MUHIM INFRATUZILMANI KIBER TAHDIDLARDAN HIMOYA QILISH

Toshkent davlat yuridik universiteti
ommaviy huquq fakulteti 2-bosqich talabasi
Xamidjonov Baxromjon

Annotatsiya: Ushbu maqolada O‘zbekiston Respublikasining muhim infratuzilma obyektlarini zamonaviy kibertahdidlardan himoya qilish masalalari ilmiy-tahliliy jihatdan o‘rganilgan. Tadqiqotda IT/OT konvergensiyasi sharoitida yuzaga kelayotgan xavflar, xalqaro standartlar: NIST CSF 2.0, ISO/IEC 27001 va O‘zbekistonning “Kiberxavfsizlik to‘g‘risida”gi qonuni (O‘RQ-764) talablari qiyosiy tahlil qilingan. Maqolada sun’iy intellekt asosidagi proaktiv himoya tizimlari, ta’minot zanjiri xavfsizligi va kadrlarni tayyorlash masalalari alohida ko‘rib chiqilgan. Tadqiqot natijalari asosida muhim infratuzilma xavfsizligini ta’minlashga doir talablar ko‘rib chiqilgan.

Kalit so‘zlar: muhim infratuzilma, kiberxavfsizlik, IT/OT konvergensiyasi, sun’iy intellekt, Zero Trust, NIST CSF 2.0, ta’minot zanjiri xavfsizligi, O‘RQ-764, SCADA, kiber chidamlilik.

Аннотация: В данной статье проведён научно-аналитический анализ вопросов защиты объектов критической информационной инфраструктуры Республики Узбекистан от современных киберугроз. В ходе исследования рассмотрены риски, возникающие в условиях конвергенции IT/OT-систем, проведён сравнительный анализ международных стандартов (NIST CSF 2.0, ISO/IEC 27001) и требований Закона Республики Узбекистан «О кибербезопасности» (ЗРУ-764). Особое внимание уделено системам проактивной защиты на основе искусственного интеллекта, безопасности цепочки поставок и подготовке кадров. По результатам исследования разработаны практические рекомендации по обеспечению безопасности критической инфраструктуры.

Ключевые слова: критическая инфраструктура, кибербезопасность, конвергенция IT/OT, искусственный интеллект, Zero Trust, NIST CSF 2.0, безопасность цепочки поставок, ЗРУ-764, SCADA, киберустойчивость.

Abstract: This article presents a scientific and analytical examination of cybersecurity challenges facing critical infrastructure facilities in the Republic of Uzbekistan against modern cyber threats. The study analyzes risks arising from IT/OT convergence, conducts a comparative review of international standards (NIST CSF 2.0, ISO/IEC 27001), and evaluates the requirements of Uzbekistan's Law on Cybersecurity (URQ-764). Special focus is given to AI-driven proactive defense systems, supply chain security, and personnel training. Based on the research findings, practical

recommendations have been developed to strengthen the protection of critical infrastructure objects.

Keywords: critical infrastructure, cybersecurity, IT/OT convergence, artificial intelligence, Zero Trust, NIST CSF 2.0, supply chain security, URQ-764, SCADA, cyber resilience.

