SECURITY SYSTEMS FOR CLASSIFIED FACILITIES: EXPERIENCE OF DEVELOPED COUNTRIES AND RECOMMENDATIONS FOR UZBEKISTAN

Yakubov Jur'at Amangeldiyevich
Ministry of Defense of the public of Uzbekistan

Annotation. *This article examines the significance of protecting critical infrastructure facilities within the framework of national security and analyzes the experience of developed countries in classifying and safeguarding such facilities. The study provides an in-depth review of the United States Critical Infrastructure Protection (CIP) framework, the European Union's Critical Entities Resilience (CER) Directive, as well as the practical approaches implemented in Japan, South Korea, China, and the Russian Federation. Particular attention is given to infrastructure categorization criteria, integration of cyber-physical security systems, public–private collaboration, risk-based management, SCADA/IoT-based monitoring technologies, and continuity planning during emergencies. Based on a comparative assessment, the article proposes a conceptual model for strengthening critical infrastructure protection in the Republic of Uzbekistan, taking into account necessary legal frameworks, technological development, risk profiling, and international cooperation. The results of the study hold scientific and practical value for shaping a comprehensive national policy aimed at ensuring the resilience and security of strategically important infrastructure.*

Key words: *critical infrastructure; facility categorization; CIP; CER; national security; cyber-physical security; SCADA; IoT; risk-based management; resilience; strategic facilities; international experience; Uzbekistan.*

СИСТЕМЫ ОХРАНЫ КАТЕГОРИРОВАННЫХ ОБЪЕКТОВ: ОПЫТ РАЗВИТЫХ СТРАН И РЕКОМЕНДАЦИИ ДЛЯ УЗБЕКИСТАНА

Якубов Журъат Амангелдиевич
Министерства обороны Республики Узбекистан

Аннотация. *В данной статье анализируется значение охраны объектов критической инфраструктуры в системе национальной безопасности, а также рассматривается опыт развитых стран по классификации и защите таких объектов. В исследовании детально изучаются модели США (Critical Infrastructure Protection – CIP), директива Европейского Союза Critical Entities Resilience (CER), а также практические механизмы Японии, Республики Корея, Китая и Российской Федерации. Особое внимание уделяется критериям категорирования объектов, интеграции кибер-физической безопасности, взаимодействию государства и частного сектора, риск-ориентированному управлению, технологиям мониторинга*

на основе SCADA/IoT и обеспечению устойчивости инфраструктуры в чрезвычайных ситуациях. На основе сравнительного анализа предлагается концептуальная модель защиты критической инфраструктуры для условий Республики Узбекистан, включающая развитие нормативно-правовой базы, современных технологических решений, профильных рисков и международного сотрудничества. Результаты исследования имеют научно-практическое значение для формирования системной политики по обеспечению устойчивости и безопасности стратегически важных объектов.

Ключевые слова: *критическая инфраструктура; категорирование объектов; CIP; CER; национальная безопасность; кибер-физическая безопасность; SCADA; IoT; риск-ориентированное управление; устойчивость; стратегические объекты; международный опыт; Узбекистан.*

TOIFALANGAN OBYEKTLARNI QO‘RIQLASH TIZIMLARI: RIVOJLANGAN DAVLATLAR TAJRIBASI VA O‘ZBEKISTON UCHUN TAVSIYALAR

Yakubov Jur’at Amangeldiyevich
O‘zbekiston Respublikasi Mudofaa vazirligi

Annotatsiya. *Ushbu maqolada toifalangan obyektlar va kritikal infratuzilma tizimlarining milliy xavfsizlikdagi ahamiyati, ularni himoya qilish bo‘yicha rivojlangan davlatlar tajribasi hamda O‘zbekiston uchun mos keluvchi yondashuvlar tahlil qilingan. Tadqiqotda AQShning Critical Infrastructure Protection (CIP) modeli, Yevropa Ittifoqining Critical Entities Resilience (CER) direktivasi, Yaponiya, Janubiy Koreya, Xitoy va Rossiya Federatsiyasining kritikal infratuzilma himoyasi bo‘yicha amaliy mexanizmlari qiyosiy o‘rganiladi. Shuningdek, obyektlarni toifalash mezonlari, kiber-fizik xavfsizlik integratsiyasi, davlat–xususiy sektor hamkorligi, risk-asoslangan boshqaruv, SCADA/IoT tizimlari asosidagi monitoring, favqulodda vaziyatlarda uzluksizlikni ta’minlash bo‘yicha zamonaviy texnologiyalar tahlil qilinadi. O‘zbekiston sharoitida kritikal infratuzilmani himoya qilishning kontseptual modeli taklif etilib, normativ-huquqiy baza, texnologik rivojlanish, xavf profillari va xalqaro hamkorlikdan kelib chiqadigan ustuvor yo‘nalishlar belgilangan. Tadqiqot natijalari milliy xavfsizlikni ta’minlash, strategik obyektlarni himoya qilish va barqaror infratuzilma boshqaruvini shakllantirish uchun ilmiy-amaliy ahamiyat kasb etadi.*

