Statixtics\\ @stats_feed.

2.Tom’s HARDWARE.com

3. Turli mamlakatlar Mudofaa vazirliklari va kiberstrategiya hujjatlari (oq qog‘ozlar, strategik hisobotlar).

4. To‘laganov A. — Axborot texnologiyalari va milliy xavfsizlik (Toshkent, 2022).

5. Xalqaro ilmiy jurnallar: Journal of Strategic Studies, Military Technology Review, Journal of Cybersecurity va boshqalar.

QUROLLI KUCHLARDA RAQAMLI TEXNOLOGIYALARNI JORIY ETISH VA RIVOJLANTIRISH MUAMMOLARI

Xudoyberdiyev M.R.

Yusupov U.A.

O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti kursanti

O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti kafedra katta o‘qituvchisi

O‘zbekiston Respublikasi Prezidentining 2020 yil 5 oktabrdagi PF-6079-sonli “Raqamli O‘zbekiston — 2030 strategiyasini” tasdiqlash va uni

samarali amalga oshirish chora-tadbirlari to‘g‘risidagi farmonida mamlakatimizda raqamli iqtisodiyotni faol rivojlantirish, barcha tarmoqlar va sohalarda, eng avvalo, davlat boshqaruvi, ta’lim, sog‘liqni saqlash va qishloq xo‘jaligida zamonaviy axborot-kommunikatsiya texnologiyalarini keng joriy etish bo‘yicha kompleks chora-tadbirlarni amalga oshirish bo‘yicha vazifalar aniq belgilab qo‘yilgan.

Global raqamlashtirish – ancha ta’sirchan eshitiluvchi tushuncha bo‘lib, bu tushunchaning mohiyati nimadan iborat ekanligi va uning jamiyat uchun qanday ijobiy taraflari borligini oddiy so‘zlar bilan ifodalashga harakat qilamiz. Globalizatsiya sharoitida ta’limni raqamlashtirish va uni tashkil etish muhim ahamiyat kasb etmoqda. Raqamli texnologiyalar ta’lim tizimiga kirib kelishi bilan jarayonlar samaradorligi oshmoqda, imkoniyatlar kengaymoqda va ta’limning sifati yaxshilanmoqda.

Bugungi globallashuv kunda raqamli texnologiyalar jadal sur’atlar bilan harbiy sohalarga kirib kelmoqda. Axborot-kommunikatsiya texnologiyalari, sun’iy intellekt, kiberxavfsizlik, robototexnika kabi yo‘nalishlarsiz zamonaviy Qurolli Kuchlarni tasavvur qilish mushkul. Ushbu texnologiyalarni samarali joriy etish esa, eng avvalo, yuqori malakali kadrlarning mavjudligiga bog‘liq. Ammo amaliyotda bu yo‘nalishda bir qator muammolar mavjud bo‘lib jumladan;

Malakali mutaxassislar yetishmasligi: Raqamli texnologiyalar sohasida chuqur bilim va tajribaga ega harbiy kadrlarning yetishmasligi texnologiyalarning samarali joriy etilishiga to‘sqinlik qiladi.

O‘quv dasturlarining eskirib borayotgani: An’anaviy harbiy ta’lim dasturlari raqamli texnologiyalarning jadal rivojlanishiga mos ravishda yangilanmayotgani, bu esa zamonaviy texnologiyalarga oid bilimlarning yetarli darajada o‘rgatilmasligiga olib keladi.

Amaliy tajriba yetishmasligi: Harbiy xizmatchilarni real sharoitlarda raqamli texnologiyalardan foydalana olish ko‘nikmalari bilan ta’minlash uchun amaliy mashg‘ulotlarning yetarli emasligi kuzatilmoqda.

O‘z navbatida yuqorida keltirilgan Qurolli Kuchlarda raqamli texnologiyalarni joriy etishda uchrayotgan asosiy muammolar va ularning yechimlari keltirib o‘tamiz

1.1 - jadval

Muammo	Tavsif	Yechim (taklif)
Mutaxassislar yetishmasligi	Sun'iy intellekt, kiberxavfsizlik bo'yicha kadrlar tanqisligi	Maxsus kurslar, xalqaro sertifikatlash orqali mutaxassislar tayyorlash
Raqamli madaniyat va motivatsiyaning pastligi	Harbiy xizmatchilar raqamli bilimlarni o'zlashtirishga qiziqishi pastligi	Raqamli savodxonlik kurslari, moliyaviy rag'batlantirish orqali
Xalqaro tajriba yetarli o'rganilmaganligi	Ilg'or harbiy raqamli ta'lim modellari to'liq o'rganilmaganligi	Raqamli savodxonlik kurslari, moliyaviy rag'batlantirish orqali.

Ta'lim dasturlarini modernizatsiya qilish: Harbiy ta'lim muassasalarida raqamli texnologiyalar bo'yicha maxsus kurslar va modullarni joriy etish, ularni zamonaviy talablar va texnologik o'zgarishlarga mos ravishda yangilab borish lozim.

Amaliy mashg'ulotlarni kuchaytirish: Harbiy xizmatchilarga real sharoitlarda raqamli texnologiyalardan foydalanish imkoniyatini beruvchi treninglar va mashg'ulotlarni tashkil etish orqali ularning amaliy ko'nikmalarini rivojlantirish kerak. Mutaxassislarni qayta tayyorlash va malaka oshirish: Mavjud harbiy kadrlar uchun raqamli texnologiyalar bo'yicha qayta tayyorlash va malaka oshirish dasturlarini ishlab chiqish va amalga oshirish muhimdir.

Xalqaro tajribadan foydalanish: Raqamli texnologiyalarni harbiy sohada muvaffaqiyatli joriy etgan davlatlarning tajribasini o'rganish va moslashtirish orqali milliy ta'lim tizimini boyitish mumkin.

Ushbu chora-tadbirlar orqali Qurolli Kuchlarda raqamli texnologiyalarni samarali joriy etish uchun zarur bo'lgan malakali kadrlar tayyorlash tizimini shakllantirish mumkin.

Qurolli Kuchlarda raqamli texnologiyalarni joriy etish — bu zamon talabi. Ushbu jarayon muvaffaqiyatli kechishi uchun kadrlar tayyorlashga tizimli va strategik yondashuv zarur. Globallashuv sharoitida raqamli texnologiyalarga doir darslarni tashkillashtirish, mahorat darslarini o'tkazishni yo'lga qo'yish ham raqamli texnologiyalarni ta'minlashga olib keladi. Bu esa, jamiyatning ta'lim muhitida axborot va telekommunikatsiya olamida mas'uliyatli va xavfsiz xulq-atvor ko'nikmalarini shakllantirishga zamin yaratadi.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasi Prezidentining qarori, 22.01.2025 yildagi PQ-17-son.
2. 2022 — 2026-yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasini insonga e’tibor va sifatli ta’lim yilida amalga oshirishga oid davlat dasturi
3. Babadjonov S.S. Axborotlashgan jamiyatda bo‘lajak harbiy xizmatchilarning media madaniyatini rivojlantirishga ta’sir etuvchi omillar./ S.S. Babadjanov // Harbiy ta’lim va fanda innovatsiyalar. – 2020.- 1 (10). 41-45-b.

QUROLLI KUCHLAR TIZIMIDA AXBOROT TEXNOLOGIYALARI

Sadirova M.Q.
Jamoat xavfsizligi universiteti kursanti
Saidbayev B.Dj.
Texnika fanlari bo‘yicha falsafa doktori (PhD), podpolkovnik
“Axborot texnologiyalari” kafedrasi dotsenti

Bugungi kunda harbiy sohada axborot texnologiyalari milliy xavfsizlikni ta’minlashda hal qiluvchi ahamiyat kasb etmoqda. Zamonaviy urush va harbiy mojarolarning aksariyati axborot ustunligi uchun kurash shaklida kechayotgani barchaga ma’lum. Shu bois, qurolli kuchlar tizimida raqamli texnologiyalarni joriy etish nafaqat qo‘shinlarni boshqarishda samaradorlikni oshiradi, balki qaror qabul qilish tezligini ham ta’minlaydi.

Axborot texnologiyalarining qo‘llanish yo‘nalishlari:

- **Harbiy boshqaruv** – qo‘shinlar joylashuvi, harakatlanishi va resurslardan foydalanishni real vaqt rejimida kuzatish.
- **Aloqa tizimlari** – xavfsiz va shifrlangan axborot almashinuvini ta’minlash.
- **Geoinformatsion tizimlar** – xarita va sun’iy yo‘ldosh ma’lumotlari asosida taktik va strategik rejalashtirish.
- **Sun’iy intellekt va dron texnologiyalari** – razvedka, kuzatuv va xavf-xatarlarni oldindan aniqlashda qo‘llash.

- **Kiberxavfsizlik** – harbiy ma’lumotlar bazasi va boshqaruv tizimlarini kiberhujumlardan himoya qilish.

Shuningdek, ilg‘or davlatlarning tajribasi shuni ko‘rsatadiki, harbiy sohada raqamli transformatsiyani jadallashtirish mudofaa qudratini sezilarli darajada kuchaytiradi. Shu bilan birga, qurolli kuchlar tizimida axborot texnologiyalarini tatbiq etishda infratuzilma yetishmovchiligi, malakali mutaxassislar kamligi va yuqori darajadagi kiberxavf muammolari mavjud.

Axborot texnologiyalari (AT) Qurolli kuchlarda (qurolli kuchlar) axborotni boshqarish, aloqa qilish, to‘plash va qayta ishlash hamda qarorlarni qo‘llab-quvvatlash uchun muhim rol o‘ynaydi. Ular kompyuterlar, dasturiy ta’minot va tarmoqlar kabi ma’lumotlarni boshqarish uchun barcha resurslarni o‘z ichiga oladi va operatsion samaradorlikni oshirish, muvofiqlashtirishni yaxshilash va xavfsizlikni ta’minlash uchun ishlatiladi.

ATni quyosh ostida qo‘llashning asosiy jihatlari:

Aloqa va boshqaruv: it aloqa tarmoqlari va qurilmalarining ishlashini ta’minlaydi, bu jang maydonidagi askarlardan tortib qo‘mondonlik punktlarigacha bo‘lgan turli bo‘linmalar o‘rtasida ma’lumot almashish imkonini beradi.

Axborotni qo‘llab-quvvatlash: AT Real vaqtda tahlil qilish va qaror qabul qilish uchun zarur bo‘lgan katta hajmdagi ma’lumotlarni yaratish, saqlash, qayta ishlash va uzatishda yordam beradi.

Xavfsizlik: IT texnologiyalari axborot va tizimlarni tashqi tahdidlardan himoya qilish, ma’lumotlarning maxfiyligi va yaxlitligini ta’minlash uchun ishlatiladi.

Ma’lumotlarni yig‘ish va tahlil qilish: it mutaxassislari potensial tahdidlarni aniqlash va milliy xavfsizlikka yordam beradigan ma’lumotlarni to‘plash uchun keng ko‘lamli tahliliy tizimlar va boshqa ilg‘or texnologiyalarni qo‘llaydilar.

Jarayonlarni raqamlashtirish: IT-ni amalga oshirish odatdagi vazifalarni avtomatlashtirishga, harbiy operatsiyalarning shaffofligi va

samaradorligini oshirishga, o‘qitish va muvofiqlashtirishni yaxshilashga imkon beradi.

Muayyan texnologiyalarga misollar:

5G uyali tarmoqlari: sohadagi turli xil qurilmalar va ilovalar uchun tez va ishonchli aloqani ta’minlaydi.

Kognitiv radarlar: maqsadlarni aniqlash va kuzatish uchun aqlli tizimlar.

Lazer texnologiyasi: maqsadlarni qidirish, yo‘naltirish va yo‘q qilishda qo‘llaniladigan takomillashtirilgan tizimlar.

Analitik tizimlar: qimmatli ma’lumotlarni olish va strategik qarorlar qabul qilish uchun katta hajmdagi ma’lumotlarni qayta ishlashga imkon beradi.

Qurolli kuchlar tizimida axborot kommunikatsiyalari

Hozirgi zamonaviy qurolli kuchlar faoliyatida **axborot-kommunikatsiya texnologiyalari (AKT)** alohida strategik ahamiyat kasb etmoqda. Chunki harbiy boshqaruv, qo‘mondonlik, razvedka, mudofaa va hujum amaliyotlarining samaradorligi ko‘p jihatdan tezkor, xavfsiz va ishonchli axborot almashinuvi hamda kommunikatsiya tizimlariga bog‘liqdir.

Qurolli kuchlar tizimida axborot-kommunikatsiyalar bir qator vazifalarni bajaradi. Avvalo, qo‘shinlar o‘rtasida tezkor buyruq va ko‘rsatmalarni uzatish, ma’lumotlarni real vaqt rejimida qayta ishlash, strategik hamda taktik boshqaruvni muvofiqlashtirish ularning eng muhim vazifalaridan hisoblanadi. Shuningdek, askarlarning joylashuvi, texnika va qurol-aslaha holatini monitoring qilish, kiberxavfsizlikni ta’minlash, maxfiy harbiy ma’lumotlarni himoya qilishda ham axborot tizimlari beqiyos ahamiyat kasb etadi.

Bugungi kunda qurolli kuchlarda axborot-kommunikatsiya texnologiyalarining turli shakllari keng qo‘llanmoqda. Masalan, sun’iy yo‘ldosh aloqa tizimlari uzoq masofalarda qo‘mondonlik markazi va qo‘shinlar o‘rtasidagi barqaror bog‘lanishni ta’minlaydi. Radiotexnik aloqa vositalari dala sharoitida tezkor boshqaruv imkonini beradi. Maxsus harbiy internet va yopiq internet tizimlari orqali ichki va tashqi ma’lumot almashinuvi xavfsiz amalga oshiriladi. Dronlar va uchuvchisiz uchish

apparatlari esa razvedka olib borishda hamda jangovar maqsadlarni aniqlashda muhim axborot uzatuvchi vositaga aylangan. Shu bilan birga, shifrlash va kodlash texnologiyalari maxfiylikni ta’minlashda asosiy omil hisoblanadi.

So‘nggi yillarda dunyo miqyosida “axborot urushi” tushunchasi keng qo‘llanilmoqda. Bu dushman davlatlar yoki terrorchi guruhlarning kiberhujumlar, dezinformatsiya va propagandalar orqali harbiy tizimlarni izdan chiqarish, jamiyatda notinchlik keltirib chiqarish hamda qaror qabul qilish jarayoniga ta’sir o‘tkazish harakatlarini anglatadi. Shu sababli ko‘plab davlatlar, jumladan, O‘zbekiston ham qurolli kuchlar tizimida maxsus kiberqo‘shinlar, axborot xavfsizligi markazlari va sun’iy intellekt asosida ishlovchi xavfsizlik tizimlarini tashkil etishga alohida e’tibor qaratmoqda.

Axborot-kommunikatsiya texnologiyalarining istiqbollari yanada keng. Kelajakda 5G va 6G mobil tarmoqlari yordamida qo‘shinlar o‘rtasida ultra-tezkor aloqa yo‘lga qo‘yiladi. Kvant aloqa texnologiyalari ma’lumotlarni deyarli buzib bo‘lmaydigan darajada himoyalash imkonini beradi. Sun’iy intellekt esa harbiy boshqaruv va razvedka tizimlarida qaror qabul qilishni avtomatlashtiradi. IoT (Internet of Things) asosidagi integratsiyalangan nazorat tizimlari yordamida esa barcha texnik vositalar yagona boshqaruv markaziga ulanib, jangovar tayyorgarlik va mudofaa samaradorligini sezilarli darajada oshiradi.

1. Axborot kommunikatsiyalarining o‘rni

Qurolli kuchlarda axborot tizimlari:

- qo‘shinlar o‘rtasida **tezkor buyruq va ko‘rsatmalarni uzatish**;
- razvedka ma’lumotlarini **real vaqt rejimida qayta ishlash**;
- **strategik va taktik boshqaruvni** muvofiqlashtirish;
- qo‘shinlarning joylashuvi, texnika va qurol-aslaha holatini **monitoring qilish**;
- **kiberxavfsizlikni ta’minlash** kabi vazifalarni bajaradi.