I. KIRISH

Har bir davlatning ijtimoiy-iqtisodiy rivojlanishining asosi sifatida muhim infratuzilma (MI) obyektlarining uzluksiz, xavfsiz va ishonchli ishlashini olishimiz mumkin. Muhim infratuzilma obyektlari o‘z ichiga energetika va elektr ta’minoti tizimlari, suvni tozalash va taqsimlash inshootlari, sog‘liqni saqlash muassasalari, transport va logistika tarmoqlari, moliya hamda bank sektorlari, shuningdek, davlat boshqaruvi va axborot-kommunikatsiya texnologiyalari (AKT) kabi tizimlarni qamrab oladi.[1] Tarixan, ushbu tizimlarni bevosita nazorat qiluvchi va boshqaruvchi operatsion texnologiyalar hamda sanoat boshqaruv tizimlari tashqi internet tarmoqlaridan butunlay uzib qo‘yilgan holda faoliyat yuritilgan. Bu izolyatsiya ularni tashqi kiberhujumlardan tabiiy ravishda himoya qilar edi. Biroq, Raqamli transformatsiya jarayonlari, internet ashyolari va To‘rtinchi sanoat inqilobi sharoitida an’anaviy axborot texnologiyalari (AT) va operatsion texnologiyalarning o‘zaro birlashuvi jarayoni vujudga kela boshladi. Ushbu IT/OT konvergensiyasi operatsion xarajatlarni kamaytirib, masofadan turib real vaqt rejimida monitoring qilish va boshqarish imkoniyatlarini kengaytirgan bo‘lsa-da, o‘z navbatida kiber jinoyatchilar uchun butunlay yangi, keng qamrovli va o‘ta xavfli hujum maydonini yaratib berdi.

Kiber makondagi tahdidlar yildan-yilga o‘sib borib, davlatlar milliy xavfsizligiga raxna solmoqda. Xalqaro ekspertlarning tahlillariga ko‘ra, kiberhujumlarning oqibatlari endilikda faqat ma’lumotlarni o‘g‘irlash yoki tizimlarni vaqtincha ishdan chiqarish bilan cheklanib qolmayapti; ular jismoniy dunyoda real talafotlar, ekologik halokatlar va inson qurbonliklariga olib kelinishiga sababchi bo‘lsihmoqda. Masalan, IBM korporatsiyasining 2024-yilda e’lon qilingan “Cost of a data breach” xalqaro hisobotiga ko‘ra, ma’lumotlar sizib chiqishi oqibatida kompaniyalar ko‘radigan o‘rtacha global zarar miqdori tarixiy rekord darajaga ko‘tarilib, 4,88 million AQSh dollarini tashkil etdi.[2]

[1] Aljumaiah, O., Jiang, W., Reddy Addula, S., & Amin Almaiah, M. (2025). Analyzing Cybersecurity Risks and Threats in IT Infrastructure based on NIST Framework. Journal of Cyber Security and Risk Auditing, 2025(2), 12–26. https://doi.org/10.63180/jcsra.thestap.2025.2.2

[2] IBM. (2024). Cost of a data breach 2024: Financial industry insights. IBM Think Insights. https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry

O‘zbekiston Respublikasida ham “Raqamli O‘zbekiston – 2030” strategiyasi va raqamli iqtisodiyotga o‘tish siyosati doirasida muhim infratuzilmani himoya qilish eng dolzarb, kechiktirib bo‘lmaydigan ustuvor vazifalardan biriga aylandi. Davlatimiz rahbariyati tomonidan mamlakat milliy axborot makonini himoya qilish, axborot xavfsizligini ta’minlashga qaratilgan bir qator strategik hujjatlar va huquqiy normalar qabul qilindi. Jumladan, O‘zbekiston Respublikasi Prezidentining 2022-yil 15-apreldagi tegishli qarori asosida O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi qonuni (O‘RQ-764) qabul qilinib, davlat kiberxavfsizlik siyosatining mustahkam huquqiy asoslari yaratildi. Qonunning VI bobi bevosita muhim axborot infratuzilmasi obyektlari kiberxavfsizligiga bag‘ishlangan bo‘lib, unda strategik obyektlarni toifalash, xavflarni baholash va yagona davlat reyestrini yuritish tartiblari belgilab qo‘yilgan.

Mazkur ilmiy maqolaning asosiy maqsadi - davlat, iqtisodiyot va aholi hayoti uchun o‘ta muhim bo‘lgan infratuzilma obyektlarini xususan, energiya tarmoqlari, moliya institutlari, sanoat boshqaruv tizimlari va kiber-fizik tizimlarni zamonaviy va kelajakdagi noma’lum kiber tahdidlardan himoya qilish mexanizmlarini tahlil qilishdir.

