

20-Sentyabr, 2026-yil

**MUHIM INFRATUZILMA OBYEKTLARINI KIBERHUJUMLARDAN
HIMOYALASH: TAHDIDLAR, O‘ZARO BOG‘LIQLIK VA RISKLARNI
BOSHQARISH YONDASHUVLARI**

Oripov Asilbek Baxtiyor o‘g‘li

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Kiberxavfsizlik fakulteti, 60611200 – Kiberxavfsizlik injiniringi yo‘nalishi

731-24 KXI guruhi 3-bosqich talabasi

Annotatsiya. Maqolada energetika, transport, telekommunikatsiya, moliya kabi muhim infratuzilma obyektlariga qaratilgan zamonaviy kiberhujumlar, infratuzilmalar o‘rtasidagi o‘zaro bog‘liqlik tufayli yuzaga keladigan kaskadli ta’sirlar hamda ularni himoyalashning risklarga asoslangan yondashuvlari tahlil qilingan. T.A. Johnson tahriri ostida nashr etilgan “Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare” kitobi materiallari asosida maqsadli fishing, ilg‘or doimiy tahdidlar (APT), nol kun zaifliklari va rootkitlar tavsiflangan, Stuxnet hodisasi misolida sanoat boshqaruv tizimlariga qaratilgan hujumlar ko‘rib chiqilgan. NIST kiberxavfsizlik freymvorkining tuzilmasi tahlil qilinib, uni O‘zbekistonda muhim axborot infratuzilmasi obyektlarini himoyalashda qo‘llash bo‘yicha takliflar berilgan.

Kalit so‘zlar: muhim infratuzilma, kiberhujum, APT, SCADA, Stuxnet, o‘zaro bog‘liqlik, kaskadli ta’sir, NIST freymvorki, risklarni boshqarish.

Аннотация. В статье анализируются современные кибератаки на объекты критической инфраструктуры (энергетика, транспорт, телекоммуникации, финансы), каскадные эффекты, возникающие вследствие взаимозависимости инфраструктур, а также риск-ориентированные подходы к их защите. На основе материалов книги «Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare» под редакцией Т.А. Джонсона описаны целевой фишинг, продвинутые устойчивые угрозы (APT), уязвимости нулевого дня и руткиты, рассмотрены атаки на промышленные системы управления на примере Stuxnet. Проанализирована структура NIST Cybersecurity Framework и предложены рекомендации по её применению для защиты объектов критической информационной инфраструктуры в Узбекистане.

Ключевые слова: критическая инфраструктура, кибератака, APT, SCADA, Stuxnet, взаимозависимость, каскадный эффект, NIST Framework, управление рисками.

Abstract. The article analyzes modern cyber attacks targeting critical infrastructures such as energy, transportation, telecommunications and finance, the cascading effects caused by interdependencies between infrastructures, and risk-based approaches to their protection. Based on the book “Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare” edited by T.A. Johnson, spear-phishing, advanced persistent threats (APT),

zero-day vulnerabilities and rootkits are described, and attacks on industrial control systems are examined using the Stuxnet case. The structure of the NIST Cybersecurity Framework is analyzed, and recommendations are proposed for its application to the protection of critical information infrastructure in Uzbekistan.

Keywords: *critical infrastructure, cyber attack, APT, SCADA, Stuxnet, interdependency, cascading effect, NIST Framework, risk management.*

KIRISH

Axborot-kommunikatsiya texnologiyalarining iqtisodiyot va davlat boshqaruvining barcha tarmoqlariga chuqur kirib borishi jamiyat hayotini ta'minlovchi tizimlarni yanada samarali qilish bilan birga ularni yangi turdagi tahdidlarga ham ochib qo'ydi. Jahon iqtisodiy forumi kiberxavfsizlikka tahdidlarni bugungi kunda dunyo mamlakatlari duch kelayotgan beshta eng jiddiy global risklar qatoriga kiritgan [1, ix b.]. Kiberhujumlar endilikda faqat alohida tashkilotlarning ma'lumotlarini o'g'irlash bilan cheklanmay, elektr ta'minoti, suv ta'minoti, transport va aloqa kabi hayotiy muhim xizmatlarning uzluksiz ishlashiga ham xavf tug'dirmoqda.

