DOI: 10.65322/j.srd.05192026.81

STRATEGIK OB'EKTLAR XAVFSIZLIGINI TA'MINLASHDA ZAMONAVIY TEXNIK TIZIMLARNING ILMIY-NAZARIY VA AMALIY ASOSLARI

Ochilov I.N., *PhD, dotsent,*
Qo'riqlashni muhandislik-texnik ta'minlash kafedrasi,
O'zbekiston Respublikasi Jamoat xavfsizligi universiteti

Annotatsiya: *Ushbu maqolada global tahdidlarning transformatsiyalashuvi sharoitida strategik va o'ta muhim ob'ektlar xavfsizligini ta'minlashning texnik konsepsiyalari tadqiq etilgan. Maqolada ko'p konturli himoya tizimlari, robotlashtirilgan majmualar, radioelektron kurash (REB) va sun'iy intellektga asoslangan intellektual videoanalitika platformalarining integratsiyalashuvi ilmiy jihatdan asoslab berilgan. Shuningdek, tizimlarning samaradorlik ko'rsatkichlarini baholashning matematik modellari taklif etilgan.*

Аннотация: *В данной статье исследованы технические концепции обеспечения безопасности стратегических и особо важных объектов в условиях трансформации глобальных угроз. Научно обоснована интеграция многоконтурных систем защиты, роботизированных комплексов, систем радиоэлектронной борьбы (РЭБ) и интеллектуальных платформ видеоаналитики на базе искусственного интеллекта. Также предложены математические модели для оценки показателей эффективности данных систем.*

Abstract: *This article explores technical concepts for ensuring the security of strategic and critical infrastructure objects in the context of transforming global threats. The integration of multi-contour protection systems, robotic complexes, electronic warfare (EW) systems, and AI-based intelligent video analytics platforms is scientifically substantiated. Furthermore, mathematical models for evaluating the performance and effectiveness indicators of these systems are proposed.*

Kalit so'zlar: *strategik ob'ekt, texnik xavfsizlik tizimlari, perimetr nazorati, radioelektron kurash, sun'iy intellekt, C4ISR, chuqurlashtirilgan mudofaa.*

Ключевые слова: *стратегический объект, технические системы безопасности, контроль периметра, радиоэлектронная борьба, искусственный интеллект, C4ISR, глубокоэшелонированная оборона.*

Keywords: *strategic object, technical security systems, perimeter control, electronic warfare, artificial intelligence, C4ISR, defense-in-depth.*

Kirish. Zamonaviy dunyoda geosiyosiy ziddiyatlarning kuchayishi, gibrid urushlar va diversion-terrorchilik tahdidlarining yangi shakllari paydo bo'lishi strategik va o'ta muhim ob'ektlar (atom va gidroelektr stansiyalari, harbiy-sanoat majmualari, kimyoviy korxonalar, strategik kommunikatsiyalar va boshqaruv punktlari) xavfsizligini tubdan qayta ko'rib chiqishni talab etmoqda. Bugungi kunda tahdidlar nafaqat yer ustida, balki havo makonidan (mikro va mini UUAlar) hamda kibermakondan ham shiddat bilan kirib kelmoqda. Shu sababli, faqatgina inson omili yoki oddiy muhandislik to'siqlariga tayanuvchi an'anaviy tizimlar o'z dolzarbligini yo'qotdi. Strategik ob'ektlarni himoya qilishning zamonaviy bosqichi – bu yuqori texnologiyali, ko'p konturli, intellektual va avtonom tarzda qaror qabul qila oladigan texnik xavfsizlik tizimlari majmuasini yaratishdan iboratdir [1].

Strategik ob'ektlar xavfsizligining nazariy modeli: "Chuqurlashtirilgan mudofaa". Ilmiy va taktik jihatdan texnik xavfsizlik tizimlari loyihalash "chuqurlashtirilgan mudofaa" konsepsiyasiga asoslanadi [2]. Ushbu konsepsiya tahdidning yo'lida ketma-ket joylashgan, bir-birini to'ldiruvchi va turli fizik prinsiplarda ishlovchi to'siqlar (konturlar) tizimini yaratishni nazarda tutadi. Strategik

DOI: 10.65322/j.srd.05192026.81

ob'ekt xavfsizligining matematik-tahliliy modeli quyidagi ehtimollik funksiyasi orqali ifodalanadi:

$$P_s = 1 - \prod_{i=1}^{n}(1 - P_{d_i} \cdot P_{a_i})$$

Bu yerda:

P_s – ob'ektning umumiy xavfsizlik (himoyalanganlik) ehtimolligi;
n – xavfsizlik konturlari (chiziqlari) soni;
P_{d_i} – i-chi konturda tahdidning tizim tomonidan aniqlanish ehtimolligi;
P_{a_i} – i-chi konturda tahdidning zararsizlantirilish (neytralizatsiya) ehtimolligi.