Muhim infratuzilma obyektlarini himoya qilish muammosi so‘nggi yillarda axborot texnologiyalari, muhandislik, harbiy xavfsizlik va huquqshunoslik sohalaridagi butun dunyo olimlari hamda nufuzli tadqiqot markazlari tomonidan qizg‘in va har tomonlama o‘rganilmoqda. Ushbu tadqiqotda I.H. Sarkerning kiber tahdidlarni aniqlashga doir yozgan ilmiy maqolalari asosida “data-driven models”, “Deep learning” va tushuntiriluvchi sun’iy intellekt “Explainable AI – XAI” usullarining keng imkoniyatlari chuqur o‘rganilgan. “AI-driven cybersecurity and threat intelligence” nomli yirik tadqiqotlarida muhim infratuzilmalarni himoya qilishda anomaliyalarni aniqlovchi va voqealarni korrelyatsiya qiluvchi neyron tarmoqlar qanchalik muhimligi, bu tarmoqlar nol-kun hujumlarini qanday qilib barvaqt aniqlay olishi matematik modellar yordamida isbotlangan.[3] Shuningdek, M.A. Ferrag, Y. Yigit va ularning xalqaro tadqiqot guruhi tomonidan olib borilgan innovatsion izlanishlarda yirik til modellari (LLMs) va generativ sun’iy intellektning CIP tizimlariga tatbiq etilishi batafsil tahlil qilingan.“Kiber xavfsizlik va fizik xavfsizlikni birgalikda tahlil qilish” uslubini ilgari surganlar, Agentic AI tizimlarining xavfsizlikni ta’minlashdagi avtonom rolini yoritib berishgan.[4] Shu bilan bir qatorda, AQShning Jorjtaun

[3] Sarker, I. H., Janicke, H., Abuadbba, A., & Ferrag, M. A. (2024). Multi-Aspect Rule-Based AI: Methods, Taxonomy, Challenges and Directions toward Automation, Intelligence and Transparent Cybersecurity Modeling for Critical Infrastructures. Internet of Things.

[4] Yigit, Y., Ferrag, M. A., Ghanem, M. C., Sarker, I. H., Maglaras, L. A., Chrysoulas, C., Moradpoor, N., Tihanyi, N., & Janicke, H. (2025). Generative AI and LLMs for Critical Infrastructure Protection: Evaluation Benchmarks, Agentic AI, Challenges, and Opportunities. Sensors, 25(6), 1666. https://doi.org/10.3390/s25061666

universiteti qoshidagi Xavfsizlik va rivojlanayotgan texnologiyalar markazi (CSET) tadqiqotchilari A. Leblang va M. McGee o‘z hisobotlarida SI faqatgina mudofaa vositasi emas, balki qora niyatli xakerlar tomonidan qo‘llaniluvchi o‘ta xavfli qurol ekanligini, shu sababli xavfsizlik amaliyotida sun’iy intellekt modellarining o‘zini ham “zaharli ma’lumotlar” va raqib xujumlaridan himoya qilish qoidalari ishlab chiqilishi lozimligini alohida ko‘rsatib o‘tishgan.[5]

Mazkur maqolada ilmiy va amaliy yo‘nalishlarni o‘rgangan holda mavjud bo‘shliq va yutuqlarni tahlil qilinadi hamda takliflar ilgari suriladi

II. METODLAR

Ushbu tadqiqotni samarali amalga oshirish maqsadida bir qancha metodologik usullardan foydalanildi, xususan:

Birinchidan, normativ-huquqiy tahlili: Tadqiqotning dastlabki bosqichida kiberxavfsizlik va sanoat boshqaruv tizimlariga (ICS) oid xalqaro qonunchilik tajribalari, xalqaro ko‘rsatmalar hamda O‘zbekiston Respublikasining me’yoriy-huquqiy bazasi huquqiy tahlil qilindi. Asosiy e’tibor 2022-yil 15-aprelda qabul qilingan va 17-iyulda kuchga kirgan “Kiberxavfsizlik to‘g‘risida”gi O‘zbekiston Respublikasi Qonuni (O‘RQ-764) talablariga, xususan, qonunning VI bobi – “Muhim axborot infratuzilmasi obyektlari kiberxavfsizligi” qoidalariga qaratildi.[6] Qonunga muvofiq, O‘zbekistonda obyeklarni toifalash va ularning yagona davlat reyestrini yuritish tartibi, xavfsizlik subyektlarining huquq va majburiyatlari tizimlashtirib o‘rganildi.

Ikkinchidan, SI va Deep learning algoritmlarini kiber-anomaliyalarni aniqlashda qo‘llash natijalari xalqaro amaliyot (Scopus, IEEE bazalari ko‘rsatkichlari) orqali o‘rganildi.

Uchinchidan, qiyosiy-huquqiy metod: O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi qonunining moddalari tahlil qilinib, obyektlarni toifalash va yagona reyestrni shakllantirish jarayonlarining ishlash mexanizmi o‘rganildi Ushbu milliy talablar Yevropa Ittifoqining 2022-yilda e’lon qilingan NIS2 direktivasi hamda AQSh federal amaliyoti bilan qiyosiy huquqiy tahlil qilindi. Bu metod.

Tadqiqotning obyekti sifatida davlat boshqaruvi, iqtisodiy barqarorlik va jamiyat xavfsizligi uchun strategik ahamiyatga ega bo‘lgan muhim infratuzilma (MI)

[5] Gerstein, A., Leblang, A., McGee, M., Rattray, G., Richards, L., & Scott, A. (2024, October). Securing Critical Infrastructure in the Age of AI. Center for Security and Emerging Technology (CSET).

[6] O'zbekiston Respublikasi qonuni. (2022). Kiberxavfsizlik to'g'risida (O'zbekiston Respublikasining 2022 yil 15 apreldagi O'RQ-764-son Qonuni). https://lex.uz/docs/5960601

obyektlarining axborot va apparat-dasturiy majmualari, Sanoat boshqaruv tizimlari (ICS), Kiber-fizik tizimlar (CPS) olingan.

III. NATIJALAR

Olib borilgan tadqiqotda, muhim infratuzilma obyektlarining (MIO) kibermakondagi xavfsizlik holati, tahdidlar va ularga qarshi kurashish siyosati bo‘yicha xalqaro va milliy tajribalar o‘rganildi. Rivojlangan davlatlar, transmilliy korporatsiyalar tajribasi va yirik xalqaro kiberxavfsizlik idoralari masalan, AQShning CISA agentligi, ENISA hisobotlari shuni tasdiqlamoqdaki, hozirgi davrda kiber tahdidlarning motivatsiyasi faqatgina shaxsiy ma’lumotlarni o‘g‘irlash yoki onlayn firibgarlikdan o‘zgarib, davlat va ijtimoiy tizimlarni falaj qilish va infratuzilmalarga to‘g‘ridan-to‘g‘ri qaratila boshlangan.

Quyidagi 1-jadvalda muhim infratuzilma axborot xavfsizligiga oid xalqaro va mahalliy miqyosdagi statistik raqamlar keltirilgan.

1-jadval. Kiberxavfsizlik ko‘rsatkichlarining asosiy statistik va iqtisodiy tahlili (2023-2025 yy.)