O'zbekistonda ham bu masalaga alohida e'tibor qaratilmoqda. “Raqamli O'zbekiston – 2030” strategiyasi doirasida davlat xizmatlari, energetika, moliya va boshqa sohalarni raqamlashtirish jadal olib borilmoqda [6]. 2022-yilda qabul qilingan “Kiberxavfsizlik to'g'risida”gi Qonunda esa muhim axborot infratuzilmasi obyektlarini himoyalash davlat siyosatining muhim yo'nalishi sifatida belgilangan [5]. Raqamlashtirish ko'lami qanchalik kengaysa, ushbu obyektlarga qaratilgan hujumlarning oqibatlari ham shunchalik jiddiy bo'ladi.

Ushbu maqolaning maqsadi – muhim infratuzilma obyektlariga qaratilgan asosiy kibertahdidlarni tizimlashtirish, infratuzilmalar o'rtasidagi o'zaro bog'liqlikning xavfsizlikka ta'sirini ochib berish hamda xalqaro amaliyotda qo'llanilayotgan risklarga asoslangan himoya yondashuvlarini tahlil qilib, ularni milliy sharoitda qo'llash bo'yicha takliflar ishlab chiqishdan iborat. Tadqiqotning asosiy manbasi sifatida T.A. Johnson tahriri ostidagi “Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare” kitobidan foydalanildi [1].

1. MUHIM INFRATUZILMA TUSHUNCHASI VA TARKIBI

Muhim infratuzilma deganda faoliyatining buzilishi yoki to'xtab qolishi davlat xavfsizligi, iqtisodiyot, aholining hayoti va sog'lig'iga jiddiy zarar yetkazishi mumkin bo'lgan tizimlar va obyektlar majmui tushuniladi. AQShda bu sohadagi asosiy hujjat 2013-yil 12-fevralda imzolangan Prezidentning PPD-21 direktivasi bo'lib, u muhim infratuzilmani 16 ta sektorga ajratgan va har bir sektor uchun mas'ul federal idorani belgilagan [1, 38–40 b.; 4].

Ushbu sektorlarga kimyo sanoati, tijorat obyektlari, aloqa, muhim ishlab chiqarish, to'g'onlar, mudofaa sanoati bazasi, favqulodda xizmatlar, energetika, moliyaviy xizmatlar, oziq-ovqat va qishloq xo'jaligi, davlat obyektlari, sog'liqni saqlash, axborot texnologiyalari, yadro reaktorlari va materiallari, transport tizimlari hamda suv ta'minoti va oqova suv

tizimlari kiradi [1, 39–40 b.]. Bu ro‘yxat muhim infratuzilma faqat texnik obyektlardan emas, balki jamiyat hayotini ta‘minlovchi keng xizmatlar majmuidan iborat ekanini ko‘rsatadi.

Muhim infratuzilmalarning aksariyati bugungi kunda SCADA (Supervisory Control and Data Acquisition) va boshqa sanoat boshqaruv tizimlari orqali masofadan boshqariladi. Bu tizimlar dastlab yopiq muhitda ishlashga mo‘ljallangan bo‘lib, ularning korporativ tarmoqlar va Internetga ulanishi hujumchilar uchun yangi imkoniyatlar yaratdi. Shu sababli muallif SCADA tizimlarining xavfsizligini tarmoqlararo ekranlar va shifrlash kabi vositalar yordamida kuchaytirish zarurligini alohida ta‘kidlaydi [1, 47 b.].

2. MUHIM INFRATUZILMAGA QARATILGAN ZAMONAVIY KIBERTAHDIDLAR

Kitobning birinchi bobida kompyuter sanoati tarixidagi muhim bosqichlar bilan birga zararli dasturlarning evolyutsiyasi ham ko‘rib chiqilgan. Dastlabki yuklash sektori va makro viruslardan boshlab, har bir tarqalishda o‘z signaturasini o‘zgartiruvchi polimorf viruslar va o‘zini yashiruvchi stealth viruslargacha bo‘lgan rivojlanish signaturaga asoslangan himoya vositalarining imkoniyatlari cheklanganini ko‘rsatadi [1, 11 b.]. Muhim infratuzilma uchun esa ancha murakkab, maqsadli hujumlar asosiy xavf manbai hisoblanadi. Ularning asosiy turlari 1-jadvalda umumlashtirilgan.

1-jadval

Muhim infratuzilmaga qaratilgan asosiy hujum turlari [1, 11–13, 175 b.]