2. Zamonaviy texnologiyalarning qo‘llanishi

Qurolli kuchlar tizimida quyidagi axborot-kommunikatsiya vositalari keng qo‘llanmoqda:

- **Sun’iy yo‘ldosh aloqa tizimlari** – uzoq masofalarda bevosita aloqani ta’minlaydi.
- **Radiotexnik aloqa vositalari** – dala sharoitida tezkor boshqaruvni amalga oshirishda qo‘llanadi.
- **Internet tarmog‘i va maxsus harbiy intranetlar** – ichki va tashqi ma’lumot almashinuvi uchun.
- **Dronlar va uchuvchisiz uchish apparatlari** – razvedka va maqsadli zarbalar berishda ma’lumot uzatish vositasi sifatida.
- **Shifrlash va kodlash texnologiyalari** – harbiy sirlarni himoyalash va raqamli axborotni xavfsiz uzatish uchun.

3. Axborot urushlari va kiberxavfsizlik

Bugungi kunda qurolli kuchlar faqatgina an’anaviy jang maydonida emas, balki **axborot urushi** deb ataluvchi yangi frontda ham faoliyat olib bormoqda. Dushman davlatlar yoki terrorchi guruhlar turli **kiberhujumlar**, dezinformatsiya va propagandalar orqali harbiy tizimlarni izdan chiqarishga urinishi mumkin. Shu bois qurolli kuchlarda:

- **maxsus kiberqo‘shinlar**,
- **axborot xavfsizligi markazlari**,
- **sun’iy intellekt asosida ishlovchi xavfsizlik tizimlari** tashkil qilinmoqda.

4. Axborot kommunikatsiyalarining istiqbollari

Kelajakda qurolli kuchlar tizimida axborot kommunikatsiyalari:

- **5G va 6G tarmoqlari**,
- **kvant aloqa texnologiyalari**,
- **sun’iy intellekt yordamida boshqaruv**,
- **IoT (Internet of Things)** asosidagi integratsiyalangan nazorat tizimlari orqali yanada rivojlanadi.

Sun’iy intellektning zamonaviy jamiyatdagi o‘rni

Bugungi kunda sun’iy intellekt (SI) texnologiyalari insoniyat hayotining deyarli barcha jabhalariga kirib bormoqda. Dastlab oddiy hisoblash va algoritmik jarayonlarni avtomatlashtirishdan boshlangan bu soha hozirgi davrda murakkab qaror qabul qilish, ma’lumotlarni chuqur tahlil qilish, tabiiy tilni tushunish hamda inson miyasi faoliyatiga yaqin bo‘lgan funksiyalarni bajarish darajasiga yetdi. Sun’iy intellektning asosiy

vazifasi — inson mehnatini yengillashtirish, samaradorlikni oshirish va mavjud resurslardan oqilona foydalanish imkonini yaratishdir.

SI texnologiyalarining eng rivojlangan yo‘nalishlari jumlasiga **mashinali o‘rganish, chuqur o‘rganish, neyron tarmoqlar, tabiiy tilni qayta ishlash, kompyuter ko‘rish va ekspert tizimlari** kiradi. Ayniqsa, mashinali o‘rganish orqali dasturlar mustaqil ravishda yangi bilimlarni o‘zlashtirib, mavjud ma’lumotlardan foydalangan holda yangicha qarorlar chiqarishi mumkin. Bu esa ishlab chiqarishdan tortib, tibbiyot, ta’lim, transport va xavfsizlik tizimlarigacha bo‘lgan sohalarda qo‘llanilmoqda.

Tibbiyotda SI yordamida turli kasalliklarni erta aniqlash, genetik ma’lumotlarni tahlil qilish va individual davolash usullarini ishlab chiqish mumkin. Ta’lim sohasida esa sun’iy intellekt asosida yaratilgan platformalar o‘quvchilarning bilim darajasini tahlil qilib, ularga shaxsiylashtirilgan topshiriqlarni taqdim etadi. Transport tizimida SI avtonom avtomobillarni boshqarish, yo‘l harakati xavfsizligini oshirish va logistikani optimallashtirishda katta ahamiyat kasb etmoqda.

Shuningdek, sun’iy intellekt xavfsizlik tizimlarida ham muhim rol o‘ynamoqda. Masalan, yuzni aniqlash, nutqni tanish va harakatlarni kuzatish imkoniyatiga ega dasturlar turli obyektlarni qo‘riqlashda keng qo‘llanmoqda. Bu esa inson omiliga bog‘liq xatoliklarni kamaytiradi va aniqroq nazorat o‘rnatadi.

Biroq sun’iy intellektning jadal rivojlanishi bilan birga turli **axloqiy, huquqiy va ijtimoiy muammolar** ham yuzaga chiqmoqda. Jumladan, ishchi kuchining qisqarishi, inson hayoti uchun mas’ul bo‘lgan qarorlarni mashinalarga topshirish, shaxsiy ma’lumotlarning himoyasi hamda algoritmlardagi xolislik muammolari dolzarb masalalardan hisoblanadi. Shu sababli, mutaxassislar SI’ni rivojlantirish jarayonida uning imkoniyatlari va xavflarini muvozanatlashtirish zarurligini ta’kidlamoqdalar.

Axborot kommunikatsiyalari tizimi zamonaviy jamiyatning eng muhim infratuzilmalaridan biri hisoblanadi. Unda ma’lumotlarni tezkor uzatish, qayta ishlash va saqlash jarayonlari asosiy o‘rinni egallaydi. Ushbu

jarayonlarni samarali tashkil etishda sun'iy intellekt (SI) texnologiyalarining roli beqiyosdir.

Birinchidan, SI axborot oqimlarini boshqarishda va ularni tahlil qilishda katta imkoniyat yaratadi. Har kuni milliardlab ma'lumotlar turli aloqa kanallari orqali uzatilmoqda. Bunday ulkan hajmdagi ma'lumotlarni inson imkoniyatlari bilan nazorat qilish qiyin, ammo sun'iy intellekt asosida yaratilgan algoritmlar real vaqt rejimida ma'lumotlarni qayta ishlash, tasniflash va saralashga qodir. Bu esa aloqa tarmoqlarining tezkorligi va ishonchliligini oshiradi.Ikkinchidan, SI axborot xavfsizligini ta'minlashda muhim o'rin tutadi. Sun'iy intellekt yordamida kompyuter tarmoqlaridagi noxush harakatlarni, xakerlik urinishlarini va zararli dasturlarni erta aniqlash mumkin. Masalan, neyron tarmoqlar asosida ishlab chiqilgan xavfsizlik tizimlari tarmoqdagi g'ayrioddiy faollikni kuzatib, avtomatik tarzda tahdidni bartaraf etish choralarini ko'radi. Shu orqali davlat va tashkilotlarning axborot kommunikatsiyalari tizimlari yanada ishonchli bo'ladi. Uchinchidan, SI foydalanuvchilar bilan samarali muloqot o'rnatishda yordam beradi. Tabiiy tilni qayta ishlash texnologiyalari orqali chat-botlar, ovozli yordamchilar va intellektual tizimlar insonning yozma yoki og'zaki murojaatlarini tezkor tushunib, kerakli javobni bera oladi. Bu aloqa jarayonini qulaylashtirib, xizmat ko'rsatish sifatini oshiradi.To'rtinchidan, axborot kommunikatsiyalarida resurslardan oqilona foydalanish masalasi ham dolzarb. Sun'iy intellekt asosida yaratilgan optimallashtirish algoritmlari tarmoqdagi yuklamani taqsimlash, uzatish tezligini muvofiqlashtirish va energiya samaradorligini oshirishda qo'llaniladi. Bu ayniqsa 5G va IoT kabi yangi texnologiyalar rivojlanayotgan bir davrda juda muhimdir.Shuningdek, SI multimedia axborotlarini qayta ishlashda ham keng qo'llanilmoqda. Masalan, video va audio signallarni siqish, sifatsiz kadrlarni tiklash, tarjima qilish yoki avtomatik subtitrlar yaratishda sun'iy intellekt inson mehnatini yengillashtiradi va aloqa samaradorligini oshiradi.

Qurolli kuchlar tizimida axborot-kommunikatsiyalar — strategik resurs: tezkor va ishonchli aloqa buyruq-barqarorlik, razvedka, logistika va monitoringni ta'minlaydi. Zamonaviy vositalar (sun'iy yo'ldosh va

radioaloqa, maxsus internetlar, dronlar, shifrlash) harbiy operatsiyalarni samarali boshqarishga imkon beradi. Shu bilan birga axborot urushi va kiberhujumlar xavfi ortib bormoqda, shuning uchun kiberxavfsizlik va maxfiylikka alohida e'tibor zarur. Kelajakda 5G/6G, kvant aloqa, AI va IoT integratsiyasi harbiy kommunikatsiyalarni yangi bosqichga olib chiqadi. Umuman olganda, AKTlarning rivoji milliy xavfsizlik va harbiy imkoniyatlarni keskin oshiradi — lekin xavfsizlik va nazorat choralari ham kuchaytirilishi lozim. Sun'iy intellekt axborot kommunikatsiyalari tizimining tezkorligi, xavfsizligi va samaradorligini oshirishda strategik ahamiyatga ega. U orqali nafaqat texnik, balki ijtimoiy jihatdan ham qulay va xavfsiz axborot muhitini shakllantirish mumkin.

Foydalanilgan adabiyotlar:

1. Karimov I.A. *Yuksak ma'naviyat – yengilmas kuch.* – Toshkent: Ma'naviyat, 2008.
2. O'zbekiston Respublikasi Mudofaa vazirligi. *Qurolli Kuchlar tizimida axborot-kommunikatsiya texnologiyalarini joriy etish bo'yicha yo'riqnoma.* – Toshkent, 2021.
3. To'xtayev Sh., Usmonov B. *Axborot xavfsizligi asoslari.* – Toshkent: Toshkent axborot texnologiyalari universiteti nashriyoti, 2019.
4. Jalilov M. *Harbiy boshqaruv tizimlarida raqamli texnologiyalar.* – Toshkent: Fan va texnologiya, 2020.
5. Qodirov A. *Kiberxavfsizlik va axborot urushi.* – Toshkent: Innovatsiya nashriyoti, 2022.
6. NATO Defence College. *Emerging Information and Communication Technologies in Military Operations.* – Rome, 2020.
7. Paul C., Matthews M. *Information Operations: Doctrine and Practice.* – RAND Corporation, 2019.
8. Singer P.W., Friedman A. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* – Oxford University Press, 2014.
9. Nye J.S. *The Future of Power.* – New York: PublicAffairs, 2011.
10. O'zbekiston Respublikasi Prezidenti qarori: *Raqamli O'zbekiston – 2030 strategiyasi.* – Toshkent, 2020.

QUROLLI KUCHLAR TIZIMIDA AXBOROT TEXNOLOGIYALARINI O‘RNI VA VAZIFASI

Majidova S.N.
Jamoat xavfsizligi universiteti talabasi

XXI asrda harbiy kuchlar samaradorligini belgilovchi asosiy unsur — axborot va u bilan ishlash qobiliyatidir. Traditsion jangovar resurslar (yana qurol-yarog‘, tanklar va h.k.) muhim bo‘lib qolaveradi, ammo ma’lumotlarni to‘plash, qayta ishlash, uzatish va himoya qilishdagi ustunlik ko‘p hollarda g‘alaba yoki mag‘lubiyatni hal etadi. Shu nuqtai nazardan, axborot texnologiyalari (kompyuter tarmoqlari, telekommunikatsiyalar, sun’iy intellekt, avtonom tizimlar va boshqalar) qurolli kuchlar tizimining barcha elementlariga integratsiyalashgan holda kirib bormoqda.

Atning qurolli kuchlarda asosiy yo‘nalishlari va ta’siri

Asosiy qism. Axborot asrida qurolli kuchlarni o‘rganish turli soha adabiyotlarini qamrab oladi: tarmoqqa yo‘naltirilgan urush nazariyasi (network-centric warfare), C4ISR konsepsiyasi, kiber mudofaa va axborot operatsiyalari mavzulari. Mazkur yo‘nalishdagi muhim manbalar sifatida D. Alberts va hamkorlarining tarmoqqa yo‘naltirilgan urush haqidagi ishlari, M. Castellsning axborot jamiyati tahlillari, NATO va turli davlatlar mudofaa strategiyalaridagi kiber siyosat hujjatlari ko‘rsatilishi mumkin. O‘zbekiston va Markaziy Osiyo sharoitida ham Atning harbiy tatbiqi va uning qonuniy-etik jihatlari bo‘yicha milliy hujjatlar va tahliliy materiallar muhim ahamiyatga ega. C4ISR tizimlari qo‘shinlarni boshqarish, vaziyatni baholash va qaror qabul qilish jarayonlarini avtomatlashtiradi. Real vaqtda axborot oqimini ta’minlovchi sun’iy yo‘ldosh aloqalari, harbiy tarmoqlar, shifrlangan radiokommunikatsiyalar va ma’lumotlar integratsiyasi qo‘mondonlarga tez va ishonchli qaror qabul qilish imkonini beradi. AT yordamida OODA (Observe–Orient–Decide–Act) tsikli tezlashadi, bu esa operativ ustunlikni oshiradi. UAV (dronlar), koinot razvedkasi, signals intelligence (SIGINT), imagery intelligence (IMINT) va boshqa tadqiqot usullari katta hajmdagi raqamli ma’lumotlarni (big data) hosil qiladi.

Sun’iy 293ac hora293 va mashina o‘rganishi bunday ma’lumotlarni filtrlash, yuzaki signallarni aniqlash va xabardorlik darajasini oshirishda muhim vositadir. Ma’lumotlarni tez va ishonchli tarzda birlashtirish (data fusion) razvedka samaradorligini oshiradi. Axborot maydoni amaliy va strategik darajada jang maydoniga aylanib bormoqda. Qurolli kuchlar tizimlariga nisbatan kiberhujumlar (infrastruktura buzilishi, ziyon yetkazish, ma’lumot o‘g‘irlash), shuningdek dezinformatsiya va psixologik operatsiyalar xavfi ortmoqda. Shu bois kibermudofaa bo‘limlari, kiberqo‘shinlar va ma’lumot xavfsizligi siyosatlari majburiy shartga aylandi. Kiberoperatsiyalarning qonuniy-axloqiy chegaralari, atribyutsiya muammosi va xakerlikka qarshi huquqiy chora-tadbirlar muhim muhokama mavzusi hisoblanadi. AT logistika jarayonlarini avtomatlashtirib, ta’minot zanjirini optimallashtiradi. IoT sensorlari va prediktiv texnik xizmat (predictive maintenance) vositalari texnik nosozliklarni oldindan aniqlash va harbiy texnikani samarali boshqarishga yordam beradi. Raqamli tizimlar yordamida zaxira ashyolar, yoqilg‘i, o‘q-dorilar va transport bilan bog‘liq jarayonlar real vaqtda kuzatish imkoniyatiga ega bo‘ladi. VR/AR trenerlar, simulyatorlar va onlayn o‘quv platformalari harbiy xizmatchilarning treningini sifat jihatdan oshiradi. Biroq inson omili — qaror qabul qilishdagi eng muhim element bo‘lib qoladi; AT insonning kognitiv yukini kamaytirishi yoki ko‘paytirishi mumkin. Shu sababli inson-mashina hamkorligi, insonning “in-the-loop” tamoyiliga rioya qilish, psixologik barqarorlik va etik ta’lim muhimdir.

Sun’iy intellekt (AI) va avtonom tizimlar (masalan, dushman tiriklarini avtomatik aniqlovchi dronlar yoki qarash tizimlari) jangovar operatsiyalarni tubdan o‘zgartirishi mumkin. Kvant texnologiyalari va 5G/6G tarmoqlari ham kommunikatsiya va kriptoanaliz sohasida tahdid hamda imkoniyatlar tug‘diradi. Ushbu texnologiyalar bilan bog‘liq xavfsizlik (masalan, Aiga qarshi hujumlar, kvant kripto tahdidi) va huquqiy masalalar alohida e’tiborni talab etadi. Axborot operatsiyalari va kiberkurash qonuniy va etik chegaralar bilan cheklanishi kerak. Xalqaro huquq (harbiy jamoatchilik uchun qoidalarga rioya), fuqarolarga qarshi axborot operatsiyalari va sun’iy yo‘ldoshdan foydalanish bo‘yicha qonuniy

asoslar muhim. Avtonom qurollar masalasida “insan nazorati” tamoyili — asosiy talablardan biri sifatida muhokama qilinmoqda.