Ko‘rsatkich / Indikator nomi	**Miqdori va yillik dinamik tavsifi**	**Manba / Asos**
Global miqyosda ma’lumotlar buzilishining o‘rtacha qiymati (2024 y.)	O‘rtacha hisobda 4,88 million AQSh dollari	IBM xalqaro tahdidlar tahlili hisoboti[7]
AQSh davlat infratuzilmalarida bloklangan zararli ulanishlar miqdori	371 million ta zararli tarmoq ulanishlari to‘xtatildi (2023-2024 yillar davomida CISA harakatlari)	CISA yillik rasmiy hisoboti[8]
O‘zbekiston Respublikasi yagona kiberxavfsizlik ko'rsatkichi (2024 y.)	NCSI (National Cyber Security Index) reytingida O'zbekiston o'z	Kiberxavfsizlik markazi

[7] IBM. (2024). Cost of a data breach 2024: Financial industry insights. IBM Think Insights. https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry

[8] CISA's 2025 Year in Review: Driving Security and Resilience Across Critical Infrastructure, accessed March 31, 2026, https://www.cisa.gov/news-events/news/cisas-2025-year-review-driving-security-and-resilience-across-critical-infrastructure

	pozitsiyasini mustahkamlab bormoqda	ma’lumotlari[9]
OT va ICS tizimlari mavjud korxonalarda kiberxavfsizlikka qaratilayotgan e’tibor	Tashkilotlarning 58 foizi o‘z e’tiborini IT dan bevosita OT xavfsizligini ta’minlashga yo'naltirmoqda	CompTIA tahliliy hisoboti.[10]
O‘zbekistonda Kiberxavfsizlik xizmati faoliyati ko'rsatkichi (2021-2023 yy.)	“UZ” milliy domen zonasida 17 milliondan ortiq zararli va shubhali tarmoq faolliklari bartaraf etildi	O'zbekiston DXX Kiberxavfsizlik markazi hisoboti.[11]

Yuqoridagi jadval ma’lumotlari tahlili shuni ko’rsatadiki, muhim infratuzilma obyektlarining kibermakonga integratsiyasi butun jahonda bo‘lgani kabi O‘zbekiston Respublikasida ham jiddiy tavakkalchiliklarni va himoya zaruratlarini oshirib yuborgan. “Kiberxavfsizlik to‘g‘risida”gi qonunning qabul qilinishi va amaliyotga tatbiq etilishi natijasida mamlakatimizda o‘ta dolzarb qadam tashlandi: yagona mudofaani yaratish uchun obyektlarni “toifalash” va davlat miqyosida “Yagona reyestr”ni shakllantirish instituti joriy qilindi. Qonunning 26 va 27-moddalariga asosan, davlat xizmatlari, energetika, moliya, sog‘liqni saqlash, kimyo va transport tizimidagi MIOlar o‘zining jamiyat uchun ijtimoiy, iqtisodiy, siyosiy va ekologik ahamiyatidan kelib chiqib tegishli xavfsizlik toifalariga ajratilmoqda hamda Davlat xavfsizlik xizmati tomonidan nazoratga olinmoqda.

Demak, ushbu obyektlarni muhofaza qilish uchun faqatgina milliy darajada emas, balki xalqaro darahada ham yaxlit bir qonunchilik hujjatini qo‘llash maqsadga muvofiq hisoblanadi.

IV. MUHOKAMA

Yuqorida keltirilgan statistika, qonunchiligi normalarini tahlil qilgan holda aytish mumkinki, muhim infratuzilma va zamonaviy raqamli iqtisodiyot sohasida “mutlaq xavfsizlik” degan tushuncha umuman mavjud emas va bo‘lishi ham mumkin

[9] O'zbekiston Respublikasi Prezidentining “O'zbekiston Respublikasi Milliy statistika qo'mitasi faoliyatini tashkil etish - Stat.uz, accessed March 31, 2026, https://stat.uz/img/news/pq-75-ijro-holati-jami_p26636.pdf

[10] State of Cybersecurity 2025 | CompTIA Report, https://www.comptia.org/en-us/resources/research/state-of-cybersecurity/