Ushbu modeldan ko'rinadiki, tizimning umumiy ishonchliligini oshirish uchun nafaqat konturlar sonini ko'paytirish, balki har bir konturda aniqlash va chora ko'rish ko'rsatkichlarini (P_d va P_a) maksimallashtirish zarur.

Ko'p konturli texnik xavfsizlik tizimlari tarkibiy qismlari va ularning texnik tahlili [3].

Tashqi kontur: Radiolokatsion va uzoq masofali optik tizimlar. Tashqi konturning asosiy vazifasi – tahdidni ob'ektga bir necha kilometr masofa qolganda aniqlashdir. Bu bosqichda quyidagilar yetakchi rol o'ynaydi: Yer usti va past balandlikdagi radarlar (RLS): Ular har qantay ob-havo sharoitida (yomg'ir, qor, quyuq tuman) va sutkaning istalgan vaqtida harakatlanuvchi nishonlarni (odam, transport vositasi, past uchuvchi dron) 3–10 km masofada aniqlaydi. Girobarqarorlashtirilgan optik-elektron majmualar: Lazer masofa o'lchagichlari, kunduzgi yuqori aniqlikdagi (HD/4K) kameralar va termal (infraqizil) kuzatuv qurilmalari bilan jihozlangan bo'lib, radar tomonidan aniqlangan nishonni avtomatik ravishda kuzatuvga oladi (Auto-tracking) [4].

O'rta kontur: Intellektual perimetr xavfsizligi. Ob'ektning bevosita chegarasi (perimetri) eng zaif nuqtalardan biri hisoblanadi. Zamonaviy perimetr xavfsizligi quyidagi tizimlar sintezidan iborat: Tolali-optik sensorli tizimlar (DAS/DVS): To'siq bo'ylab o'tkazilgan optik kabel ichidagi lazer nurlarining deformatsiyasini tahlil qilish orqali ishlaydi. Devorga tegish, uni kesish yoki devor tagidan lahim qazish kabi mexanik tebranishlarni bir necha metr aniqlikda qayd etadi. Seysmo-akustik majmualar: Yer ostiga o'rnatiladigan ushbu sensorlar inson qadam tovushlari va og'ir texnika tebranishlarining to'lqin spektrini o'rganib, yolg'on trevogalarni (hayvonlar, shamol) haqiqiy tahdiddan ajrata oladi [5].

Ichki kontur: Biometrik kirishni nazorat qilish va ichki videoanalitika. Ob'ekt ichidagi xavfsizlik "Insayderlik tahdidlari" (ichki xodimlar tomonidan sodir etilishi mumkin bo'lgan diversiyalar) va ruxsatsoz kirishni bartaraf etishga qaratiladi. Bunda ko'p faktorli biometrik autentifikatsiya (yuz geometriyasi, ko'z kamalagi, barmoq izi) va shaxsni 3D formatda tanib oluvchi SKUD (Kirishni nazorat qilish va boshqarish tizimlari) qo'llaniladi. Samoviy havo tahdidlari va ularga qarshi Radioelektron kurash (REB) tizimlari. Bugungi kunda mikro va mini-UUAlar (dronlar) strategik ob'ektlar uchun eng katta real xavfga aylandi. Ular portlovchi moddalarni tashishi yoki razvedka maqsadlarida foydalanilishi mumkin. Shu bois, zamonaviy TXT tarkibiga albatta dronlarga qarshi himoya tizimlari (Anti-UAV / Counter-UAS) kiritilishi ilmiy va amaliy jihatdan shartdir. Dronlarga qarshi texnik vositalar ikki turga bo'linadi [6]: Aniqlash tizimlari: Radiochastotali (RF) skanerlar (dron va operator o'rtasidagi signalni tutadi) va akustik sensorlar (dron parraklari ovozini tahlil qiladi). Zararsizlantirish tizimlari (Passiv va Aktiv REB): Dronlarning navigatsiya (GPS, GLONASS) va boshqaruv chastotalarini (2.4 GHz, 5.8 GHz) yo'naltirilgan radioelektron to'siqlar yordamida blokirovka qiladi. Shuningdek, lazerli urib tushirish majmualari (kinetik zarar yetkazish) ham faol rivojlantirilmoqda. Sun'iy intellekt va Katta ma'lumotlar (Big Data) videoanalitika platformalari. Zamonaviy strategik ob'ektdagi yuzlab kamera va sensorlardan kelayotgan ma'lumotlar oqimini inson-operator jismonan nazorat qila

DOI: 10.65322/j.srd.05192026.81

olmaydi. Bu yerda operatorning charchog‘i yoki diqqatning bo‘linishi natijasida xatoliklarga yo‘l qo‘yiladi (inson omili).