Amalga oshirishdagi muammolar va cheklovlar. Interoperabellik: turli platformalar va yetkazib beruvchilar tizimlari o‘rtasida moslashuv muammosi. Legacy-sistemalar: eski tizimlarni yangilash qiyin va qimmat. Kadrlar tanqisligi: kiber-mutaxassislar va AI muhandislarga bo‘lgan talab yuqori.

Moliyalashtirish: har doim cheklangan budjet va prioritetlar. Xavfsizlik va ishonchlilik: uzluksizlik, zaifliklar va supply-chain hujumlari xavfi. Qonunchilik va siyosiy cheklovlar: xalqaro hamkorlik va ma’lumot almashinuvida cheklovlar.

Amaliy misollar va saboq. Estoniya 2007 yildagi kiberhujumlari: davlat infrastrukturasi va raqamli xizmatlarga qarshi amalga oshirilgan keng miqyosli hujumlar kibermudofaaning qanday muhimligini namoyon etdi. Zamonaviy ziddiyatlarda dron va raqamli razvedkaning roli: (turli zonalarda kuzatilgan tajribalar) real vaqt ma’lumotlarining jangovar samaradorlikka ta’siri yaqqol ko‘rinadi. (Bu misollar sifatida umumiy tarzda ko‘rsatilgan; har bir voqea bo‘yicha chuqur tahlil alohida tadqiqotni talab qiladi.)

Strategik tavsiyalar.

1. Milliy kiberstrategiyani kuchaytirish: markazlashtirilgan, ammo bo‘linma asosida faoliyat yurituvchi kibermudofaa tizimini rivojlantirish.

2. C4ISR infratuzilmasini modernizatsiya qilish: standartlar, shifrlash va ma’lumot almashinuvi protokollarini joriy etish.

3. Kadrlarni tayyorlash va qayta tayyorlash: yuqori malakali kiber va AT mutaxassislarini tayyorlash, sarmoya kiritish.

4. Ta’lim va tadqiqot (R&D): AI, kvant va avtonom tizimlar bo‘yicha milliy ilmiy dasturlar va sanoat hamkorligini mustahkamlash.

5. Xalqaro hamkorlik va ma’lumot almashinuvi: ittifoqchilar bilan kiber razvedka va mudofaa sohasida hamkorlik.

Xulosa. Axborot texnologiyalari qurolli kuchlar tizimining barcha jihatlariga kirib bordi va kelajakdagi harbiy-siyosiy muvozanatda hal qiluvchi omilga aylanmoqda. C4ISR, ISR, kibermudofaa, logistika va

ta’lim sohalarida Atni chuqur integratsiya qilish orqali harbiy samaradorlikni sezilarli oshirish mumkin. Biroq buni amalga oshirishda huquqiy-etik me’yorlar, inson omili va uzluksizlik (rezilyentlik)ni birinchi o‘ringa qo‘yish zarur. Milliy strategiya, kadrlar tayyorlash va xalqaro hamkorlik 295ac h’lda asosiy ustuvorlik bo‘lishi lozim.

Foydalanilgan adabiyotlar:

1. Alberts, D.S., Garstka, J., & Stein, F. — Network Centric Warfare: Developing and Leveraging Information Superiority (tanlangan bosma yoki hisobotlar).

2. Castells, M. — The Information Age: Economy, Society and Culture (Wiley-Blackwell, turli nashrlar).

3. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) — tahliliy materiallar va hisobotlar.

4. Turli mamlakatlar Mudofaa vazirliklari va kiberstrategiya hujjatlari (oq qog‘ozlar, strategik hisobotlar).

5. To‘laganov A. — Axborot texnologiyalari va milliy xavfsizlik (Toshkent, 2022).

6. Xalqaro ilmiy jurnallar: Journal of Strategic Studies, Military Technology Review, Journal of Cybersecurity va boshqalar.

RAQAMLI ASRDA KRIPTOGRAFIYA VA XABARLAR XAVFSIZLIKNI TA’MINLASH

Jabborova M

O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti talabasi

Axborot va internet yer yuzini ko‘rganidan beri insonlar ijtimoiy tarmoqlar orqali turli xil ma’lumotlarni almashadi. Xabarlarning xavflilik darajasini bilish yoxud sodir bo‘lishi mumkin bo‘lgan xavfni bartaraf etish, oldini olish uchun ularni o‘qish insonlarning huquqlari jiddiy tarzda buzish hisoblanadi. Axborotlarning maxfiyligi insonlar uchun juda muhim, chunki u shaxsiy hayotning daxlsizligini ta’minlaydi va insonlarning erkinligini muhofaza qiladi. Zamonaviy dunyoda axborot maxfiyligi nafaqat shaxsiy manfaatlar uchun, balki ijtimoiy barqarorlik va xavfsizlik uchun ham katta ahamiyatga ega.

Axborot maxfiyligining ahamiyati- shaxsiy hayotni himoya qilish – har bir inson shaxsiy hayotiga boshqalar aralashmasligini xohlaydi. Agar shaxsiy ma'lumotlar, masalan, telefon raqamlari, bank ma'lumotlari yoki sog'liqqa doir ma'lumotlar oshkor bo'lsa, bu insonga moliyaviy yoki emotsional zarar yetkazishi mumkin. Ijtimoiy erkinlikni saqlash – axborot maxfiyligi odamlarga o'z fikrlarini erkin bayon qilish va harakat qilish imkonini beradi. Agar insonlar kuzatuvda ekanini bilsa, ular o'zini erkin his qilmasligi mumkin. Kiberxavfsizlik – shaxsiy ma'lumotlar firibgarlar yoki hakerlar qo'liga tushsa, u ayniqsa moliyaviy yoki shaxsiy zararga olib kelishi mumkin. Masalan, shaxsiy ma'lumotlar suiiste'mol qilinib, kimningdir shaxsiy akkauntlari yoki pullari o'g'irlanishi mumkin. Ishonchli aloqalarni qo'llab-quvvatlash – axborot maxfiyligi davlat, biznes yoki shaxslar o'rtasida ishonchli munosabatlarni o'rnatish uchun asos bo'ladi. Agar ma'lumotlar maxfiyligiga kafolat bo'lmasa, odamlar kompaniyalar yoki davlat xizmatlariga ishonchsiz bo'ladi.

Xabarlarni shifrlash va ularning xavfsizligini ta'minlashda kriptografiyaning ham ahamiyati katta. Kriptografiya – bu ma'lumotni faqat vakolatli shaxslar tushunadigan shaklga aylantirish orqali himoya qilish fan va amaliyotidir. U ma'lumotlarning maxfiyligini, yaxlitligini, haqiqiyligini va ruxsatsiz kirishdan himoya qilishni ta'minlash uchun ishlatiladi. Kriptografiya" atamasi dastlab "yashirish, yozuvni berkitib qo'ymoq" ma'nosini bildirgan. Birinchi marta u yozuv paydo bo'lgan davrlardayoq aytib o'tilgan. Hozirgi vaqtda kriptografiya deganda har qanday shakldagi, ya'ni diskda saqlanadigan sonlar ko'rinishida yoki hisoblash tarmoqlarida uzatiladigan xabarlar ko'rinishidagi axborotni yashirish tushuniladi. Kriptografiyani raqamlar bilan kodlanishi mumkin bo'lgan har qanday axborotga nisbatan qo'llash mumkin. Maxfiylikni ta'minlashga qaratilgan kriptografiya kengroq qo'llanilish doirasiga ega. Aniqroq aytganda, kriptografiyada qo'llaniladigan usullarning o'zi axborotni ximoyalash bilan bog'liq bo'lgan ko'p jarayonlarda ishlatilishi mumkin.

Bugungi kunda respublikada axborotni kriptografik himoyalashni ta'minlash maqsadida kompleks chora-tadbirlar amalga oshirilmoqda.

O‘tgan davr mobaynida respublikaning qator oliy ta’lim muassasalarida axborot tizimlari va texnologiyalari, axborot xavfsizligi, kiberxavfsizlik injiniringi hamda kriptografiya va kriptotahlil yo‘nalishlari va mutaxassisliklari bo‘yicha yuqori malakali kadrlarni tayyorlash tizimi yo‘lga qo‘yildi. Shu bilan birga, axborot va kiberxavfsizlik sohasidagi zamonaviy tahdidlarning oshib borishi, kvant texnologiyasiga asoslangan tezkor kompyuterlarning yaratilishi va kelgusida ulardan noqonuniy maqsadlarda foydalanish imkoniyatining mavjudligi, axborotni himoyalashda qo‘llanadigan kriptografik algoritmlarni doimiy ravishda takomillashtirib borishni taqozo etadi. Ushbu sohada ilg‘or xorijiy davlatlar erishgan yutuqlar milliy kriptologiya maktabini yanada rivojlantirishga qaratilgan chora-tadbirlarni amalga oshirish zaruratini ko‘rsatmoqda.

Uning turlari va usullari, qo‘llanilish jarayon va uslublari ham turli xil shakllarda namoyon bo‘lgan va hozirgi kunda ham o‘z samaralarini bermoqda. Har bir narsaning ikki tomoni bo‘lgani kabi ushbu soha ya’ni kriptogragiyaning ham ijobiy va salbiy tomonlari juda ham ko‘p va keng tarqalgan. Uning bir qator ijobiy tomonlari mavjud:

1. Ma’lumotlarning maxfiyligini ta’minlash- Kriptografiya ma’lumotlarni shifrlash orqali ularga ruxsatsiz kirishni oldini oladi. Masalan, onlayn bank operatsiyalarida ma’lumotlar shifrlangani uchun faqatgina huquqli tomonlar ularga kirish huquqiga ega bo‘ladi.

2. Ma’lumotlarning yaxlitligini saqlash- Kriptografiya ma’lumotlarga uchinchi tomon tomonidan o‘zgartirish kiritilmaganligini tasdiqlash imkonini beradi. Hash funksiyalari yordamida fayllarning buzilmaganligiga ishonch hosil qilinadi.

3. Autentifikatsiya- Kriptografiya orqali foydalanuvchilar va tizimlar o‘zlarining haqiqiyligini tasdiqlashlari mumkin. Bu, ayniqsa, onlayn tizimlarda kiberhujumlardan himoya qilish uchun muhimdir.

4. Raqamli imzolar- Kriptografik texnologiyalar hujjatlar uchun raqamli imzolar yaratish imkonini beradi, bu esa hujjatning haqiqiyligini va muallifligini tasdiqlaydi.

5. E'tibordan chetda bo'lish- Shifrlangan ma'lumotlarni to'g'ridan-to'g'ri tushunish qiyin bo'lgani sababli, ular kiberjinoyatchilar tomonidan hujumga uchrashi ehtimoli pastroq bo'ladi.

6. Tizimlarning xavfsizligini oshirish- Tarmoq xavfsizligi, jumladan VPN, SSL/TLS protokollari, va xavfsiz pochta xizmatlari kriptografik algoritmlarga tayanadi.

7. Axborot almashish imkoniyatlari-Kriptografiya yordamida turli tomonlar o'zaro ishonchli va xavfsiz ma'lumot almashish imkoniga ega bo'ladilar. Bu ayniqsa harbiy va moliyaviy sohalarda dolzarbdir.

Shu o'rinda qonunchiligimizda ham Maxfiy axborotni kriptografik muhofaza qilish vositalari va kriptotizimdan foydalanish va ta'mirlashga O'zbekiston Respublikasi davlat sirlari bilan ishlashga qonun hujjatlarida belgilangan tartibda ruxsat berilgan shaxslargagina ruxsat etiladi.

Kriptografiya ko'plab afzalliklarga ega bo'lsa-da, uning ba'zi salbiy tomonlari va cheklovlari ham mavjud. Quyida asosiy salbiy jihatlar keltirilgan: Murakkablik va resurs talabchanligi – kriptografik algoritmlar ko'p hollarda murakkab hisoblashlarni talab qiladi, bu esa tizimning ishlashiga salbiy ta'sir ko'rsatishi va resurslarni (CPU, xotira) ko'proq iste'mol qilishi mumkin. O'z vaqtida eskirish xavfi – kriptografik algoritmlar vaqt o'tishi bilan eskiradi. Masalan, ilgari xavfsiz hisoblangan algoritmlar (MD5, SHA-1) bugungi kunda zaif bo'lib qoldi. Shuning uchun algoritmlarni muntazam yangilab turish zarur. Noto'g'ri qo'llanilishi – kriptografiyani noto'g'ri sozlash yoki qo'llash tizim xavfsizligiga jiddiy xavf tug'dirishi mumkin. Masalan, kalitlarni noto'g'ri boshqarish yoki zaif shifrlash algoritmlaridan foydalanish xavfsizlikni buzadi. Kriptografik kalitlarni boshqarish muammosi – kalitlarning xavfsiz saqlanishi va boshqarilishi muhimdir. Agar kalit yo'qolsa yoki buzilib qolsa, ma'lumotlarga kirish imkoni butunlay yo'qolishi mumkin. Bundan tashqari, kalitlarning noto'g'ri qo'llanishi ma'lumotlarning oshkor bo'lishiga olib kelishi mumkin. Jinoyatchilar tomonidan foydalanilishi – kriptografiya jinoyatchilar tomonidan ham noqonuniy faoliyatlarini yashirish uchun ishlatilishi mumkin. Masalan, shifrlangan aloqa vositalari kiberjinoyatlar yoki terrorizm maqsadlarida qo'llaniladi. Hujumlarning

rivojlanishi- kriptografik tizimlar doimiy ravishda yangi hujum usullariga qarshi himoyaga muhtoj. Masalan, kvant kompyuterlarning rivojlanishi bugungi kriptografiya asoslarini zaiflashtirishi mumkin. Qo‘shimcha xarajatlar – kriptografiya texnologiyalarini joriy qilish va boshqarish ko‘pincha qo‘shimcha xarajatlarni talab qiladi, masalan, sertifikatlar sotib olish, yangi algoritmlar bo‘yicha mutaxassislarni tayyorlash va boshqalar. Foydalanuvchilar uchun noqulayliklar- kriptografiyadan foydalanish ba’zan foydalanuvchilar uchun noqulaylik tug‘diradi. Masalan, murakkab parollarni eslab qolish, ikki faktorli autentifikatsiya va boshqa xavfsizlik choralarini qabul qilish qo‘shimcha vaqt va e’tibor talab qiladi. Ma’lumotlarga kirishning yo‘qolishi- agar shifrlash kaliti yo‘qotilsa, shifrlangan ma’lumotlarga hech qanday yo‘l bilan kirib bo‘lmaydi. Bu kompaniya yoki shaxs uchun katta zarar yetkazishi mumkin

Kriptografiya – bu axborotni shifrlash va uni ruxsatsiz kirishdan himoya qilish usullari bilan shug‘ullanuvchi fan. Ko‘plab olimlar va mutaxassislar kriptografiya haqida turli fikrlar bildirgan. Quyida ba’zi mashhur olimlarning fikrlarini misol keltirish mumkin:

Klod Shennon (1916–2001) – Zamonaviy axborot nazariyasi asoschisi: “Yaxshi kriptotizim shunday bo‘lishi kerakki, dushman tizim ichidagi barcha narsani bilsa ham, baribir xabarning ma’nosini tushunolmasin.” Shennon kriptografiyani matematik asosda o‘rganib, shifrlashning xavfsizlik jihatlarini chuqur tadqiq qilgan. U “Mukammal maxfiylik” (Perfect Secrecy) tushunchasini ishlab chiqqan.

Bruce Schneier – zamonaviy kriptografiya eksperti : “Kriptografiya – bu nafaqat matematikaga, balki tizim xavfsizligiga ham bog‘liq. Eng kuchli shifr ham noto‘g‘ri ishlatilsa, foydasiz bo‘lib qoladi.” Schneier amaliy kriptografiya bo‘yicha ko‘plab kitoblar yozgan va zamonaviy xavfsizlik muammolari haqida keng fikr bildirgan.