[11] «Kiberxavfsizlik to'g'risida»gi qonun: DXXga qanday yangi vakolatlar berildi? - Kun.uz, https://kun.uz/66602542

emas. Ma’lumotlarning va ishlab chiqarish vositalarining tezkorlik bilan raqamlashuvi va IT/OT arxitekturasining qaytarilmas konvergensiyasi ishlab chiqarish samaradorligi uchun imkoniyatlar yaratish bilan birga, mutlaqo inobatga olinmagan, iqtisodiyotni xonavayron qilishi mumkin bo‘lgan jiddiy kiber tavakkalchiliklarni tug‘dirmoqda.[12] Avvalgi o‘n yillikda amalda bo‘lgan va ko‘pchilik operatsion texnologiyalar muhandislari tomonidan hamon xavfsizlikning oltin standarti sifatida ko‘riladigan “Air-gap” yopiq tizimlarning tashqi tarmoqlarga mutlaqo ulanmasdan ishlashini eskirga usul deb qavbul qilsak bo‘ladi, chunki “Air-gap” endilikda o‘zini oqlaydigan konsepsiya emas. Eronning Natanz yadroviy stansiyasidagi voqealarni yuzaga keltirgan “Stuxnet” qurt-virusi va undan keyingi sanoat tajribasi isbotladiki, to‘g‘ridan-to‘g‘ri internetga ulanmagan eng maxfiy va yopiq tizimlarga ham muhandislarning oddiy noutbuklari, himoyalanmagan USB fleshkalari, uchinchi tomon yetkazib beruvchilarining buzilgan dasturlari yoki bevosita xodimlar yordamida osonlik bilan zararli kod kiritilishi, tizim izdan chiqarilishi mumkin.[13]

O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi qonunida qabul qilingan markazlashgan davlat boshqaruvi va MIOlarning yagona reyestrini shakllantirib, yuritish tizimini davlatchilik ehtiyojlari nuqtai nazaridan amalga oshirilishi ijobiy o‘zgarish hisobalandi. Buning sababi juda oddiy: davlat o‘z hududida aynan qaysi inshootlar MIO maqomiga ega ekanligini, ular davlat yoki xususiy sektor vakillari qatoridan kimga tegishli ekanligini, ular qanday dasturiy ta’minotdan foydalanayotgani va ularning hozirgi xavfsizlik bahosi qanday ekanligini hisobga olmasdan va ro‘yxatdan o‘tkazmasdan turib, xorijiy tahdidlarga qarshi yagona milliy mudofaa qura olmaydi. O‘zbekistondagi MIO reyestrini yuritish aynan Davlat xavfsizlik xizmati (DXX) organlari tomonidan amalga oshirilishi bu kabi obyektlarning joylashuvi va xavfsizlik sirlarining tarqalib ketmasligini ta’minlashda va davlat nazoratini o‘rnatish uchun eng maqbul yo‘l hisoblanadi.

Ushbu tadqiqot jarayonida muhim infratuzilma tizimlari himoyasini tahlil qilish va tashkilot barqarorligini baholashda dunyoda qo‘llanilayotgan bir nechta xalqaro standart va metodlar chuqur tahlil qilinib, qiyosiy solishtirib ko‘rildi. Birinchi navbatda boshqaruv standartlari solishtirildi. Yevropa Ittifoqida va Osiyo davlatlarida keng tarqalgan, ISO/IEC 27001 axborot xavfsizligi standarti tashkilotlardan hujjatlarni qanday yuritish kerakligi haqida qat’iy normativ qoidalar hamda axborot xavfsizligini boshqarish majburiyatlarini talab qiladi. Biroq, MIOlar o‘ta xilma-xil bo‘lganligi

[12] Botunac, I., Akrap, G., & Esterhajer, J. (2025). Supply Chain Security and AI Risk Governance Model for Critical Infrastructure under the NIS2 Directive. ACIG Journal.