Hujum turi	Mohiyati	Misol
Maqsadli fishing (spear-phishing)	Tashkilotning aniq xodimi, ko‘pincha rahbari haqida oldindan ma‘lumot yig‘ilib, uning qiziqishlariga moslashtirilgan zararli ilova yoki havola yuboriladi	Rahbar kompyuteriga o‘rnatilgan zararli dastur buyruq-boshqaruv serveridan ko‘rsatma kutadi
Ilg‘or doimiy tahdid (APT)	Hujumchi tizimga kirib, uzoq vaqt aniqlanmasdan qoladi va maxfiy ma‘lumotlarni yig‘adi yoki o‘zgartiradi	RSA SecurID hujumi (2011), Flame (2012)
Nol kun zaifligi	Ishlab chiqaruvchiga hali ma‘lum bo‘lmagan, tuzatish chiqarilmagan zaiflikdan foydalaniladi	Operation Aurora
Rootkit	Tizimda administrator huquqlarini qo‘lga kiritib, zararli dastur mavjudligini yashiradi	Stuxnet (Natanz obyekti, 2010)
Hujum vositalari to‘plami	Obuna asosida sotiladigan, tajribasi kam jinoyatchilar ham foydalana oladigan tayyor zararli dasturlar	ZeuS: 18 oy davomida onlayn hisoblardan 70 mln dollar o‘g‘irlangan

“O‘ZBEKISTONDA UCHINCHI RENESSANS VA INNOVATSION JARAYONLAR JURNALI”

20-Sentyabr, 2026-yil

Hujum turi	Mohiyati	Misol
Botnet va DDoS	Zararlangan kompyuterlar tarmog‘i orqali xizmatlar ishdan chiqariladi	Estoniya (2007), Gruziya (2008) davlat saytlariga hujumlar

Ushbu hujumlar orasida Stuxnet alohida o‘rin tutadi. Kitobda ta’kidlanishicha, Eronning Natanz uran boyitish obyektiga qarshi qo‘llanilgan bu hujumda rootkit yordamida tizimga kirilgan va o‘ta murakkab kompyuter chuvalchangi joylashtirilgan. Hujumni amalga oshirish kiberkirish usullari bo‘yicha chuqur bilim va eng zamonaviy ekspluatlarni yaratish imkoniyatini talab qilgani uchun u APT hujumining yaqqol namunasi hisoblanadi [1, 13 b.]. Stuxnet tarixda birinchi marta kiberhujum orqali sanoat uskunasiga jismoniy ta’sir ko‘rsatish mumkinligini amalda isbotladi [7].

Kitobning to‘rtinchi bobida keltirilgan davlat darajasidagi kiberhujumlar ro‘yxati ham e’tiborga loyiq. Unda Estoniya hukumati, ommaviy axborot vositalari va banklari saytlarining DDoS hujumlari bilan ishdan chiqarilishi (2007), Gruziyaga harbiy bostirib kirish oldidan davlat serverlariga qilingan hujumlar (2008) hamda Saudi Aramco kompaniyasining 30 mingdan ortiq kompyuterini yo‘q qilgan hujum qayd etilgan [1, 175 b.]. Bu misollar kiberhujumlar harbiy va siyosiy mojarolarning ajralmas qismiga aylanib borayotganini ko‘rsatadi.

3. INFRATUZILMALARNING O‘ZARO BOG‘LIQLIGI VA KASKADLI TA’SIRLAR

Muhim infratuzilmani himoyalashdagi eng murakkab masalalardan biri – ularning bir-biriga bog‘liqligidir. Aydaho milliy laboratoriyasi olimlari P. Pederson, D. Dudenhoefter, S. Hartley va M. Permann tadqiqotlariga ko‘ra, infratuzilmalar siyosat, tartib-qoidalar yoki jismoniy yaqinlik orqali o‘zaro ta’sirlashadi. Bu esa bir infratuzilma chegarasidan chiqib ketadigan murakkab bog‘liqliklarni yuzaga keltiradi [1, 40 b.; 8].