Whitfield Diffie va Martin Hellman – Ochiq kalitli kriptografiyaning asoschilari: “Kriptografiya orqali biz bir-birimizga ishonmasak ham, axborot almashishimiz mumkin.” Diffie va Hellman 1976-yilda ochiq kalitli kriptografiya g‘oyasini ilgari surishgan. Bu kriptografik tizimlar rivojlanishida inqilobiy o‘zgarish bo‘ldi.

Adi Shamir – RSA algoritmining hammuallifi: “Kriptografiyada xavfsizlik faqat matematik model bilan emas, balki amaliy tajribalar va hujumlar bilan ham tekshirilishi kerak.” RSA algoritmi zamonaviy shifrlash tizimlarida eng ko‘p ishlatiladigan algoritmlardan biridir.

Edward Snowden – Axborot xavfsizligi bo‘yicha tanqidchi: “Kriptografiya – bu shaxsiy hayot va erkinlikni saqlab qolishning oxirgi vositasidir.” Snowden kriptografiyaning inson huquqlari va maxfiylikni himoya qilishdagi ahamiyatiga urg‘u bergan. Kriptografiya hozirgi kunda nafaqat kompyuter xavfsizligi, balki moliyaviy tizimlar, harbiy strategiyalar va shaxsiy ma’lumotlarni himoya qilish uchun ham juda muhim soha hisoblanadi.

Xulosa o‘rnida aytish lozimki kriptografiya sohasining asosiy vazifalari axborotlarni xavfsizligini ta’minlashdir. Kripto tushunchasi esa shifrlashning ilmiy ifodasidir. Insonlar va davlat o‘zining va boshqalarning manfaatlarini xavfsizligini ta’minlash uchun zamonaviy tarzda yaratilgan shifrlar ham texnologiyalardan foydalanmog‘i lozim. **Shifrlash** oddiy matnni shifrlangan matnga aylantirish uchun murakkab algoritmlardan foydalanadigan kriptografik usul bo‘lib, uni ruxsatsiz shaxslarga shifrlab bo‘lmaydi. Jarayon kriptografik kalitlardan foydalanishni o‘z ichiga oladi, bu yerda shifrlangan kalit ma’lumotlarni o‘zgartiradi va tegishli shifrni ochish kaliti uni asl ko‘rinishiga qaytaradi. Shifrni ochish kalitisiz shifrlangan matn tushunarsiz bo‘lib qoladi. Shifrlash – dam olish va o‘tish paytida maxfiy ma’lumotlarni himoya qilishning eng samarali usuli, ammo uni amalga oshirish va boshqarish ham eng murakkab. Bu avtorizatsiya qilingan foydalanuvchilarga to‘g‘ri shifrlash kaliti yordamida shifrlangan matnni ochiq matnga aylantirish imkonini beradi. Ikki kalitli tizim maxfiy ma’lumotlarning xavfsiz aloqasi va saqlanishini ta’minlaydi va ma’lumotlarning buzilishi va ruxsatsiz kirishdan himoya qiladi.

Bu borada qo‘shimcha sifatida internet xavfsizligini ta’minlash uchun quyidagi choralarni amalga oshirish tavsiya etiladi. Bu choralar shaxsiy va korporativ darajada xavfsizlikni oshirishga yordam beradi. ***Kuchli parollardan foydalanish***- har bir hisob uchun noyob, murakkab (katta va kichik harflar, raqamlar, maxsus belgilarni o‘z ichiga olgan)

parollar yaratish, parol menejerlaridan foydalanib, ularni xavfsiz saqlash. ***Ikki faktorli autentifikatsiyani (2FA) yoqish***- onlayn hisoblaringizda ikki faktorli autentifikatsiyani faollashtirish orqali qo‘shimcha himoya darajasini ta’minlash, SMS yoki autentifikatsiya dasturlari orqali kodlar bilan hisobga kirish tizimlarini yoqish. ***Antivirus va xavfsizlik dasturlaridan foydalanish***- qurilmangizda yangilangan antivirus dasturi va zararli dasturlarni aniqlash vositalarini o‘rnatib, ularni muntazam yangilab turish- tarmoq xavfsizligi uchun tarmoq monitoring dasturlaridan foydalanish. ***Dasturlarni yangilash***- operatsion tizim, brauzerlar va dasturlarni yangilab turish. Bu dasturlarni zararli hujumlardan himoya qiluvchi xavfsizlik yamalarini o‘z ichiga oladi. ***Shubhali havolalardan saqlanish***- pochta yoki xabarlar orqali yuborilgan noma’lum havolalarga bosmaslik, HTTPS protokoli bilan himoyalangan veb-saytlardan foydalanish. ***Jamoat Wi-Fi tarmoqlarida ehtiyot bo‘lish***- jamoat Wi-Fi tarmoqlaridan foydalanganda maxfiy ma’lumotlarni kiritmaslik, VPN xizmatlaridan foydalanganda, ma’lumotlaringizni shifrlash. ***Shaxsiy ma’lumotlarni himoyalash***- keraksiz shaxsiy ma’lumotlarni internetda baham ko‘rmaslik,i jtimoiy tarmoqlarda maxfiylik sozlamalarini tekshirib turish. ***Zaharlangan pochta va fayllardan ehtiyot bo‘lish***- pochtaga kelgan noma’lum yoki shubhali jo‘natuvchilardan xabarlar yoki fayllarni ochmaslik, qo‘shib yuborilgan fayllarni antivirus bilan tekshirib turish. ***Zaxira nusxalarini yaratish***- muhim ma’lumotlarning zaxira nusxalar yaratish. Kriptografiya internet, mobil aloqa, bank tizimlari va boshqa ko‘plab sohalarda axborotni himoya qilish uchun ishlatiladi. Zamonaviy kriptografiya murakkab matematik algoritmlar va hisoblash resurslariga asoslangan. Kompyuter quvvati oshgani sari, yangi shifrlash usullari yaratilmoqda, kvant hisoblash texnologiyasi esa mavjud kriptografik tizimlarga tahdid solmoqda. Kriptografiya nafaqat xavfsizlik, balki inson huquqlari, maxfiylik va erkinlikni himoya qilishda ham muhim vosita hisoblanadi. Kuchli kriptografik tizimlar ham noto‘g‘ri ishlatilsa yoki zaif joylari ochib berilsa, xavfsizlik zaiflashishi mumkin. Kriptografiya kelajakda axborot xavfsizligini ta’minlashda yanada muhim ahamiyat kasb etadi. Kvant kompyuterlarning rivojlanishi bilan an’anaviy shifrlash

usullari zaiflashishi mumkin, shuning uchun kvant kriptografiya yanada mustahkam va buzib bo‘lmaydigan xavfsizlik tizimlarini yaratishga yordam beradi. Bu esa bank tizimlari, hukumat ma’lumotlari va harbiy aloqa uchun yangi imkoniyatlar ochadi.

Elektron saylovlar va hujjat autentifikatsiyasida ham kriptografik texnologiyalar keng qo‘llanilib, saylov natijalarining buzilmasligi va shaxsiy hujjatlarning qalbakilashtirilishining oldini olishga yordam beradi. Shaxsiy hayotni himoya qilish masalasi ham dolzarb bo‘lib, kelajakda kuchaytirilgan shifrlash texnologiyalari yordamida foydalanuvchilar o‘z ma’lumotlarini davlatlar va korporatsiyalarning kuzatuvidan himoya qila oladi. Umuman olganda, kriptografiya kelajakda axborot xavfsizligi, moliya, sun’iy intellekt, huquqiy tizimlar va shaxsiy ma’lumotlarni himoya qilishda hal qiluvchi rol o‘ynaydi va inson hayotini yanada xavfsiz, ishonchli hamda maxfiy qiladi.

Foydalanilgan adabiyotlar:

1. Journal of Academic Research and Trends in Educational Sciences, 85-89, 2024 https://ijournal.uz

2.O‘zbekiston Respublikasida kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida O‘zbekiston Respublikasi Prezidentining qarori 15.08.2024-yildagi PQ-293-son https://lex.uz

3. O‘zbekiston Respublikasida axborotni kriptografik muhofaza qilishni tashkil etish chora tadbirlari to‘g‘risidagi Prezident qarori 03.04.2007-yildagi PQ-614-son https://lex.uz

4. https://wwwsolix.com

5. Шеннон К. Работы по теории информации и кибернетике. – М.: Наука, 1963.

6. Diffie W., Hellman M. New Directions in Cryptography // IEEE Transactions on Information Theory. – 1976. – Vol. 22(6). – P. 644–654.

7. Rivest R., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems // Communications of the ACM. – 1978. – Vol. 21(2). – P. 120–126.

8. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. – New York: John Wiley & Sons, 1996.

9. Stallings W. Cryptography and Network Security: Principles and Practice. – 7th ed. – Pearson, 2016.

10. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. – CRC Press, 1996.

11. Katz J., Lindell Y. Introduction to Modern Cryptography. – 2nd ed. – CRC Press, 2014.

12. Климов С., Шнайер Б. Прикладная криптография. – СПб.: Питер, 2003.

13. Schneier B. Secrets and Lies: Digital Security in a Networked World. – Wiley, 2015.

14. Национальная стратегия Узбекистана в области кибербезопасности. – Тошкент: O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi, 2021.

15. Қурбонов А., Абдуллаев А. Криптографик усуллар ва ахборот хавфсизлиги. – Тошкент: ТАТУ нашриёти, 2020.

16. O‘zbekiston Respublikasi “Axborotlashtirish to‘g‘risida”gi Qonuni, 2003-yil (oxirgi tahrirlar bilan).

QUROLLI KUCHLAR TIZIMIDA RAQAMLI TEXNOLOGIYALARNI QO‘LLASHNING NAZARIY-AMALIY JIHATLARI

Boymirzayeva X.F.
Jamoat xavfsizligi universiteti Maxsus fakultet 2-bosqich talabasi
Kamilov M.A.
Jamoat xavfsizligi universiteti Axborot texnologiyalari kafedrasi katta o‘qituvchisi, dotsent

So‘nggi yillarda dunyo miqyosida raqamli texnologiyalar hayotning barcha jabhalariga chuqur kirib kelmoqda. Bu jarayon qurolli kuchlar faoliyatini ham chetlab o‘tmadi. Harbiy sohada zamonaviy axborot tizimlari, sun’iy intellekt, dron texnologiyalari hamda kiberxavfsizlik vositalarining qo‘llanilishi mudofaa salohiyatini mustahkamlashda muhim omil bo‘lib xizmat qilmoqda. Shu sababli qurolli kuchlar tizimida raqamli

texnologiyalarni qo‘llashning nazariy va amaliy jihatlarini tahlil qilish bugungi kunda dolzarb masalalardan biridir.

Raqamli texnologiyalarni qo‘llash nazariy jihatdan qurolli kuchlar boshqaruvini samarali tashkil etishga, qo‘shinlar harakatini tezkor muvofiqlashtirishga, real vaqt rejimida ma’lumot almashishni ta’minlashga qaratilgan. Zamonaviy axborot-kommunikatsiya tizimlari orqali harbiy bo‘linmalar o‘rtasidagi o‘zaro hamkorlik yanada mustahkamlanadi, bu esa strategik qarorlar qabul qilish jarayonida muhim ahamiyat kasb etadi. Shuningdek, raqamli texnologiyalar yordamida jangovar sharoitni model qilish, turli vaziyatlarni oldindan aniqlash imkoniyati paydo bo‘ladi. Amaliyotda raqamli texnologiyalar keng qamrovda joriy etilmoqda. Masalan, uchuvchisiz uchish apparatlari va dronlar jangovar vazifalarni bajarishda qo‘llanilmoqda, sun’iy intellekt asosidagi razvedka tizimlari esa tezkor ma’lumot to‘plash imkonini bermoqda. Shuningdek, kiberxavfsizlikni ta’minlash dasturlari axborot makonida yuzaga keladigan xavflarga qarshi samarali himoya vositasi sifatida xizmat qilmoqda. Harbiy mashg‘ulotlarda simulyatsion dasturlar va virtual haqiqat texnologiyalaridan foydalanish qo‘shinlarning tayyorgarlik darajasini oshirishda katta samara bermoqda.

Strategik boshqaruvda raqamli texnologiyalar muhim ahamiyat kasb etadi. Masalan, “big data” tahlili asosida dushmanning ehtimoliy harakatlari prognoz qilinadi, sun’iy intellekt algoritmlari yordamida esa harbiy taktik rejalar optimallashtiriladi.Bu jarayon qo‘mondonlarning tezkor va to‘g‘ri qaror qabul qilishiga zamin yaratadi.

Biroq raqamli texnologiyalarni tatbiq etishda ayrim muammolar mavjud. Avvalo, kiberxavfsizlikka bo‘lgan tahdidlarning ortib borishi, texnik infratuzilmaning yetarli darajada rivojlanmaganligi hamda malakali mutaxassislarni tayyorlash zarurati asosiy masalalardan hisoblanadi. Bundan tashqari, harbiy sohada chet el dasturiy mahsulotlariga haddan ortiq tayanish milliy xavfsizlik uchun xavf tug‘dirishi mumkin. Shu sababli, milliy platformalar va dasturiy ta’minotlarni ishlab chiqish dolzarb ahamiyat kasb etadi.

Xalqaro tajriba shuni ko‘rsatmoqdaki, rivojlangan mamlakatlar o‘z qurolli kuchlarida raqamli transformatsiyaga alohida e’tibor qaratmoqda. NATO mamlakatlarida qo‘mondonlik markazlari real vaqt rejimida ishlaydigan yagona axborot tizimlariga ulangan bo‘lsa, Osiyo mamlakatlarida dron va robototexnika sohasida katta yutuqlarga erishilmoqda. O‘zbekiston uchun ushbu tajribalarni o‘rganish va milliy sharoitga moslashtirish muhimdir.

Huquqiy asoslar ham raqamli texnologiyalarni joriy etishda katta ahamiyatga ega. “Mudofaa to‘g‘risida”gi qonun, “Kiberxavfsizlik to‘g‘risida”gi qonun va “Raqamli O‘zbekiston – 2030” strategiyasi mazkur yo‘nalishdagi islohotlarning huquqiy zaminini yaratadi. Bu esa qurolli kuchlar tizimida raqamli texnologiyalarni keng joriy etishga imkon beradi.

Mazkur muammolarni hal etish uchun muntazam ravishda harbiy xizmatchilarni raqamli texnologiyalar bilan ishlash bo‘yicha o‘qitish, ilg‘or xorijiy tajribalarni o‘rganish, milliy dasturiy ta’minotlarni ishlab chiqish va kiberxavfsizlikni kuchaytirishga qaratilgan islohotlarni amalga oshirish zarur. Kelajakda raqamli transformatsiya qurolli kuchlarning jangovar imkoniyatlari va boshqaruv samaradorligini sezilarli darajada oshirishi kutilmoqda.

Qurolli kuchlar tizimida raqamli texnologiyalarni qo‘llash nazariy va amaliy jihatdan ham dolzarbdir. Ular harbiy xavfsizlikni mustahkamlash, boshqaruv tizimini takomillashtirish va jangovar tayyorgarlik samaradorligini oshirishga xizmat qiladi. Shu bilan birga, mavjud muammolarni bartaraf etish va ilg‘or yechimlarni joriy etish orqali qurolli kuchlar salohiyatini yangi bosqichga olib chiqish mumkin.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasining Konstitutsiyasi (2023-yilgi tahriri). – lex.uz

2. “Mudofaa to‘g‘risida”gi Qonun, 2001-yil 11-may, O‘RQ–240. – lex.uz

3. “Axborotlashtirish to‘g‘risida”gi Qonun, 2003-yil 11-dekabr, O‘RQ–560. – lex.uz

4. “Kiberxavfsizlik to‘g‘risida”gi Qonun, 2022-yil 15-aprel, O‘RQ–776. – lex.uz

5. O‘zbekiston Respublikasi Prezidenti qarori: “Raqamli O‘zbekiston – 2030” strategiyasini amalga oshirish chora-tadbirlari to‘g‘risida”, PQ–6079-son, 2020-yil 5-oktabr. – lex.uz

6. To‘rayev, A. Harbiy xavfsizlikni ta’minlashda axborot-kommunikatsiya texnologiyalarining o‘rni. – Toshkent: “Iqtisodiyot va huquq” jurnali, 2023.