Kalit so‘zlar: *toifalangan obyektlar; kritikal infratuzilma; CIP; CER; Milliy xavfsizlik; kiber-fizik xavfsizlik; SCADA; IoT; risk-asoslangan boshqaruv; uzluksizlik; strategik obyektlar; xalqaro tajriba; O‘zbekiston.*

Zamonaviy dunyoda davlat va jamiyat normal faoliyatining uzluksizligini ta’minlovchi infratuzilmalar energetika tarmoqlari, transport yo‘llari,

kommunikatsiya, bank va moliya tizimlari, yadro, suv-gaz tarmoqlari va boshqa strategik obyektlar — tobora ortib borayotgan global tahdidlar (kiber-xavfsizlik muammolari, terrorchilik, sabotaj, tabiiy ofatlar, transmilliy bog‘liqlik) sababli har qachongidan ham muhim ahamiyat kasb etmoqda. Bunday obyektlar — “toifalangan obyektlar” yoki “kritikal infratuzilma” deb ataladi. Ularning himoyasi milliy xavfsizlik strategiyasining ajralmas qismi bo‘lib, davlatning ijtimoiy-iqtisodiy barqarorligi, xavfsizlik va xavfsizlik strategiyasining dolzarbligini ta’minlaydi.

Ushbu maqola maqsadi rivojlangan davlatlar (AQSh, Yevropa Ittifoqi, Yaponiya, Janubiy Koreya, Xitoy, Rossiya) tajribasini tahlil qilish, ularning toifalangan obyektlarni himoya qilish tizimlaridagi yondashuvlari, afzalliklari va kamchiliklarini solishtirish hamda O‘zbekiston sharoitida moslashtirilishi mumkin bo‘lgan konseptual tavsiyalarni aniqlashdan iborat.

“Obyekt” tushunchasi keng: lekin “toifalangan obyektlar” (critical infrastructure / strategic facilities) — davlat va jamiyatning uzluksiz va normal faoliyatini ta’minlaydigan, yuqori ijtimoiy-iqtisodiy, ekologik yoki strategik salmog‘ga ega infratuzilma obyektlari. Bunday obyektlarga energetika stansiyalari, transport va logistika tarmoqlari, yadro va kimyo sanoati, kommunikatsiya tarmoqlari, bank-moliya tizimi markazlari, davlat boshqaruvi markazlari, suv va gaz ta’minoti infratuzilmalari, sog‘liqni saqlash tizimi, axborot-kommunikatsiya markazlari va boshqalar kiradi.

Kritikal infratuzilmaning turlari va “toifalanish mezonlari” ko‘plab omillarga asoslanadi — obektning milliy-iqtisodiy ahamiyati, texnologik jarayonlarning murakkabligi, uzluksizlik talablari, ekologik xavf, ijtimoiy barqarorlikka ta’siri, strategik / harbiy ahamiyati, hamda xavf (risk) darajasi.

Ilmiy adabiyotlarda “critical infrastructure protection (CIP)”, “strategic asset protection”, “critical entities resilience”, “kiber-fizik infratuzilma himoyasi (cyber-physical security)” kabi tushunchalar keng qo‘llaniladi. Bunday yondashuv infratuzilma xavfsizligini nafaqat fizik, balki kiber va integratsiyalashgan usullar bilan ta’minlashga urg‘u beradi.