Tadqiqotchilar Kaliforniyadagi energetika inqirozini tahlil qilib, bir infratuzilmadagi uzilishning boshqalarga bosqichma-bosqich tarqalishini ko‘rsatib berganlar. Birinchi darajali ta’sirlar gaz ta’minoti, neft quvurlari va suv ta’minotiga, ikkinchi darajali ta’sirlar kogeneratsiya, neftni qayta ishlash, saqlash terminallari va qishloq xo‘jaligiga tushgan. Uchinchi darajada esa neft qazib olish, avtomobil va havo transporti hamda bank-moliya sohasi zarar ko‘rgan [1, 40 b.]. Muallifning xulosasiga ko‘ra, faqat bitta infratuzilma uchun ishlab chiqilgan himoya strategiyasi bu bog‘liqliklarni hisobga olmaydi va shu sababli yetarli bo‘lmaydi.

Kitobda bundan ham muhim xulosa keltirilgan: davlat iqtisodiyotiga jiddiy zarba berish uchun 16 ta sektordan atigi uchtagina – energetika, transport va telekommunikatsiyaga muvaffaqiyatli hujum qilish kifoya qilishi mumkin. Elektr tarmog‘i qolgan 15 ta infratuzilmaning barchasi bilan bog‘liq bo‘lgani uchun unga qilingan hujum oqibatlarini butun iqtisodiyotga tarqaladi [1, 58 b.]. Bundan tashqari, bunday hujumlar aholining davlat

xavfsizlik va iqtisodiy barqarorlikni ta'minlash qobiliyatiga bo'lgan ishonchini ham susaytiradi.

4. RISKLARGA ASOSLANGAN HIMOYA: NIST KIBERXAVFSIZLIK FREYMVORKI

Muhim infratuzilmaning katta qismi xususiy sektorga tegishli bo'lgani uchun uni himoyalash davlat va biznesning hamkorligini talab qiladi. Kitobda qayd etilishicha, xususiy sektor uzoq vaqt davomida axborot oshkor bo'lishi, sud jarayonlari, intellektual mulkni yo'qotish va shaxsiy ma'lumotlar bilan bog'liq xavotirlar sababli bu hamkorlikdan tiyilib kelgan [1, 58 b.]. Shu muammoni hal qilish maqsadida 2013-yil 12-fevralda imzolangan 13636-sonli farmon bilan NIST ga davlat va xususiy sektor bilan birgalikda muhim infratuzilma kiberxavfsizligini oshirish freymvorkini ishlab chiqish topshirildi. Freymvorkning 1.0 versiyasi 2014-yil fevralida e'lon qilindi [1, 58–59 b.; 2].

Freymvork uch tarkibiy qismdan iborat: freymvork yadrosi, joriy etish darajalari va freymvork profili. Yadro barcha sektorlar uchun umumiy bo'lgan kiberxavfsizlik faoliyati turlari, kutilgan natijalar va tegishli standartlarni o'z ichiga oladi. Joriy etish darajalari tashkilotning risklarni boshqarish amaliyoti qanchalik rivojlanganini “qisman” (1-daraja) dan “moslashuvchan” (4-daraja) gacha bo'lgan shkala bo'yicha tavsiflaydi. Profil esa tashkilotning joriy holatini (“as is”) maqsadli holati (“to be”) bilan solishtirib, takomillashtirish ustuvorliklarini aniqlash imkonini beradi [1, 61–62 b.]. Yadroning beshta asosiy funksiyasi 2-jadvalda keltirilgan.

2-jadval

NIST freymvorki yadrosining asosiy funksiyalari [1, 62–63 b.; 2]

Funksiya	Vazifasi	Kategoriyalarga misollar
Aniqlash (Identify)	Tizimlar, aktivlar, ma'lumotlar va imkoniyatlarga oid kiberxavfsizlik risklarini tushunish va boshqarish uchun asos yaratish	Aktivlarni boshqarish, biznes muhiti, boshqaruv, risklarni baholash
Himoyalash (Protect)	Muhim xizmatlarning uzluksizligini ta'minlovchi himoya choralarini joriy etish	Kirishni nazorat qilish, xodimlarni o'qitish, ma'lumotlar xavfsizligi
Aniqlab olish (Detect)	Kiberxavfsizlik hodisalarini o'z vaqtida aniqlash	Anomaliyalar va hodisalar, uzluksiz monitoring
Javob berish (Respond)	Aniqlangan hodisaga nisbatan choralar ko'rish	Javob berishni rejalashtirish, kommunikatsiya, tahlil
Tiklash (Recover)	Hodisa natijasida buzilgan imkoniyat va xizmatlarni qayta tiklash	Tiklash rejasi, takomillashtirish

Muhim jihati shundaki, bu funksiyalar ketma-ket bajariladigan bosqichlar emas, balki bir vaqtda va uzluksiz amalga oshiriladigan faoliyat yo‘nalishlaridir [1, 62 b.]. Kitob nashr etilganidan keyin freymvork rivojlantirilib, 2024-yilda e‘lon qilingan 2.0 versiyasiga oltinchi funksiya – “Boshqaruv” (Govern) qo‘shildi. U kiberxavfsizlik strategiyasi, rollar va mas‘uliyat hamda risklarni boshqarish siyosatini tashkilot rahbariyati darajasida belgilashga qaratilgan [3].