7. Karimov, B. Kiberxavfsizlik va mudofaa sohasida raqamli transformatsiya. – “Yuridik fanlar axborotnomasi”, 2022, №4.

FAVQULODDA HOLATLARDA UCHUVCHISIZ UCHISH APPARATLARI YORDAMIDA VIDEOAXBOROTLARNI TEZKOR UZATISH VA TAHLIL QILISH

Ziyayev B.N.
O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti
magistratura tinglovchisi

Zamonaviy jamiyatda tabiiy ofatlar (yer qimirlashi, suv toshqinlari, yong‘inlar) va texnogen avariyalar ko‘plab mamlakatlar uchun katta xavf tug‘dirmoqda. Bunday holatlarda qutqaruv ishlarining samaradorligi to‘g‘ri va tezkor axborot bilan ta’minlanish darajasiga bog‘liq. Uchuvchisiz uchish apparatlari (UUA) ana shunday vaziyatlarda axborot yig‘ish va yetkazib berishning eng ishonchli manbalari sifatida namoyon bo‘lmoqda.

UUA’lar yuqori sifatli kamera va sensorlar bilan jihozlanib, joriy vaqt rejimida axborot uzatish imkoniyatiga ega. Ular inson hayoti uchun xavfli hududlarga kirib bormasdan turib, qutqaruvchilarga aniq va ishonchli ma’lumot yetkazib beradi. Shu bilan birga, sun’iy intellekt texnologiyalari orqali yig‘ilgan videoma’lumotlarni tahlil qilish qutqaruv ishlarida muhim qarorlarni tez qabul qilishga yordam beradi.

UUAlar yordamida videoaxborotlarni yig‘ish va uzatish

Uchuvchisiz uchish apparatlari zamonaviy kameralar, infraqizil sensorlar va teplovizorlar bilan jihozlangan. Ular yordamida yong‘in

manbalari, suv toshqini hududlari yoki avariya sodir bo‘lgan obyektlar haqida joriy vaqt rejimida ma’lumot yig‘iladi.

Ma’lumotlarni uzatishda LTE, 5G va maxsus radiokanallardan foydalaniladi. 5G tarmog‘i katta hajmdagi videopotoklarni yuqori tezlikda va kechikishsiz uzatish imkonini beradi. Bu qutqaruv ishlarida har daqiqa muhim hisoblangan vaziyatlarda juda katta ustunlikdir.

Sun’iy intellekt texnologiyalari

Sun’iy intellekt videoma’lumotlarni tahlil qilish jarayonida quyidagi vazifalarni bajaradi:

Avtomatik obyekt aniqlash. Dronlar orqali olingan tasvirlarda odamlar, texnika va xavfli obyektlar tezda aniqlanadi.

Sifatni oshirish. AI algoritmlari yordamida tuman, yomg‘ir yoki yomon yoritish sharoitida ham aniq tasvir olish mumkin.

Edge Computing. UUA’ning o‘zida dastlabki qayta ishlash amalga oshirilib, markaziy serverga faqat muhim ma’lumot uzatiladi. Bu tarmoq yuklamasini kamaytiradi va tezkorlikni oshiradi.

Shu orqali qutqaruv xizmatlari tezkor qaror qabul qilishi va inson hayotini saqlab qolishi mumkin bo‘ladi.

Xavfsiz ma’lumot uzatish

Favqulodda holatlarda yig‘ilgan ma’lumotlar strategik ahamiyatga ega. Shuning uchun ularni xavfsiz uzatish muhim. Kiberxavfsizlikni ta’minlash maqsadida kriptografik shifrlash, autentifikatsiya va ma’lumotlarning dublikat kanallar orqali uzatilishi qo‘llaniladi. Masalan, LTE tarmog‘i ishdan chiqsa, ma’lumot maxsus radiochastota orqali uzatilishi mumkin.

Amaliyotda qo‘llanilishi

Tabiiy ofatlarda. Yer qimirlashidan keyin zarar ko‘rgan binolarni baholash va evakuatsiya yo‘nalishlarini belgilash.

Yong‘inlarda. Issiqlik tarqalishini kuzatib, xavfli joylarni qutqaruvchilar uchun belgilash.

Texnogen avariyalarda. Gaz va neft quvurlaridagi yoriqlarni aniqlab, portlashlarning oldini olish.

Infratuzilmani nazorat qilish. Yirik energetika tarmoqlari va ko‘priklarni muntazam kuzatish.

XULOSA

Favqulodda holatlarda UUAlardan foydalanish inson hayotini saqlash va zararni kamaytirishda muhim ahamiyatga ega. Joriy vaqt rejimida axborot uzatish va sun'iy intellekt yordamida tahlil qilish qutqaruv ishlarini samarali tashkil etish imkonini beradi. Shu bilan birga, xavfsiz ma'lumot uzatish usullari kelgusida bu tizimlarni yanada ishonchli qiladi.

Foydalanilgan adabiyotlar:

1. Abdullayev A., "Uchuvchisiz uchish apparatlari texnologiyalari", Toshkent, 2022.
2. Raxmonov I., "Axborot tizimlarida sun'iy intellekt qo'llanilishi", Samarqand, 2021.
3. Xamidov SH., "Kiberxavfsizlik va axborot muhofazasi", Toshkent, 2020.
4. Hasanov B., "Drones in Disaster Management: Real-time Data Transmission and AI Analysis", Tashkent, 2023.
5. *Journal of Unmanned Systems and AI Applications*, 2024 yilgi maxsus son.

YOLO ALGORITMI ASOSIDA JETSON NANO QURILMASIDA REAL VAQT REJIMIDA ODAM VA VELOSIPEDLARNI ANIQLASH VA SON JIHATDAN MONITORING QILISH USULLARINI ISHLAB CHIQISH

Mambetsharipov Y.R.

Jamoat xavfsizligi universiteti axborot texnologiyalari kafedrasi dotsenti, t.f.f.d (PhD)

Obyektlarni videokuzatuv kameralardan foydalanib avtomatik tarzda yuqori aniqlik va ishonchlilik bilan hisoblash uzoq vaqt davomida izlanayotgan muammo hisoblanadi. Obyektlarni aniqlash va hisoblash odatdagiga nisbatan osonroq bo'lsa - da, tashqi ya'ni noaniq muhitlarda bu jarayon yanada murakkablashadi. Bunga atrof muhitning tabiati, obyektlarning o'lchami, shakli, orientatsiyasi va fonning murakkabligi kabi omillar sabab bo'ladi. Shu sababli, real vaqtda obyektlarni aniqlash va hisoblash uchun samarali va energiya sarfi tejamkorligi yechimlari zarur.

Chekka hisoblash (edge computing) texnologiyalari, ayniqsa Jetson Nano kabi kichik va quvvatni tejaydigan qurilmalar, bu sohada muhim imkoniyatlar yaratadi. YOLO (You Only Look Once) kabi chuqur o‘rganish tarmoqlari va V-IOU kabi kuzatuv algoritmlari yordamida obyektlarni aniqlash va kuzatish jarayonlarini optimallashtirish mumkin. Biroq, real vaqtda ishlashni ta’minlash uchun ramka tezligini oshirish, xotira ishlatishni kamaytirish va energiya sarfini optimallashtirish kabi masalalarni hal qilish zarur. Ushbu ishda, real vaqtda obyektlarni aniqlash va hisoblash uchun YOLO tarmog‘i va V-IOU kuzatuvchisi qo‘llanilib, selektiv ramka kamaytirish algoritmi yordamida tizimning samaradorligi oshirilgan. So‘nggi yillarda obyektlarni aniqlash va kuzatish uchun turli algoritmlar va usullar taklif etilgan. Fachrie va boshqalar YOLOv3 modelidan foydalanishni taklif qilishgan, ammo ularni har bir kadrda kuzatish algoritmi bilan qo‘llashni ko‘rsatmagan. Bharadhwaj va boshqalar Tiny-YOLO modelini Knowledge Distillation bilan yaxshilab, SORT kuzatuvchisini qo‘llaganlar. OpenDataCam esa real vaqtda obyektlarni aniqlash uchun ochiq manba kodli to‘plamni taqdim etadi. Bochkovskiy va boshqalar YOLOv4 va Tiny-YOLOv4 modellaridan foydalanib, IOU kuzatuvchisining modifikatsiyalangan versiyasini qo‘llaganlar.

So‘nggi yillarda, obyektlarni aniqlash va kuzatish sohasida turli yondashuvlar taklif etilgan. Ultralytics tomonidan ishlab chiqilgan YOLOv5 modeli, turli o‘lchamdagi arxitekturalar va MAP (mean Average Precision) ko‘rsatkichlari bilan taqdim etilgan. OpenDataCam loyihasida ishlatilgan IOU kuzatuvchisi, vizual kuzatuvchi bilan kengaytirilgan bo‘lib, V-IOU kuzatuvchisini tashkil etgan.

Bundan tashqari, SORT kuzatuvchisi, DeepSORT bilan yangilangan bo‘lib, unda masofa o‘lchovchisi sifatida konvolyutsion neyron tarmog‘i (CNN) qo‘llanilgan.

Ushbu ishda, real vaqtda odamlar va velosipedlarni aniqlash, kuzatish va hisoblash uchun optimallashtirilgan tizim taqdim etiladi. Tizim Nvidia Jetson Nano 2 GB chekka sun’iy intelekt qurilmasida joylashtirilgan bo‘lib, turli tezlikdagi obyektlarni samarali tarzda qayta ishlash imkonini beradi. Aniqlash moduli YOLOv5 algoritmiga asoslangan bo‘lib, IOU va

V-IOU kuzatuvchilari bilan birgalikda ishlaydi. Bundan tashqari, tizim obyektlarning tezligiga asoslangan selektiv ramka kamaytirish algoritmini qo‘llaydi, bu esa kadr tezligini obyektlarning harakatiga qarab moslashtirish imkonini beradi. Natijada, tizim kerakli bo‘lmagan kadrlarni e’tibordan chetda qoldirib, real vaqtda ishlashni ta’minlaydi va kuzatuv samaradorligini saqlaydi. Eksperimentlar natijasida, selektiv ramka kamaytirish algoritmasi xotira ishlatishni kamaytirish va aniqlikni saqlashda muvaffaqiyatli bo‘lgan.

Biroq, yuqorida keltirilgan barcha yondashuvlar, past quvvatli chekka sun’iy intelekt qurilmalarida ishlashda samaradorlikni saqlashda qiyinchiliklarga duch kelgan. Bu sharoitda, manzilli holatlarda og‘irroq, lekin samaraliroq hisoblash modellarini va kuzatuv algoritmlarini joriy etish chekka hisoblash muhitida ko‘pincha imkonsiz bo‘ladi, chunki qurilmalar cheklangan hisoblash quvvati, xotira va energiya manbalariga ega. Turli usullar obyektlarni real-vaqtli video kadrlarida aniqlash va hisoblash muammosini hal etishga yo‘naltirilgan. Muhammad Fachrie va boshqalar [1] – mos ravishda YOLOv3 tarmog‘idan foydalangan transport vositalarini hisoblash tizimini taklif etdilar. Ushbu tarmoq oldindan MS COCO to‘plamida o‘qitilgan edi. To‘liq Kadrma-kadr obyekti kuzatuvchisidan foydalanish o‘rniga, mualliflar aniqlangan obyektning markaziy nuqtasi (centroid) bilan hisoblash chizig‘i orasidagi masofani hisoblashga asoslangan soddalashtirilgan usulni qo‘llaganlar, va agar bu masofa ma’lum threshold qiymatdan kichik bo‘lsa, obyekt hisobga qo‘shilgan. Shu bilan birga, bir xil transport vositasining bir necha marta hisobga olinmasligi uchun uchta ketma-ket kadr tahlil qilingan va ularning markaziy nuqtalari oldingi kadr bilan solishtirilgan. Natijada, faqat oldidan qarashli yo‘l manzarasida olingan video uchun 97.72 % aniqlik darajasiga erishilgan.

Obyektlarni aniqlash modellari

So‘nggi yillarda obyektlarni aniqlash sohasi sezilarli darajada rivojlandi. Dastlab, R-CNN (Region-based Convolutional Neural Network) tarmog‘i taklif qilinib, mavjud modellar bilan solishtirganda yuqori mAP (mean Average Precision) ko‘rsatkichlariga erishilgan. Ushbu

model uch bosqichda ishlaydi: avvalo, taxminan 2000 ta region taklifi ajratiladi, keyin har bir region uchun xususiyatlar olinadi, va nihoyat, har bir sinf uchun tayyorlangan SVM yordamida klassifikatsiya amalga oshiriladi. Biroq bu yondashuv katta hisoblash resurslarini talab qiladi. Shuning uchun keyinchalik Fast R-CNN va Faster R-CNN kabi optimallashtirilgan arxitekturalar ishlab chiqildi.

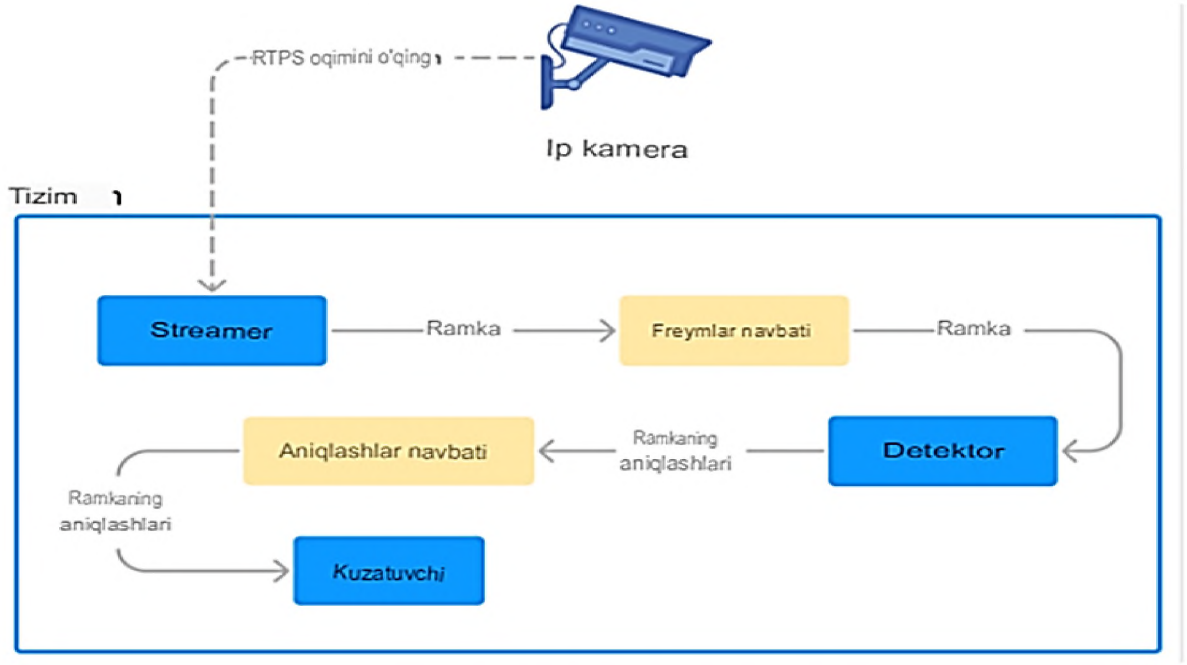
YOLO (You Only Look Once) algoritmi esa Redmon va boshqalar tomonidan taklif qilinib, obyektlarni aniqlash muammosini yagona regressiya muammosiga aylantirdi. Tasvir S × S panjaraga bo‘linadi, va har bir panjara bo‘lagi obyekt markaziga to‘g‘ri kelsa, u obyektni aniqlash uchun javobgar bo‘ladi. Model bir nechta bounding box’lar, ularning ishonchlilik koeffitsientlari va klass ehtimollarini bashorat qiladi. YOLOning dastlabki versiyalari kichik obyektlarni aniqlashda aniqligi past bo‘lgan, biroq keyingi versiyalar, jumladan YOLOv4 va YOLOv5, bu muammolarni sezilarli darajada kamaytirgan.