Rivojlangan davlatlar tajribasi: modellar va yondashuvlar. *AQSh — Department of Homeland Security (DHS) va Critical Infrastructure Protection (CIP) modeli.*

AQShda kritikal infratuzilmalarni himoya qilish konsepsiyasi nisbatan 1990-yillardan boshlab shakllana boshlagan. 1998–2001 yillardagi Prezident qarorlari (masalan, “Presidential Decision Directive 63”) bilan birinchi keng qamrovli CIP tizimi yo‘lga qo‘yilgan. Keyinchalik, 2001-yil 11-sentabr voqealaridan so‘ng — terrorchilik va sabotaj tahdidlari ortishi bilan, bu tizim keskin rivojlandi va kengaytirildi.

Hozirgi kunda DHS, xususan, uning tarkibidagi Cybersecurity and Infrastructure Security Agency (CISA) kritikal obyektlarni identifikatsiyalash, ularni himoya qilish, kiber hamda fizik xavfsizlikni ta'minlash, davlat va xususiy sektor o'rtasida hamkorlikni yo'lga qo'yish kabi vazifalarni bajaradi. CIP modeli federal va shtat darajasida ko'p bosqichli boshqaruvga asoslanadi; xususiy sektor esa infratuzilmaning katta qismini tashkil etganligi sababli himoyada markaziy rol o'ynaydi.

Texnologik jihatdan — CIP doirasida SCADA tizimlarining himoyasi, kiber-xavfsizlik (firewall, intrusion detection systems, segmentatsiyalangan tarmoqlar), IoT sensorlari, AI va katta ma'lumotlar (Big Data) tahlili, dronlar va robot patrullari, "Zero Trust Architecture" kabi zamonaviy yondashuvlar qo'llanilmoqda. Tahdidlar tahlili va risk boshqaruvi uchun xalqaro va milliy standartlardan foydalaniladi.

Bu modelning afzalliklari — kuchli texnologik baza, davlat-xususiy sektor hamkorligi, resurslar va byudjetning yetarliligi, murakkab tahlil va monitoring imkoniyati. Kamchiligi esa — federal–shtat bo'yicha koordinatsiya murakkabligi, byurokratik qiyinchiliklar, xususiy sektor manfaatlari bilan davlat xavfsizlik talablarining ba'zan mos kelmasligi, va kiber tahdidlarning doimiy o'sib borishi.

Yevropa Ittifoqi — Critical Entities Resilience Directive (CER) 2022/2557. Yevropa davlatlari kritikal infratuzilma himoyasida yagona standart va normativ bazani yaratishga intiladi. Shunday yo'l bilan 2022 yilda qabul qilingan CER direktivasi 2023-yildan boshlab YI (Yevropa Ittifoqi) davlatlari uchun majburiy hisoblanadi. Bu direktiva kritikal infratuzilma obyektlarini aniqlash, ularni tasniflash, risk baholash va himoya choralarini belgilash, kiber va fizik xavfsizlikni integratsiyalashgan yondashuvda ta'minlash, favqulodda vaziyatlarga tayyorlik va davlatlararo hamkorlik mexanizmlarini o'z ichiga oladi.

YI modelining o'ziga xos jihati — transchegaraviy integratsiya va bog'liqlik. Energetika, transport, raqamli infratuzilma, data markazlar, logistika koridorlari va boshqa obyektlar bir-biri bilan kuchli bog'liq; shuning uchun bitta mamlakatda bo'ladigan uzilish yoki hujum butun mintaqaga ta'sir qilishi mumkin. CER direktivasi bu holatlarni oldindan baholash, birgalikda javob choralarini rejalashtirish va standartlashtirilgan xavfsizlik mexanizmlarini joriy etishni nazarda tutadi. Bu modelning afzalligi — yagona normativ baza, integratsiyalashgan boshqaruv, transchegaraviy xavflarni boshqarish, ma'lumot almashinuvi, hamda keng ko'lamli hamkorlik. Kamchiligi esa — har bir davlatning milliy qiziqishlari, huquqiy va byudjet imkoniyatlari farq qilishi, hamda integratsiyalashuv bilan bog'liq murakkabliklar.

Osiyo tajribalari: Japan va South Korea. **Yaponiya** — tabiiy ofatlar, zilzila, tsunami, bo'ron, yong'in kabi yuqori xavfga ega hududda joylashgan. Shuning

uchun Yaponiya kritikal obyektlar himoyasida fizik xavfsizlik, kiber-fizik integratsiya va uzluksizlikka katta e'tibor beradi. Yadro, energetika, transport, telekommunikatsiya infratuzilmalari SCADA, IoT sensorlari, AI va robototexnika, real vaqt monitoring, kuchli perimetr himoyasi, favqulodda holatlarga tayyorlik kabi usullar bilan ta'minlangan. Fukushima yadro inqirozidan so'ng Yaponiya xavfsizlik standartlarini tubdan ko'rib chiqqan, yangi mustahkam himoya va monitoring tizimlarini joriy qilgan.