[13] Unveiling the Dark Side: Common Attacks and Vulnerabilities in Industrial Control Systems, https://www.levelblue.com/blogs/spiderlabs-blog/unveiling-the-dark-side-common-attacks-and-vulnerabilities-in-industrial-control-systems/

uchun standart hamma joyda bir xil natija bermaydi. AQSh Milliy standartlar va texnologiyalar instituti tomonidan taqdim etilgan NIST CSF 2.0 metodologiyasi esa ISO dan farqli o‘laroq moslashuvchanlikka va xavflarni markazlashtirib boshqarishga yo‘naltirilgan. Ya’ni NIST doirasida har qanday obyekt uchun o‘z moliyaviy va texnik imkoniyatlaridan kelib chiqib, moslashtirilishi oson kechadi (NIST, 2024).[14]

O‘zbekistonda Kiberxavfsizlik markazi DUK tomonidan sohaga oid davlat standartlari ishlab chiqilgan bo‘lib, ular asosida doimiy reyting yuritilishi va ekspertiza tizimlari (IT-audit) orqali yuridik tashkilotlar o‘z obyektlarida qonunchilik talablarini qay darajada bajarayotganligini nazorat qilish mexanizmlari joriy etilgan (Kiberxavfsizlik markazi, 2023).[15] Bunga misol qilib yuqorida tilga olingan O'zbekiston Markaziy bankining normativ qarorlari asosida, MIO deb huquqiy tan olingan elektron to'lov tizimlari 5 km dan kam bo'lmagan uzilmas masofada o'z ma'lumotlar bazasining zaxira qilingan ko'chirmasini (backup) ishlash holatida ushlab turish sharti rasman belgilanishini keltirish mumkin. Bu O'zbekistondagi MIO himoyasining faqatgina sof IT sohasi emas, balki qat'iy qonuniy byurokratiya va texnik qoidalar simbiozi ekanligi hamda davlat kafolatlarini mustahkamlashdagi muhim normativ qadamdir (O'zbekiston Respublikasi Markaziy banki, 2023).[28]

V. XULOSA

Amalga oshirilgan tadqiqot shuni ko‘rsatdiki, davlatning muhim obyektlarini (elektr stantsiyalari, banklar, suv ta’minoti va h.k.) xakerlardan himoya qilish - bu bir marta qilib qo’yiladigan ish emas, balki doimo yangilanib, rivojlanib turishi kerak bo‘lgan jarayon. Bugungi xakerlar endi faqat bitta tizimni buzib zarar etkazish bilan cheklanmay, butun davlatning iqtisodiyoti va kundalik hayotini izdan chiqarishga harakat qilmoqda. Shu sababli bir qancha muhim choralar ko‘rish tavsiya etiladi. Birinchidan, zavodlar va elektr stantsiyalari kabi obyektlarning tizimlari oddiy internet va ofis kompyuterlaridan to‘liq ajratilishi kerak. Ikkinchidan, xalqaro standartlar asosida majburiy tekshiruv tartibi joriy etilishi lozim. Uchinchidan, hujum bo‘lgandan keyin emas, bo‘lishidan oldin sezib avtomatik to‘xtatadigan sun’iy intellekt tizimlari o‘rnatilishi zarur. To‘rtinchidan, ko‘pincha xakerlar katta obyektni emas, unga xizmat ko‘rsatuvchi kichik firmani nishonga olgani uchun barcha pudratchilar ham xavfsizlik talablariga javob berishi shart. Va nihoyat, xodimlar muntazam ravishda amaliy o‘quv mashg'ulotlaridan o'tkazilishi kerak, chunki eng zaif nuqta ko‘pincha texnologiya emas, odamlarning o‘zi bo‘ladi.

[14] Cybersecurity and the NIST Framework: A Systematic Review of its Implementation and Effectiveness Against Cyber Threats, https://thesai.org/Downloads/Volume16No6/Paper_72-Cybersecurity_and_the_NIST_Framework.pdf

[15] Kiberxavfsizlik markazi. (2023). O'zbekiston Respublikasi Kiberxavfsizligi - 2023 yil hisoboti. O'zbekiston Respublikasi DXX "Kiberxavfsizlik markazi" DUK.