Tizim arxitekturasi va modullarning ishlash tartibi

Taklif etilgan tizim arxitekturasi Bharadhwaj va boshqalar tomonidan ilgari surilgan “aniqlash–kuzatish–hisoblash” ketma-ketligiga asoslangan. Ushbu arxitekturaning umumiy ko‘rinishi 1-rasmda tasvirlangan. Tizim uchta asosiy moduldan iborat: Video oqimini olish moduli – bu modul real vaqt rejimida video kadrlarni uzluksiz qabul qiladi. Obyekt aniqlash moduli – har bir kadrda mavjud obyektlarni aniqlash uchun mas’ul bo‘lib, YOLOv5 modeliga asoslanadi. Kuzatuv va hisoblash moduli – aniqlangan obyektlarni ketma-ket kadrlar bo‘ylab kuzatib boradi va ular hisoblash chizig‘ini kesib o‘tganda hisobga oladi.

Har bir modul alohida jarayon sifatida bajariladi va ular o‘zaro xabar navbatlari (queue) orqali bog‘langan. Bunday arxitektura modullarni parallel ishlashga imkon beradi va ketma-ket bajarilishga nisbatan samaradorlikni oshiradi. Jarayonlar o‘rtasidagi sinxronlash muammolarining oldini olish uchun multiprocessing.Queue klassidan foydalanilgan bo‘lib, u blokirovka va semaforlar yordamida xavfsiz ma’lumot almashinuvini ta’minlaydi.

Video oqimi moduli kadrlarni 15 FPS tezlikda aniqlash moduliga uzatadi. Aniqlash moduli esa har bir kadrda tegishli obyektlarni aniqlab, ularni kuzatuv moduliga yuboradi. Kuzatuv moduli mavjud obyektlar bilan moslikni aniqlaydi yoki yangi kuzatuv yo‘llarini yaratadi.



1-rasm. Tizim arxitekturasi

Agar kuzatuv yo‘li hisoblash chizig‘i bilan kesishsa, u holda obyekt hisobga olinadi. Tizim arxitekturasi moslashuvchan tarzda ishlab chiqilgan bo‘lib, kelajakda yangi aniqlash modellarini yoki kuzatuv algoritmlarini integratsiya qilish imkonini beradi.

YOLOv5s arxitekturasi real-vaqtli aniqlash uchun yaxshiroq natijalar berdi, ammo uning ramka navbati doimiy ravishda yangi ramkalar bilan to‘ldirilishi tizimning xotira resurslarini tezda tugatishiga olib kelishi mumkin, bu esa hozirgi loyiha uchun nojo‘ya hisoblanadi.





klassga bog‘liq bo‘lmagan NMS dan oldin

klassga bog‘liq bo‘lmagan NMS dan keyin

Agar tizim YOLOv5n yordamida olinadigan ramkalarni o‘tkazib yuborsa, navbatni osonlik bilan bo‘shatishi mumkin, lekin YOLOv5s bilan bu navbat har soniyada taxminan besh ramkaga ortib boradi. Uzoq video yoki real-vaqtli tasvirlarni tahlil qilishda Jetson Nano xotirasi tugashi mumkin, bu esa oldini olish zarur.

Xulosa

Ushbu tadqiqotda kam quvvatli chekka hisoblash qurilmasi Jetson Nano da YOLO algoritmi asosida odamlar va velosipedlarni real vaqtda aniqlash, kuzatish va hisoblash imkonini beruvchi samarali yechim taklif etildi. Sistema arxitekturasida aniqlash (detection), kuzatish (tracking) va hisoblash (counting) bosqichlari aniq tarzda modullarga taqsimlangan, hamda ma’lumot oqimlari navbatlar (queues) orqali boshqarilgan.

Foydalanilgan adabiyotlar:

1. Fachrie, M. YOLOv3 modeli yordamida chuqur o‘rganish asosida oddiy transport vositalarini hisoblash tizimi. J. Resti (Rekayasa Sist. Dan Teknol. Inf.), 2020, 4, 462–468.

2. Redmon, J.; Farhadi, A. YOLOv3: inkremental yaxshilanish. arXiv, 2018.

3. Bharadhwaj, M.; Ramadurai, G.; Ravindran, B. Chekka qurilmada transport vositalarini aniqlash: bilim disertatsiyasi yordamida samaradorlikni oshirish. IEEE/CVF konferensiyasi, New Orleans, AQSh, 2022.

4. Allen-Zhu, Z.; Li, Y. Chuqur o‘rganishda ansambl, bilim disertatsiyasi va o‘z-o‘zini o‘rganishga oid ishlanmalar. arXiv, 2020.

5. Bewley, A. va boshqalar. Oddiy onlayn va real vaqtda kuzatish. IEEE ICIP konferensiyasi, Phoenix, AZ, AQSh, 2016.

6. OpenDataCam. Real vaqtda obyektlarni aniqlash uchun ochiq kodli dastur, 2021.

7. Bochkovskiy, A. va boshqalar. YOLOv4: obyekt aniqlash tezligi va aniqligi. arXiv, 2020.

8. Jiang, Z. va boshqalar. Yaxshilangan YOLOv4-tiny asosida real vaqt obyekt aniqlash usuli. arXiv, 2020.

9. Bochinski, V.E.; Sikora, T. Tasvir ma'lumotisiz yuqori tezlikli kuzatish. 2017.

10. Ultralytics. YOLOv5, 2022.

11. Bochinski, E. va boshqalar. IOU asosida ko'p obyektli kuzatishni vizual ma'lumotlar bilan kengaytirish. Auckland, Yangi Zelandiya, 2018.

12. Wojke, N. va boshqalar. Oddiy va real vaqtda kuzatish uchun chuqur assotsiatsiya metrikasi. Beijing, Xitoy, 2017.

13. Nvidia. Nvidia Jetson Nano. 2022.

RAQAMLI TA'LIMDA VR TEXNOLOGIYALARNING O'RNI

Mambetsharipov Y.R.

Jamoat xavfsizligi universiteti axborot texnologiyalari kafedrasi dotsenti, t.f.f.d (PhD)

Zamonaviy texnologiyalarning rivojlanishi bilan ta'lim sohasida sezilarli o'zgarishlar yuz bermoqda. Raqamli ta'lim an'anaviy o'qitish usullarini tubdan o'zgartirib, yangi imkoniyatlar va metodologiyalarni taklif etmoqda. Virtual reallik (VR) texnologiyalari esa raqamli ta'limning eng istiqbolli yo'nalishlaridan biriga aylanib, o'quv jarayoniga chuqurroq va interaktivroq tajribani olib kirish imkoniyatini yaratmoqda.

Virtual reallik - bu foydalanuvchini sun'iy ravishda yaratilgan raqamli muhitga cho'mdirish texnologiyasidir. VR texnologiyalari maxsus qurilmalar (shlem, ko'zoynak) orqali foydalanuvchiga haqiqatga o'xshash vizual, audio va ba'zan taktil sezgilar bilan ta'minlaydi.

VR texnologiyalarining ta'lim sohasida qo'llanilishi 1990-yillarning boshlariga borib taqalsa ham, asosiy taraqqiyot so'nggi o'n yil ichida amalga oshirildi. Bugungi kunda nisbatan arzon VR qurilmalarining paydo bo'lishi bu texnologiyani ta'lim muassasalari uchun ham qulay qildi.

Murakkab Tushunchalarni Vizuallashtirish - Murakkab ilmiy tushunchalar (masalan, molekulyar tuzilmalar, astronomik hodisalar) VR yordamida aniqroq va tushunarliroq tarzda taqdim etilishi mumkin. Bu abstrakt fikrlash qobiliyatini rivojlantirishga yordam beradi.

VR texnologiyalarini ta'lim jarayoniga integratsiya qilish yo'llari - **Maxsus VR ilovalar va dasturlar**: Google Expeditions, Engage, zSpace

kabi platformalar o‘quvchilarni turli sohalar bilan tanishtirishda xizmat qiladi.

Ta’lim platformalari bilan integratsiya: Moodle, Edmodo, Coursera kabi platformalarda VR kontentlardan foydalanish imkoniyati yaratilmoqda.

Laboratoriyalar va VR markazlar tashkil etish: Maktab va oliy o‘quv yurtlarida maxsus VR sinfxonalari tashkil etish orqali o‘quvchilarga yangi tajriba taqdim etish.

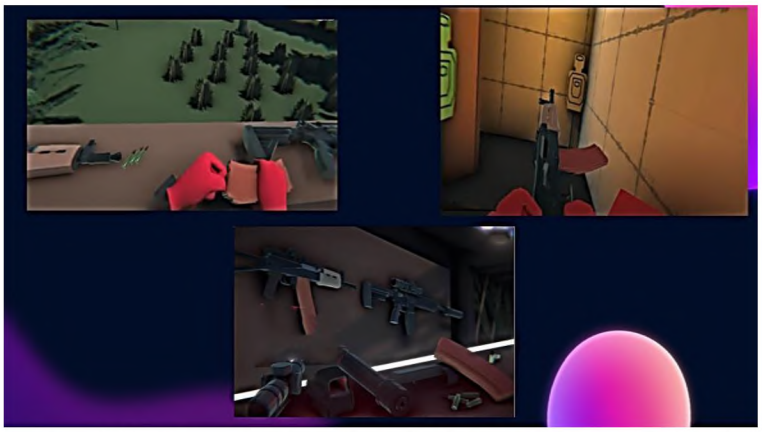
Murakkab amaliyotlarni xavfsiz o‘rganish VR o‘quvchilarni xavf ostiga qo‘ymasdan, murakkab, xavfli yoki qimmat turadigan amaliy mashg‘ulotlarni simulyatsiya qilishga imkon beradi. Masalan, kimyoviy portlashlar, yuqori kuchlanishli elektr qurilmalari bilan ishlash, yoki yurak operatsiyasi kabi tibbiy jarayonlar VR orqali xavfsiz o‘rganiladi.

Harbiy ta’lim va tayyorgarlikda yangi bosqich Zamonaviy urushlar va xavfsizlik tahdidlari harbiy xizmatchilarni nafaqat jismoniy, balki intellektual va texnologik jihatdan ham tayyorlashni talab qiladi. Bu borada virtual reallik texnologiyalari harbiy tayyorgarlikda katta o‘rin egallamoqda. VR vositalari orqali jangovar holatlarni simulyatsiya qilish, taktik va strategik qarorlarni mashq qilish, xavfli sharoitlarda to‘g‘ri harakat qilishni o‘rgatish mumkin.

Harbiy ta’lim muassasalarining o‘quv jarayoniga va harbiy xizmatchilarning jangovar tayyorgarligi tizimiga VR texnologiyalar asosidagi kompyuter trenajyorlarini joriy etish orqali olingan nazariy bilimlarni sifat jihatidan mustahkamlash, amaliy ko‘nikmalarni o‘z vaqtida shakllantirish mumkin bo‘ladi. VR texnologiyalar asosidagi kompyuter simulyatorlaridan foydalanish har bir kursantning o‘quv faoliyati, nazariy bilimlari hamda o‘zlashtirish darajasi va amaliy ko‘nikmalarni rivojlantirishdan kelib chiqqan holda shaxsiy baholanishiga imkon beradi.

VR qalqon simulatori mijoz va server arxitekturasi asosida ishlash imkoniyatiga ega. Mijoz tomonda unity dvijogida ishlaydi.

Harbiy va favqulodda holatlar xizmatida mutaxassislarni tayyorlash uchun virtual reallik (VR) asosidagi simulyatsiya texnologiyalari keng qo‘llanilmoqda. Ayniqsa, mina va portlovchi moddalarni aniqlash, zararsizlantirish bo‘yicha mashg‘ulotlar real hayotda yuqori xavfli bo‘lgani sababli, bu yo‘nalishda simulyatorlar muhim o‘rin tutadi. Ushbu maqolada sapyor (mina zararsizlantiruvchi) simulyatori misolida VR texnologiyalari yordamida xavfsiz, ammo realistik mashg‘ulotlar o‘tkazish imkoniyatlari tahlil qilinadi.



1-rasm. VR qalqon simulatorining umumiy ko‘rinishi.

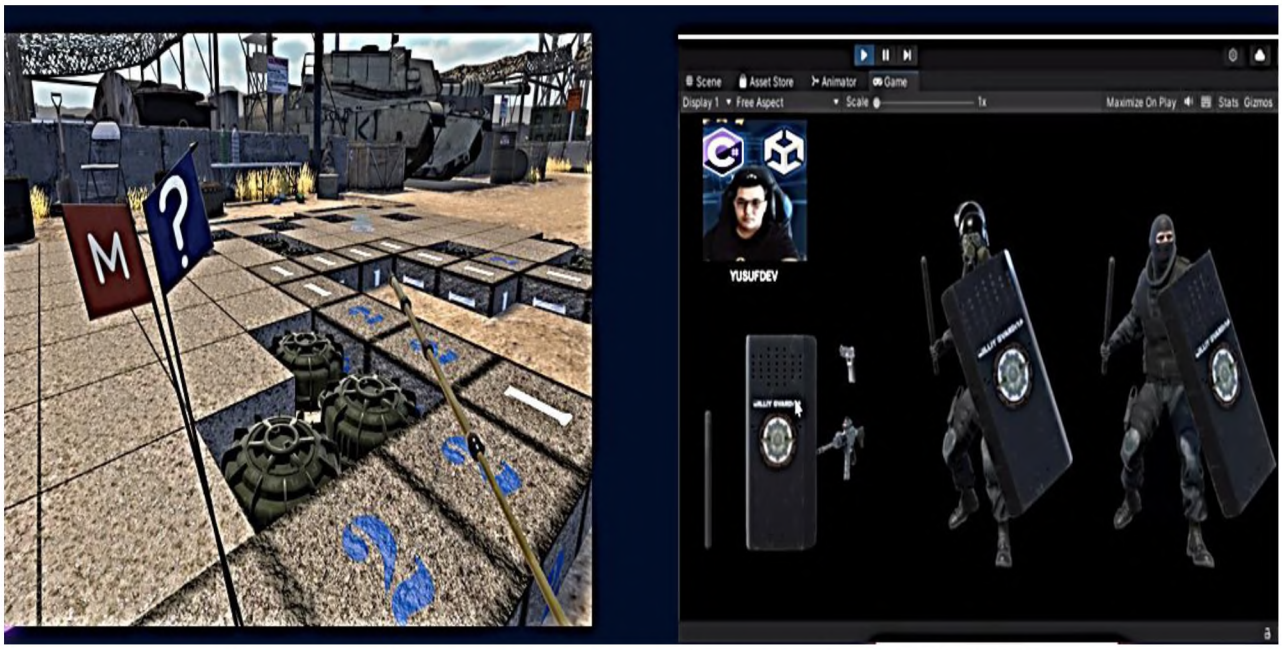
Sapyor simulyatori — bu portlovchi moddalarni aniqlash, xavfsiz tarzda zararsizlantirish bo‘yicha amaliy ko‘nikmalarni shakllantirishga xizmat qiluvchi o‘quv tizimidir. VR texnologiyasi asosida ishlab chiqilgan simulyatorlar quyidagi afzalliklarga ega:

- Real xavfdan holi o‘quv muhiti;
- Qayta-qayta mashq qilish imkoniyati;
- Turli murakkablikdagi ssenariylar yaratish;
- O‘quvchilarning xatti-harakatlarini monitoring qilish va baholash imkoniyati

VR tizimi quyidagi asosiy komponentlardan iborat:

- VR shlemlar (headsetlar): foydalanuvchini virtual muhitga olib kiradi;
- Harakatni aniqlovchi datchiklar: foydalanuvchining qo‘l, tana harakatlarini simulyatsiyaga uzatadi;
- Grafik dvigatellar (Unity/Unreal Engine): realistik muhit va obyektlar yaratadi;
- Interaktiv elementlar: foydalanuvchiga moslashuvchan va interaktiv mashg‘ulot imkonini beradi.