Janubiy Koreya esa — yuqori raqamlashtirilgan, 5G va IoT infrastrukturasi keng tarqalgan, kiber-xavfsizlik darajasi yuqori mamlakatdir. Bu mamlakatda "Smart Security" konsepsiyasi asosida kiber va fizik xavfsizlik integratsiyalashgan: AI kameralari, yuzni tanish tizimlari, dronlar, aqlli kirish nazorati, real vaqt monitoring, Zero Trust yondashuvi, IoT sensorlar va SCADA tizimlari keng qo'llanadi. Bu jihatlar Koreyani kritikal obyektlarni himoya qilishda dunyodagi ilg'or davlatlar qatoriga qo'yadi.

Boshqa misollar: China va Russian Federation. Xitoy global raqamlashtirish va sanoat innovatsiyalar strategiyasi ("Made in China 2035" kabi) doirasida kritikal infratuzilma himoyasini ham davlat siyosatini muhim yo'nalishlaridan biriga aylantirgan. Ular markazlashgan boshqaruv, davlat-va xususiy sektor hamkorligi, AI, IoT, SCADA va kiber-fizik integratsiyani keng joriy etmoqda, favqulodda vaziyatlarga tayyorlik va uzluksizlikni ta'minlash strategiyasini ilgari surmoqda.

Rossiya Federatsiyasi esa — geosiyosiy pozitsiyasi, hududning geografik kengligi, strategik infratuzilma majmualari mavjudligi sababli kritikal infratuzilmalarni himoya qilishda sistematik va markazlashgan yondashuvga tayanadi: kiber va fizik xavfsizlik integratsiyasi, favqulodda vaziyatlar bo'yicha koordinatsiya, davlat nazorati, SCADA va IoT tizimlari, tezkor reaktsiya imkoniyati mavjud.

Solishtirma tahlil va umumiy tendensiyalar. Turli davlat modellari tahlil qilinsa — bir nechta umumiy tendensiyalar aniq ko'zga tashlanadi:

Barcha rivojlangan davlatlar toifalangan obyektlarni xavf darajasi, ijtimoiy-iqtisodiy va strategik salmog'i asosida tasniflaydi.

Texnologik murakkab, uzluksiz xizmat ko'rsatishga mo'ljallangan infratuzilmalar (energetika, transport, kommunikatsiya, axborot, yadro, suv-gaz kabi) har doim yuqori prioritetga ega.

Kiber xavfsizlik — bugungi kunda eng katta tahdidlardan biri; zamonaviy tizimlar SCADA, IoT, AI, Big Data, dron va robot patrullar, real vaqt monitoring, Zero Trust yondashuvini joriy qilmoqda.

Transchegaraviy bog'liqlik (xususan Yevropa, Xitoy, global energetika va transport tarmoqlari) modelida — bir mamlakatdagi falokat butun mintaqa uchun

xavf tug‘diradi. Shuning uchun xalqaro hamkorlik, normativlar va koordinatsiyalashgan boshqaruv zarur.

Davlat–xususiy sektor hamkorligi — ko‘plab infratuzilmalar xususiy sektorga tegishli bo‘lganligi sababli, himoyada ularga ham katta rol beriladi.

Tavsiyalar va O‘zbekiston sharoitida moslashtirish konsepsiyasi. Rivojlangan davlatlar tajribasi va tahlilga asoslanib, quyidagi tavsiyalar O‘zbekiston sharoitida toifalangan obyektlar xavfsizligini kuchaytirish uchun muhimdir:

Kritikal obyektlarni tasniflash: ijtimoiy-iqtisodiy ahamiyati, uzluksizlik darajasi, texnologik murakkabligi, ekologik va strategik ta’sir kabi mezonlar asosida;

Risk-asoslangan yondashuv: har bir obyekt bo‘yicha tahdid profili (fizik, kiber, tabiiy), ehtimollik va oqibatlarni baholash, va mos himoya choralarini ishlab chiqish;