Xulosa qilib aytganda, muhim obyektlarni himoya qilish - bu faqat qimmat dastur sotib olish emas, balki madaniyat, ta’lim, aqlli texnologiyalar va qonun nazoratining birgalikdagi, uzluksiz ishi ekanligi isbotlandi.

Foydalanilgan adabiyotlar ro‘yxati.

1. Aljumaiah, O., Jiang, W., Reddy Addula, S., & Amin Almaiah, M. (2025). Analyzing Cybersecurity risks and threats in IT infrastructure based on NIST Framework. Journal of cyber security and risk auditing, 2025(2), 12–26. https://doi.org/10.63180/jcsra.thestap.2025.2.2
2. IBM. (2024). Cost of a data breach 2024: Financial industry insights. IBM Think Insights. https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry
3. Sarker, I. H., Janicke, H., Abuadbba, A., & Ferrag, M. A. (2024). Multi-Aspect Rule-Based AI: Methods, Taxonomy, Challenges and Directions toward Automation, Intelligence and Transparent Cybersecurity Modeling for Critical Infrastructures. Internet of Things.
4. Yigit, Y., Ferrag, M. A., Ghanem, M. C., Sarker, I. H., Maglaras, L. A., Chrysoulas, C., Moradpoor, N., Tihanyi, N., & Janicke, H. (2025). Generative AI and LLMs for critical infrastructure protection: evaluation benchmarks, Agentic AI, challenges, and opportunities. Sensors, 25(6), 1666. https://doi.org/10.3390/s25061666
5. Gerstein, A., Leblang, A., McGee, M., Rattray, G., Richards, L., & Scott, A. (2024, October). Securing Critical Infrastructure in the Age of AI. Center for security and emerging technology (CSET).
6. O‘zbekiston Respublikasi qonuni. (2022). Kiberxavfsizlik to‘g‘risida (O‘zbekiston Respublikasining 2022 yil 15 apreldagi O‘RQ-764-son Qonuni). https://lex.uz/docs/5960601
7. IBM. (2024). Cost of a data breach 2024: Financial industry insights. IBM Think Insights. https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry
8. CISA’s 2025 Year in Review: Driving Security and Resilience Across Critical Infrastructure, https://www.cisa.gov/news-events/news/cisas-2025-year-review-driving-security-and-resilience-across-critical-infrastructure
9. State of Cybersecurity 2025 | CompTIA Report, https://www.comptia.org/en-us/resources/research/state-of-cybersecurity/
10. «Kiberxavfsizlik to'g'risida»gi qonun: DXXga qanday yangi vakolatlar berildi? - Kun.uz, https://kun.uz/66602542
11. O‘zbekiston Respublikasi Prezidentining “O'zbekiston Respublikasi Milliy statistika qo'mitasi faoliyatini tashkil etish - Stat.uz, accessed March 31, 2026, https://stat.uz/img/news/pq-75-ijro-holati-jami_p26636.pdf

12. Botunac, I., Akrap, G., & Esterhajer, J. (2025). Supply Chain Security and AI Risk Governance Model for Critical Infrastructure under the NIS2 Directive. ACIG Journal.
13. Unveiling the Dark Side: Common Attacks and Vulnerabilities in Industrial Control Systems, https://www.levelblue.com/blogs/spiderlabs-blog/unveiling-the-dark-side-common-attacks-and-vulnerabilities-in-industrial-control-systems/
14. Cybersecurity and the NIST Framework: A Systematic Review of its Implementation and Effectiveness Against Cyber Threats, https://thesai.org/Downloads/Volume16No6/Paper_72-Cybersecurity_and_the_NIST_Framework.pdf
15. Kiberxavfsizlik markazi. (2023). O'zbekiston Respublikasi Kiberxavfsizligi - 2023 yil hisoboti. O'zbekiston Respublikasi DXX "Kiberxavfsizlik markazi" DUK.