Sapyor simulyatorining VR texnologiyalari asosida ishlab chiqilishi nafaqat o‘quv jarayonini xavfsiz va samarali qiladi, balki real holatlarga yaqin tajriba orttirishga imkon beradi. Bunday texnologiyalar zamonaviy harbiy va xavfsizlik tayyorgarligi uchun muhim yechim sanaladi. Kelgusida bu tizimlarni sun’iy intellekt, haptik aloqa (teginish sezgisi) va kengaytirilgan reallik (AR) bilan integratsiya qilish istiqbollari mavjud. VR texnologiyalari raqamli ta’limda katta imkoniyatlar ochib bermoqda.



2-rasm. Sapyor simulyatori umumiy ko‘rinishi.

Ular nafaqat ta’lim jarayonini yanada qiziqarli va samarali qiladi, balki o‘quvchilarning amaliy ko‘nikmalarini rivojlantirish, chuqur bilimlarni o‘zlashtirishda muhim rol o‘ynaydi. Shu boisdan, VR texnologiyalarini ta’lim tizimiga integratsiya qilish bo‘yicha izchil strategiyalar ishlab chiqilishi, o‘qituvchilarni tayyorlash va infratuzilmani rivojlantirish zarur.

Foydalanilgan adabiyotlar

1. Freina, L., & Ott, M. (2015). A literature review on immersive virtual reality in education: state of the art and perspectives.
2. Merchant, Z., et al. (2014). Effectiveness of virtual reality-based instruction on students’ learning outcomes in K-12 and higher education.
3. Radianti, J., et al. (2020). A systematic review of immersive virtual reality applications for higher education.
4. Ivanov, A. (2023). *Virtual reality in military training*. Defense Technology Journal.
5. Hasanov, B. (2024). *Simulyatsiya tizimlari va ularning xavfsizlik sohasidagi qo‘llanilishi*. Toshkent: Innovatsion Texnologiyalar Nashriyoti.
6. Unity Documentation. (2025). *VR Development Guide*. [Online].
7. NATO Research Paper (2022). *Demining and EOD Simulation Technologies*.

TAKLIFLAR VA TAVSIYALAR

Qurolli Kuchlar tizimida raqamli texnologiyalarni joriy etish – zamonaviy harbiy salohiyatni oshirishning ajralmas qismi hisoblanadi. Bu zamonaviy harbiy operatsiyalarni tashkil etish va boshqarishda muhim ahamiyatga ega. Raqamli texnologiyalar yordamida Qurolli Kuchlarning samaradorligini oshirish, ma'lumotlarni tez va to'g'ri yig'ish, tahlil qilish, shuningdek, boshqaruv tizimini yaxshilash mumkin. Biroq, bu jarayonda bir qator muammolar mavjud bo'lib, ularni hal etish uchun aniq takliflar va tavsiyalar keltirilgan.

1. Sun'iy intellektning harbiy maqsadlarda qo'llanishi katta imkoniyatlar yaratadi, biroq u bilan bog'liq etik va huquqiy muammolarni hal qilish zarur. Davlatlar, xalqaro tashkilotlar va olimlar bu borada aniq qoidalarni ishlab chiqish va amaliyotga joriy qilish ustida ish olib borishlari kerak. O'zbekiston Respublikasida sun'iy intellektdan foydalanish sohasini transchegaraviy huquqiy va texnologik xavf-xatarlarni hisobga olgan holda tartibga solish bo'yicha quyidagi takliflarni shakllantirish mumkin:

- harbiy maqsadlarda qo'llaniladigan sun'iy intellektning qonuniy ta'rifini mustahkamlash. Unda avtonomlik darajasi, ehtimoliy zarar miqyosi, foydalanish maqsadlari, dasturiy ta'minotni buzib kirish xavfi va milliy manfaatlarga zarar yetkazish ehtimoli aniq belgilab berilish;
- avtonom sun'iy intellektdan harbiy sohada foydalanishning qabul qilinadigan chegaralarini va uni faollashtirish shartlarini ma'muriy tartibga solish;
- sun'iy intellektdan foydalanish bo'yicha universal qoidalar ishlab chiqilishi. Bu qoidalar harbiy avtonom tizimlardan foydalanishda yuzaga keladigan vaziyatlarni yagona standart asosida talqin qilishga imkon berish;
- amaldagi me'yorlarga qo'shimchalar kiritilish, ya'ni sun'iy intellekt qabul qilgan qarorlarning kiruvchi ma'lumotlar asosida qabul qilinishi qayta ishlanishi, talqin qilinishi va natija shakllantirilishi jarayonlarida ishlab chiquvchi, foydalanuvchi va tizim administratorining javobgarlik zonalarni aniqlashtirilish.

2. Bugungi kunda harbiy sohada himoyalangan aloqa tizimlarini joriy etish, maxsus harbiy ehtiyojlar uchun yopiq aloqa tarmoqlarni yaratish muhim masalasiga aylandi. Ushbu yo'nalishda muammolarni hal etish uchun quyidagi takliflar va tavsiyalar keltirilgan:

- kriptografik himoyani kuchaytirish maqsadida harbiy va davlat aloqa tizimlarida kuchli simmetrik va assimmetrik kriptografik algoritmlarni joriy etish. Har bir foydalanuvchi uchun individual kalitlar tizimini yo‘lga qo‘yish. Aloqa vositalari kriptografik bilan jihozlanishi lozim. Kalitlar almashinuvi xavfsiz kanallar orqali amalga oshirilishini ta’minlash;

- maxsus himoyalangan aloqa vositalarini ishlab chiqish bo‘yicha masalalarni yechish uchun himoyalangan mobil telefonlar, radiostansiyalar va terminal qurilmalarni ishlab chiqish yoki xorijiy analoglarni milliylashtirish. Harbiy dronlar, qurolli tizimlar va mobil boshqaruv punktlari uchun mustaqil va shifrlangan tarmoq kanallarini yaratish. Mahalliy ishlab chiqaruvchilar bilan hamkorlikda milliy serverlar va bulutli tizimlarni rivojlantirish. Zaxira tarmoq kanallari va avariyali rejimlarni yo‘lga qo‘yish. Qurilmalar signal uzatish vaqtida shifrlashni avtomatik amalga oshirishi zarur. Har bir qurilma uchun kiberxavfsizlikka oid sinovdan o‘tkazish va sertifikatlashtirish tizimi bo‘lishi lozim;

- tarmoq infratuzilmasini mustahkamlash maqsadida himoyalangan virtual tarmoqlar va maxsus izolyatsiyalangan infratuzilmalarda aloqa qurish. Qurolli Kuchlarga tegishli ma’lumotlar uzatiladigan barcha kanallarni davlat ichki tarmog‘i orqali yo‘naltirish. Xavfsiz marshrutlash va paketlar tahlilini amalga oshiruvchi tizimlar joriy etish. Tarmoq xavfsizligini buzgan har qanday holatni aniqlovchi tizimlarni o‘rnatish;

- kiberxavfsizlikni integratsiyalash maqsadida har bir aloqa tizimiga doimiy monitoring, kiberhujumlarga qarshi javob berish modullarini qo‘shish. Xavfsizlik devorlari (firewall), antivirus tizimlari va trafikni nazorat qiluvchi mexanizmlarni integratsiya qilish. Harbiy aloqa tarmoqlari uchun kiberxavfsizlik bo‘yicha doimiy tahdid modeli ishlab chiqilishi kerak. Har yili xavfsizlik bo‘yicha audit va sinovlar o‘tkazish majburiy bo‘lishi zarur.

3. Dunyoda raqamli tizimlar orqali dushman tomonidan josuslik, ma’lumotlar o‘g‘irlanishi yoki tizimga zarar yetkazish holatlari kuzatilmoqda. Axborot xavfsizligi, kiberxavfsizlik va raqamli suverenitetni ta’minlash uchun quyidagi chora-tadbirlar taklif qilinmoqda:

- raqamli tizimlarning ko‘p darajali himoya arxitekturasini joriy etish maqsadida har bir tizim uchun chuqurlashtirilgan himoya tamoyiliga asoslangan ko‘p qatlamli xavfsizlik choralarini joriy etish. Tarmoq darajasida xavfsizlik devorlari (firewall), kirishni nazorat qilish tizimlari (NAC), kirishni autentifikatsiya qilish (MFA) tizimlarini o‘rnatish. Har bir foydalanuvchiga minimal kerakli huquqlarni berish. Harbiy tizimlar

uchun maxsus ishlab chiqilgan izolyatsiyalangan infratuzilmalardan foydalanish;

- kiberhujumlarni aniqlash va ularga javob berish tizimini kuchaytirish maqsadida IDS/IPS (Intrusion Detection and Prevention Systems) tizimlarini joriy etish orqali har qanday noan'anaviy faoliyatni aniqlash. SIEM (Security Information and Event Management) tizimlari yordamida real vaqt rejimida xavfsizlik holatini nazorat qilish. Kiberhujum holatida tezkor javob berish bo'yicha harbiy "CERT" (Computer Emergency Response Team) tuzilmasini shakllantirish. Foydalanuvchilar faoliyati va tizim loglarini doimiy monitoring va tahlil qilish;

- yopiq va mustaqil dasturiy ta'minotdan foydalanish maqsadida milliy operatsion tizim, messendjerlar va ofis dasturlarini ishlab chiqish yoki mavjud ochiq kodli tizimlarni milliylashtirish. Xorijiy ishlab chiquvchilardan mustaqil axborot infratuzilmasini shakllantirish, shuningdek, harbiy sohada milliy antivirus va xavfsizlik dasturlarini ishlab chiqish, kiberhujum va tahdidlardan himoya qilish uchun ilg'or xavfsizlik protokollarini joriy etish. Barcha strategik tizimlar faqat milliy yoki to'liq nazoratdagi dasturiy vositalarda ishlashi kerak. Tashqi axborot almashuvlari faqat nazorat ostidagi, xavfsiz protokollar orqali amalga oshirilishi zarur.

4. Ko'pgina raqamli uskunalar va dasturiy ta'minotlar xorijiy ishlab chiqaruvchilarga bog'liq. Ushbu muammolarni hal etish uchun quyidagi takliflar va tavsiyalar keltirilgan:

- import o'rnini bosuvchi milliy raqamli texnologiyalarni yaratish;

- mahalliy IT-startaplarni harbiy buyurtmalar orqali qo'llab-quvvatlash;

- xavfsizlik nuqtai nazaridan ochiq kodli dasturlarga o'tishni rag'batlantirish.

5. Harbiy operatsiyalarni bajarish uchun avtonom dronlar va robot tizimlarni joriy etish bugungi kunda o'z muhimligini ko'rsatmoqda. Ushbu texnologiyalar zamonaviy harbiy strategiyada muhim o'rin egallab, inson ishtirokini minimallashtirish, aniqlikni oshirish va xavfsizlikni ta'minlash imkonini beradi. Ushbu yo'nalishda masalalarni yechish uchun quyidagi takliflar va tavsiyalar keltirilgan:

- harbiy dronlar va robot tizimlarning turlarini aniqlab, vazifalar bo'yicha ixtisoslashtirish maqsadida harbiy doktrinaga asoslangan holda dron va robotlar turlari bo'yicha spetsifikatsiyalar ishlab chiqish. Har bir vazifa turi uchun optimal yechimlarni tanlash: tezlik, manevrlik, aniqlik,

radius va avtonomiya mezonlari asosida. Uchuvchisiz uchish apparatlari va robotizatsiya tizimlarini qo‘llash orqali xavfsizlikni oshirish;

- avtonom boshqaruv va sun’iy intellektni integratsiyalash maqsadida dron va robotlarga mashinali o‘rganish, obyektni aniqlash, harakatni bashorat qilish kabi funksiyalarni yuklash. Nishonlarni avtonom tanish va zarba berish imkonini beruvchi algoritmlarni ishlab chiqish. Harbiy sun’iy intellekt modellarini doimiy o‘qitish va real tajribalarda sinovdan o‘tkazish. Avtonom tizimlarga inson nazorati ostida “oxirgi qaror qabul qilish” mexanizmini kiritish;

- aloqa va boshqaruv tizimini kuchaytirish maqsadida dronlar va robotlarni boshqarish uchun xavfsiz, shifrlangan, aralashuvga chidamli aloqa kanallarini yaratish. Harbiy boshqaruv markazlaridan real vaqt rejimida buyruqlar uzatish va javob olish imkonini beruvchi interfeyslar ishlab chiqish. Radioaloqa uzilgan holatda avtonom rejimda ishlash strategiyalarini ishlab chiqish. Optik yoki kvant aloqa texnologiyalarini izlanishga olish;

- milliy ishlab chiqarishni yo‘lga qo‘yish maqsadida dron va robotlar uchun mahalliy komponentlar (sensorlar, dvigatellar, mikroprotsessorlar) ishlab chiqarishni rivojlantirish. Harbiy-texnik korxonalar, ilmiy-tadqiqot institutlari va universitetlar hamkorligida ishlab chiqish markazlari yaratish. Importdan mustaqillikni ta’minlash uchun ochiq kodli platformalarni milliylashtirish. Davlat xaridlari orqali mahalliy ishlab chiqaruvchilarga rag‘bat berish;

- kadrlar tayyorlash va qo‘llash protokollarini ishlab chiqish maqsadida operatorlar, texnik xizmat ko‘rsatuvchilar va sun’iy intellekt mutaxassislari uchun alohida o‘quv kurslarini tashkil etish. Dronlardan foydalanish bo‘yicha qo‘llanmalar va standart operatsion protseduralar ishlab chiqish. Harbiy amaliyotlarda avtonom tizimlar ishtirokini sinovdan o‘tkazish uchun maxsus poligonlar tashkil etish. Dronlar va robotlar ishtirokidagi mashg‘ulotlar sonini oshirish;

- etik va huquqiy me’yorlarni shakllantirish maqsadida avtonom zarba beruvchi tizimlarga xalqaro harbiy etikani hisobga olgan holda ishlov berish. Harbiy avtonom tizimlardan foydalanish bo‘yicha milliy huquqiy tartiblarni ishlab chiqish. Inson ishtirokisiz o‘limga olib keluvchi qarorlarni qabul qilishni cheklovchi hujjatlar tayyorlash. Xalqaro tajribani o‘rganib, milliy etik kodeks ishlab chiqish.

6. **Optik tolali sensor tizimlari zamonaviy xavfsizlik infratuzilmasining muhim qismidir va ularni to‘g‘ri joriy etish orqali**

yuqori darajadagi kuzatuv va ogohlantirishni ta'minlash mumkin. Ushbu tizimlarni joriy etish uchun quyidagi takliflar va tavsiyalar keltirilgan:

- muhim obyektlari xavfsizligini oshirish maqsadida optik tolali sensorlarni geografik, iqlimiy va sharoitiga mos ravishda joylashtirish bo'yicha texnik hujjatlar ishlab chiqish. Tizimlar elektr uzilishlarida ham ishlashi uchun avtonom quvvat manbai bilan ta'minlanishi;

- analitik va ogohlantirish tizimlarini integratsiyalash maqsadida optik sensorlardan kelayotgan ma'lumotlarni real vaqt rejimida tahlil qiluvchi sun'iy intellekt asosidagi dasturlarni joriy etish. Ogohlantirish tizimini markaziy boshqaruv paneli, mobil qurilmalar va radioaloqa tizimlariga bog'lash. Ogohlantirish darajasiga qarab avtomatik javob choralari (masalan, dron yuborish, yorug'lik signalini yoqish) tizimlarini ishlab chiqish. Noto'g'ri ogohlantirishlarni kamaytirish uchun filtratsiya algoritmlarini joriy etish;

- optik tolali tizimlarini sinovdan o'tkazish va sertifikatlashtirish maqsadida tizimni ekspluatatsiyaga topshirishdan avval turli sharoitlarda (ob-havo, vibratsiya, harorat) testdan o'tkazish. Milliy xavfsizlik standartlariga moslik sertifikatini olish tizimini joriy qilish. Har yili rejalashtirilgan profilaktik test va kalibrovka ishlarini o'tkazish. Yangi texnologiyalar paydo bo'lishi bilan tizimlarni doimiy yangilab boriladi;

- kadrlar va texnik xizmat ko'rsatish masalalarini hal etish uchun optik sensor tizimlar bilan ishlay oladigan mutaxassislarni tayyorlashda maxsus o'quv kurslarini yo'lga qo'yish. Harbiy va fuqaro obyektlarida texnik xizmat ko'rsatish brigadalarini shakllantirish. Tizimlarni o'rnatish va ishlatish bo'yicha qo'llanma va video materiallar tayyorlash;

- integratsiyalashgan xavfsizlik tizimining bir qismi sifatida qo'llash uchun optik tolali sensor tizimlarini videokuzatuv, harbiy xavfsizlik tizimlari bilan integratsiyalash. Tizimni GIS (geografik axborot tizimi) bilan bog'lab, xavfsizlik xaritalarini real vaqt rejimida yuritish. Katta obyektlar yoki strategik infratuzilmalar uchun ko'p darajali xavfsizlik zonalari (perimetr ichki zona) yaratish. Har bir integratsiyalangan element uchun yagona boshqaruv interfeysini ishlab chiqish.