Markazlashtirilgan monitoring va boshqaruv tizimi: SCADA / IoT integratsiyasini joriy etish, real vaqt monitoring, kiber-fizik integratsiya, dron / robot patrul, AI asosida tahdid aniqlash va prognozlash;

Davlat–xususiy sektor hamkorligi: xususiy sektor infratuzilmasiga egalik qiladigan obyektlarning himoyasida davlat va xususiy sektor o‘rtasida standartlar, majburiyatlar va hamkorlik tartibini yo‘lga qo‘yish;

Normativ-huquqiy bazani yaratish va standartlashtirish: xalqaro tajriba asosida normativlar va standartlar ishlab chiqish, himoya siyosatini qonuniy asosda tartibga solish;

Favqulodda holatlarga tayyorlik va kadrlar tayyorlash: treninglar, simulyatsiyalar, favqulodda vaziyat rejalarini ishlab chiqish va testlash;

Davlatlararo hamkorlik va xalqaro tajriba almashuv: transchegaraviy infratuzilmalar bo‘yicha hamkorlik, ma’lumot almashish, xavfsizlik standartlarini uyg‘unlashtirish.

Xulosa va kelajak istiqbollari. Bugungi global geosiyosiy va texnologik muhitda faqat fizik himoya — eskirgan yondashuv; kiber-fizik integratsiya, real vaqt monitoring, risk-asoslangan yondashuv va davlat–xususiy sektor hamkorligi asosida qurilgan tizimlar — zamon talabiga mos. Rivojlangan davlatlar tajribasidagi (AQSh CIP, YeI CER, Yaponiya, Janubiy Koreya, Xitoy, Rossiya va boshqalar) yondashuvlar O‘zbekiston uchun foydali bo‘lishi mumkin. Ammo, ularni joriy etishda iqtisodiy, texnologik, normativ va ijtimoiy sharoitlar hisobga olinishi lozim. Agar O‘zbekistonda Kritikal Infratuzilma himoyasini mustahkamlash bo‘yicha tizimli harakatlar olib borilsa — bu nafaqat individual obyektlar xavfsizligini oshiradi, balki butun mamlakat barqarorligi, milliy xavfsizlik va iqtisodiy salohiyat uchun muhim omil bo‘lib xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. European Parliament and the Council. (2022). *Directive (EU) 2022/2557 on the resilience of critical entities (CER Directive).* Brussels: EU Publications.

2. U.S. Department of Homeland Security. (2021). *National Infrastructure Protection Plan (NIPP): Partnering for Critical Infrastructure Security and Resilience.* Washington, DC.

3. National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity.* Gaithersburg, MD.

4. International Organization for Standardization. (2018). *ISO/IEC 27001: Information Security Management Systems Requirements.*

5. Boin, A., & McConnell, A. (2019). *Managing transboundary crises: The emergence of European crisis governance.* Journal of European Public Policy, 26(2), 157–175.

6. Lewis, J. A. (2020). *Critical Infrastructure Protection in the United States.* Center for Strategic and International Studies (CSIS).

7. Correa, J., & Yusta, J. (2021). *Critical infrastructure risk assessment: A review of current approaches.* Reliability Engineering & System Safety, 210, 107–117.

8.Chang, S. E., & Shinozuka, M. (2018). *Measuring improvements in the disaster resilience of communities.* Earthquake Spectra, 34(4), 1937–1954.

9. Park, J., & Seung, H. (2020). *Cyber–physical security challenges in South Korea’s critical infrastructure.* Journal of Cybersecurity, 6(1), 1–16.

10. Ministry of Economy, Trade and Industry of Japan. (2020). *Guidelines on Ensuring the Security of Critical Infrastructure.* Tokyo.

11. Korea Internet & Security Agency (KISA). (2021). *National Cybersecurity Strategy of the Republic of Korea.* Seoul.

12. МВД РФ. (2017). *О безопасности критически важных объектов и объектов повышенной опасности.* Москва.

13.ФСБ РФ. (2020). *Методические рекомендации по защите объектов критической информационной инфраструктуры.* Москва.

14.Haimes, Y. Y. (2018). *Risk Modeling of Interconnected Critical Infrastructure Systems.* New York: Springer.

15Dunn, M., & Wigert, I. (2019). *International CI protection policies and best practices.* NATO Cooperative Cyber Defence Centre.