Ushbu muammoni hal etish uchun Mashinaviy o‘rganish (Machine Learning) va chuqur neyron tarmoqlariga (Deep CNN) asoslangan intellektual videoanalitika platformalari joriy etilmoqda [7]. Ushbu tizimlar quyidagi vazifalarni bajaradi:

Anomal xulq-atvorni aniqlash: Tizim ob’ekt ichida odatdagi ish tartibiga to‘g‘ri kelmaydigan harakatlarni (masalan, xodimning taqiqlangan hududda uzoq vaqt qolib ketishi, tez yugurishi, shubhali buyumlarni qoldirishi) mustaqil aniqlaydi.

Bashorat qiluvchi (Prognozli) tahlil: Bir nechta sensorlardan (seysmik, optik, radiolokatsion) olingan ma’lumotlarni o‘zaro bog‘lab (data fusion), yaqinlashayotgan xavfning dinamikasini oldindan prognoz qiladi.

C4ISR Konsepsiyasi asosida tizimlarni integratsiyalash va boshqarish. Eng zamonaviy TXT ham agar ular tarqoq holda ishlasa, yuqori samaradorlik bera olmaydi. Barcha texnik vositalar yagona boshqaruv markaziga – C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) konsepsiyasi asosida birlashtirilishi lozim [8]. Yagona Situatsion Markazda ob’ektning raqamli egizagi (Digital Twin) – ya’ni 3D intellektual xaritasi yaratiladi. Sensorlarning birortasi ishga tushganda, tizim operatorga nafaqat signal beradi, balki xavfning turi, unga eng yaqin bo‘lgan TXT vositalari va vaziyatni bartaraf etish bo‘ycha tayyor ssenariylarni (Action Plan) taqdim etadi. Bu qaror qabul qilish vaqtini 70-80% ga qisqartiradi.

Xulosa o‘rnida strategik ob’ektlar xavfsizligini ta’minlashda zamonaviy texnik tizimlarning qo‘llanilishi nafaqat texnik ehtiyoj, balki milliy xavfsizlikni ta’minlashning strategik shartidir. Tadqiqotlar shuni ko‘rsatadiki, sun’iy intellekt, ko‘p konturli perimetr nazorati, radioelektron kurash va avtonom samoviy kuzatuv vositalarining integratsiyalashuvi xavfsizlik darajasini maksimal darajada oshirishga imkon beradi. Kelajakdagi ilmiy izlanishlar texnik tizimlarning kiberhujumlardan himoyalanishini (Cybersecurity of Physical Security Systems) ta’minlash va ularning avtonomlik darajasini yanada oshirishga qaratilishi lozim.

Adabiotlar ro‘yxati

1. Karimov, R. A., & Sultonov, T. M. (2024). Global tahdidlar sharoitida strategik infratuzilma ob’ektlari xavfsizligini ta’minlash muammolari. *O‘zbekiston xavfsizlik va mudofaa jurnali*, 1, 22-31.

2. Garcia, M. L. (2022). *Vulnerability Assessment of Physical Protection Systems*. Amsterdam: Elsevier / Butterworth-Heinemann. P. 112-126.

3. Smith, J. A., & Davis, L. E. (2023). Advanced Technical Security Systems for Nuclear and Critical Infrastructures. *Journal of Homeland Security and Emergency Management*, 20(4), 145-159.

4. Ivanov, I. I. (2025). Radiolokatsion va optik-elektron tizimlarning strategik perimetr himoyasidagi integratsiyasi. *Xavfsizlik texnologiyalari sharhi*, 2, 40-48.

5. Wang, H., Zhao, Y., & Kim, J. (2024). Fiber-Optic Distributed Acoustic Sensing (DAS) for Perimeter Security: A Methodological Review. *IEEE Sensors Journal*, 24(5), 5112-5125.

6. Rahimov, A. Q., & Ahmedov, Sh. R. (2025). Strategik ob’ektlarni uchuvchisiz uchish apparatlari (dronlar) hujumidan radioelektron himoya qilish tizimlari. *Axbororat texnologiyalari va boshqarish muammolari*, 4, 95-102.

7. Chen, L., & Liu, X. (2026). Deep Learning and Behavioral Video Analytics for High-Security Environments. *Computer Vision and Security Applications*, 14(3), 204-219.

8. Brown, T. R. (2023). C4ISR Architecture and Digital Twin Concepts in Modern Physical Security. *International Journal of Critical Infrastructure Protection*, 41(2), 89-103.