7. **Raqamli texnologiyalar bo'yicha harbiy innovatsiya markazlarini tashkil etish va yangi ishlanmalarni sinovdan o'tkazish – bu mudofaa salohiyatini oshirish, texnologik suverenitetni ta'minlash va ilg'or texnologiyalarni joriy qilish uchun muhim ahamiyatga ega.** Harbiy innovatsiya markazlarini tashkil etish va yangi

ishlanmalarni sinovdan o‘tkazish uchun imkoniyat yaratish maqsadida uchun quyidagi takliflar va tavsiyalar keltirilgan:

- harbiy innovatsiya markazlarini tashkil etish uchun sun’iy intellekt, kiberxavfsizlik, robototexnika, dron texnologiyalari, kvant texnologiyalari bo‘yicha alohida yo‘nalishlarda ixtisoslashgan markazlarni yaratish. Innovatsion markazlarni harbiy institutlari, harbiy texnika korxonalari va universitetlar bazasida tashkil etish. Harbiy-texnik inkubatorlar va startap zonalarini markazlar tarkibida ochish. Innovatsion yechimlarni tezkor joriy etish uchun soddalashtirilgan reglamentlar ishlab chiqish. Harbiy va ilmiy muassasalar o‘rtasida to‘g‘ridan-to‘g‘ri hamkorlik mexanizmini joriy etish. Raqamli texnologiyalar rivojlanishi va innovatsiyalarni qo‘llab-quvvatlash maqsadida davlat va xususiy o‘rtasida hamkorlikni kuchaytirish. Mudofaa vazirligi va yetakchi oliy ta’lim muassasalari o‘rtasida doimiy ilmiy-texnik loyihalarni yuritish. Magistratura va doktorantura bosqichlarida harbiy yo‘nalishdagi texnologik ishlanmalarni ilmiy izlanish obyekti sifatida tanlash. Mahalliy ishlab chiqaruvchilar, IT-kompaniyalar va harbiylar o‘rtasida uzviy hamkorlik tizimini yaratish. Harbiy ehtiyojlar uchun ishlanayotgan texnologiyalarni tezkor prototiplash va sinovdan o‘tkazish mexanizmini yo‘lga qo‘yish;

- yangi ishlanmalarni sinovdan o‘tkazish tizimini joriy etish uchun har bir yangi raqamli texnologiyani sinovdan o‘tkazish uchun maxsus poligonlar va laboratoriyalar tashkil etish (virtual va real muhitlarda). Harbiy operatsion ssenariylarga asoslangan modellashtirilgan sinov tizimlarini ishlab chiqish;

- harbiy texnologik standartlar ishlab chiqish maqsadida raqamli qurilmalar va dasturiy vositalar uchun milliy harbiy standartlar (MHS) ishlab chiqish va tatbiq etish. Har qanday yangi mahsulot harbiy foydalanishga qabul qilinishidan avval ushbu standartlarga muvofiqligi tekshirilishi zarur;

- innovatsion loyihalarni moliyaviy qo‘llab-quvvatlash maqsadida harbiy innovatsion ishlanmalarni moliyalashtirish uchun mudofaa innovatsiya fondi tashkil etish. Yil yakunida eng samarali innovatsion ishlanmalarga davlat grantlari, mukofotlar ajratish tizimini yo‘lga qo‘yish;

- kadrlar salohiyatini oshirish uchun innovatsiya markazlari tarkibida malaka oshirish va doimiy ta’lim bo‘limlari tashkil etish. Harbiy o‘quv yurtlarida harbiy IT-mutaxassis, muhandis-programmachi va texnolog-robototexniklar yo‘nalishlarini ochish.

8. **Qurolli Kuchlarda raqamli texnologiyalarni joriy etishda kadrlar tayyorlash muammolari dolzarb masala hisoblanadi. Shu bilan birga, raqamli tizimlar bilan ishlash uchun maxsus tayyorgarlikka ega bo‘lgan harbiy mutaxassislar soni yetarli emas.** Ushbu muammolarni hal etish uchun quyidagi takliflar va tavsiyalar keltirilgan:

- harbiy o‘quv yurtlarida raqamli texnologiyalarni joriy etishga oid o‘quv dasturlarini ishlab chiqish va har doim yangilashtirish. O‘quv dasturlariga axborot xavfsizligi, sun’iy intellekt va kiberxavfsizlik bo‘yicha maxsus kurslarni kiritish va kengaytirish;

- zamonaviy xizmat va qurollar bilan ishlash bo‘yicha amaliy treninglar, simulyatorlar, kurslar orqali muntazam qayta tayyorlash tizimini joriy etish. Zamonaviy laboratoriyalar va simulyatsiya markazlarini yaratish;

- raqamli texnologiyalar bo‘yicha o‘qituvchi va mutaxassislarni tayyorlash uchun xorijiy harbiy o‘quv yurtlari bilan hamkorlik o‘rnatish. Ilg‘or xorijiy tajribalarni o‘rganib, sharoitlarga moslab o‘qitish metodikasini ishlab chiqish;

- amaliy mashg‘ulotlar va tajriba almashinuvini kengaytirish maqsadida kadrlarni zamonaviy harbiy texnologiyalarni real sharoitlarda qo‘llashga yo‘naltirilgan amaliyot dasturlariga jalb qilish. Kiberxavfsizlik, raqamli aloqa tizimlari va dron texnologiyalari bo‘yicha amaliy treninglar tashkil etish. Mudofaa sanoatidagi tashkilotlar bilan integratsiyalashgan o‘quv-amaliy markazlar tashkil etish. Xususiy IT-kompaniyalar bilan hamkorlik dasturlarini yaratish;

- kadrlar salohiyatini baholash va rag‘batlantirish tizimini joriy etish maqsadida raqamli texnologiyalarni o‘zlashtirgan harbiy xizmatchilar uchun sertifikatlash tizimini joriy qilish. Innovatsion g‘oya va ishlanmalari bo‘lgan mutaxassislarni moddiy va ma’naviy rag‘batlantirish. Harbiy sohadagi raqamlashtirish tashabbuslari uchun alohida grantlar va mukofotlar tizimini yo‘lga qo‘yish. Harbiy rahbarlar uchun raqamli yetakchilik va boshqaruv bo‘yicha malaka oshirish kurslarini tashkil etish.

MUNDARIJA

KIRISH SO‘ZI.....3
Karimov Sh.S. Muhim axborot infratuzilmasida kibertahdidlarni intellektual tahlil qilishning konseptual modeli.....5
Karimov N.M., Akbaraliyev B.B. Jangovar ziddiyatli vaziyatlarda noaniq mantiq asosida qaror qabul qilish algoritmi.....12
Jaksimov D.B. Krizis holatlarida resurslar boshqaruvi va zaxira kuchlarni optimallashtirishda sun’iy intellektdan foydalanish.....18
Nurjanov F.R. Yuz tasvirini identifikatsiyalash tizimlarini avtomatlashtirishda sun’iy intellektning roli va ahamiyati.....30
Parpiyeva A.J. Harbiy faoliyatda robot tizimlarining rivojlanish tendensiyalari.....36
Пен А.Ю. Материально-техническое обеспечение службы связи силовых ведомств.....50
Nigmatov Z.Z. Qurolli Kuchlar tizimida sun’iy intellekt texnologiyalarni qo‘llashning zamonaviy yechimlari.....52
Yusupov U.A., Tashmanov Y.B. Harbiy obyektlar perimetrini muhofaza qilishda tolali-optik datchiklar tahlili.....57
Raximov B.N., Muxtdinov X.A,Yusupov B.K. Sun’iy intellekt tizimlarida ma’lumotlar va bilimlar bazasini tashkil etish usullari tahlili.....62
To‘rayev B.Z., Rayimov M.Sh. Toifalangan obyektlarga qaratilgan kiberhujum turlari va ulardan himoyani tashkil etish usullari.....69
Базаров А.Б. Применение искусственного интеллекта в современных коммуникационных технологиях специального назначения.....75
Qurbonov M.R. Qurolli Kuchlar tuzilmalarida kiberxavfsizlik mutaxassislarini tayyorlash uchun kiberpoligon yechimi.....79
Abdulxayev N.M., Musayev A.I. Telekommunikatsiya sohasida mutaxassislik fanini masofaviy o‘qitishning metodlari va usullari.....85
Абдуллаева С.М., Дехконов О.Р. Внедрение искусственного интеллекта и автоматизированных систем управления в Вооруженные Силы Узбекистана.....88
Xurramov A.I Raqamli texnologiyalarni qo‘llash orqali harbiy ekzoskelet yaratish.....94
Umarov M.A., Bozorboyeva Z.Q., Xudoyberdiyev Sh.B., Giyasova G.A., Samarov Sh.X. Tasvirlardan yo‘l belgilarini tanib oluvchi dasturiy vositaning interfeysi.....98
Jalolov A.A., Achilov F.B. Ommaviy tartibsizliklar jarayonida toifalangan obyektlarni himoyalashning zamonaviy texnik yechimlari.....105
Telmonov J.J., Xatamov B.B. Avtomatlashtirilgan aloqa tizimlari va ularning kiberhujumlarga barqarorligi.....113

Tashmanov Y.B Portlovchi qurilmalarni zararsizlantirishda masofadan boshqariladigan yer usti transport vositalaridan videooqimlarni uzatish tahlili.....118
Abdiraximov A.A. Raqamli texnologiyalar asosida professor-o‘qituvchilarning samaradorligini smart reyting tizimi orqali baholash.....121
Fayzullayev A.X., Sindarov Sh.O‘. Optik tolali aloqa kabellari orqali boshqariladigan dronlarning mudofaa va xavfsizlik sohasida qo‘llanishi: imkoniyatlar va cheklovlar.....126
Anvarov F.I., Yusupov U.A., Tashmanov Y.B. Harbiy obyektlarni muhofaza qilishda fazali tolali-optik datchiklar tahlili.....132
Tashmanov Y.B. Ommaviy tartibsizliklarda odam sanash modellari tuzilishining tahlili.....135
Пен А.Ю. Ресурсная методология в управлении безопасностью систем связи силовой структуры.....139
Saidbayev B.Dj. Mudofaa sohasidagi harbiy sun’iy intellektning afzalliklari va muammolari.....144
Shaymardonov J.Z. “Jxu Tracker” Axborot texnologiyalari asosida jamoat xavfsizligini ta’minlash vositasi.....151
Bozorov A.A. Videokuzatuv tizimlarida tasvir sifatini baholash tadqiqoti.....155
Kamalov M.E. Xitoy, Hindiston, Rossiya va Nato tajribasi asosida harbiy sohada raqamli texnologiyalarni qo‘llash muammolari.....162
Xamidov G‘.S. Yo‘l harakati xavfsizligi xizmati faoliyatida uchuvchisiz uchish apparatlaridan foydalanish imkoniyatlari.....170
Baxtiyorova S.U., Xatamov B.B. IoT-texnologiyalarni qurolli kuchlarda qo‘llash: imkoniyatlar va tahdidlar.....174
Asqarov U.J., Mamatqulov M.Y., Uzaqov V.R. Tor hududda joylashgan radioelektron vositalarning elektromagnit moslashuvchanligini baholash algoritmi.....182
Tuxliyev Sh.Yu., Misirov Sh.Ch. Axborot-o‘quv trenajorlarini ishlab chiqishdagi asosiy qonuniyatlar va prinsiplar tahlili.....189
Ochilov I.N. O‘zbekiston Respublikasi Milliy Gvardiyasi bo‘linmalari obyektlarini qo‘riqlashda axborot xavfsizligi tushunchasi va uning asosiy tamoyillari.....200
Xamidov G‘.S. Hodisa joyini ko‘zdan kechirishda ilg‘or texnologiyalardan foydalanishning innovatsion yondashuvi.....208
Шайманов А.Т. О роли цифровых технологий в подготовке специалистов инженерно-саперных подразделений.....214
Kamilov M.A. Kiberxavfsizlik: Qurolli Kuchlarda Axborot himoyasini ta’minlash muammolari va chora-tadbirlari.....218
Хатамов Б.Б. Сетецентрические войны: роль цифровых технологий в управлении боевыми действиями.....226

Убайдуллаева А.А. Анализ процесса формирования профессиональной коммуникативной компетенции на основе информационно-коммуникационных технологий (икт).....233
Saidbayev B.Dj. Raqamli xavfsizlik va shaxsiy ma'lumotlar himoya qilish.....239
Mambetsharipov Y.R. Harbiy obyektlar videokameralaridan ma'lumotlarni uzatish protokollarining tahlili.....246
Ochilov I.N. Milliy Gvardiyasi bo'linmalarida axborot xavfsizligi hamda obyektlar xavfsizligini ta'minlashda axborot texnologiyalari va texnik qo'riqlash vositalarining o'rni.....250
Jalolov A.A. Ommaviy tartibsizliklarning oldini olishda profilaktik chora-tadbirlarning ahamiyati.....256
Ziyayev B.N. Uchuvchisiz uchish apparatlarida videoaxborot uzatish texnologiyalarining rivojlanish tendensiyalari.....265
Uzakov E.O., Yusupov U.A. Qurolli Kuchlar tizimida raqamli texnologiyalar.....266
Qilichov B., Jalolov A.A. O'zbekiston Respublikasining Qurolli Kuchlarida yangi texnologiyalar va yangliklar kiritish.....277
Xudoyberdiyev M.R., Yusupov U.A. Qurolli Kuchlarda raqamli texnologiyalarni joriy etish va rivojlantirish muammolari.....281
Sadirova M.Q., Saidbayev B.Dj. Qurolli Kuchlar tizimida axborot texnologiyalari.....284
Majidova S.N. Qurolli Kuchlar tizimida axborot texnologiyalarini o'rni va vazifasi.....292
Jabborova M. Raqamli asrda kriptografiya va xabarlar xavfsizlikni ta'minlash.....295
Boymirzayeva X.F., Kamilov M.A. Qurolli Kuchlar tizimida raqamli texnologiyalarni qo'llashning nazariy-amaliy jihatlari.....303
Ziyayev B.N. Favqulodda holatlarda uchuvchisiz uchish apparatlari yordamida videoaxborotlarni tezkor uzatish va tahlil qilish.....306
Mambetsharipov Y.R. Yolo algoritmi asosida jetson nano qurilmasida real vaqt rejimida odam va velosipedlarni aniqlash va son jihatdan monitoring qilish usullarini ishlab chiqish.....308
Mambetsharipov Y.R. Raqamli ta'limda vr texnologiyalarning o'rni.....314
Takliflar va Tavsiyalar.....318

QUROLLI KUCHLAR TIZIMIDA RAQAMLI TEXNOLOGIYALARNI QO‘LLASH MUAMMOLARI VA YECHIMLARI

II Respublika ilmiy-amaliy konferensiya
MATERIALLARI TO‘PLAMI

2025 yil 26 sentabr

Muharrir: Tashmanov Ye.B.
Texnik muharrir: Rahmonov A.A
Korrektor: Odilova F.K.

Bosishga ruxsat berildi 05.11.2025. Buyurtma № 616 Format 60x90/16
Times New Roman garniturasi bilan raqamli bosma usulida bosildi.
Hajmi: 20,5 sh.b.t. 14,83 t.-h.t. Adadi: 2 nusxa.

O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti bosmaxonasi