5. O‘ZBEKISTON SHAROITIDA QO‘LLASH BO‘YICHA TAKLIFLAR

Yuqoridagi tahlil asosida mamlakatimizda muhim axborot infratuzilmasi obyektlarini himoyalashni kuchaytirish uchun quyidagi yo‘nalishlarni taklif etish mumkin:

1. O‘zaro bog‘liqlik xaritasini yaratish. Muhim axborot infratuzilmasi obyektlarini sektorlar kesimida aniqlash bilan birga ular o‘rtasidagi bog‘liqliklarni modellashtirish va birinchi, ikkinchi hamda uchinchi darajali ta’sirlarni baholash lozim. Bunda energetika, telekommunikatsiya va transport sektorlariga ustuvor e‘tibor qaratilishi kerak.

2. Profilga asoslangan o‘zini baholashni joriy etish. Har bir obyekt NIST freymvorki yoki unga mos milliy metodika asosida o‘zining joriy va maqsadli profilini aniqlab, farqni bartaraf etish rejasini ishlab chiqishi maqsadga muvofiq. Bu cheklangan resurslarni eng muhim risklarga yo‘naltirish imkonini beradi.

3. Sanoat boshqaruv tizimlarini himoyalash. Stuxnet tajribasi ko‘rsatganidek, SCADA tizimlarini korporativ tarmoq va Internetdan segmentatsiya qilish, olib qo‘yiladigan qurilmalardan foydalanishni cheklash va texnologik tarmoqlarda uzluksiz monitoringni yo‘lga qo‘yish zarur.

4. Davlat-xususiy sheriklik va axborot almashish. Obyekt egalari va vakolatli davlat organi o‘rtasida hodisalar haqida tezkor axborot almashish tizimini yaratish, shu bilan birga xususiy sektorning maxfiylik va javobgarlik bilan bog‘liq xavotirlarini qonunchilik darajasida hal qilish lozim.

5. Kadrlar tayyorlash. Kitobning so‘nggi bobida virtualizatsiya, ijtimoiy tarmoqlar, narsalar interneti, bulutli hisoblash va katta ma’lumotlar kiberxavfsizlik sohasini tubdan o‘zgartirayotgani va kelajak avlodni bu o‘zgarishlarga tayyorlash zarurligi ta’kidlangan [1, 287, 321 b.]. Shu sababli oliy ta’lim dasturlariga sanoat boshqaruv tizimlari xavfsizligi va kiberhodisalarga javob berish bo‘yicha amaliy mashg‘ulotlarni kengroq kiritish maqsadga muvofiq.

XULOSA

O‘tkazilgan tahlil muhim infratuzilmaga qaratilgan kibertahdidlar oddiy zararli dasturlardan davlatlar tomonidan qo‘llaniladigan, uzoq vaqt yashirin harakat qiluvchi murakkab hujumlargacha rivojlanganini ko‘rsatdi. Stuxnet, Estoniya va Gruziyaga qilingan hujumlar kiberhujumlarning jismoniy va siyosiy oqibatlarga olib kelishi mumkinligini isbotladi.

Infratuzilmalarning o‘zaro bog‘liqligi sababli bitta obyektidagi uzilish kaskad tarzda boshqa sohalarga tarqaladi. Shuning uchun himoya strategiyasi alohida obyekt emas, balki butun tizim darajasida, bog‘liqliklarni hisobga olgan holda ishlab chiqilishi kerak. NIST

20-Sentyabr, 2026-yil

freymvorki kabi risklarga asoslangan yondashuvlar tashkilotlarga o‘z holatini baholash, maqsadli holatni belgilash va resurslarni ustuvor yo‘nalishlarga yo‘naltirish imkonini beradi. Ushbu tajribani “Kiberxavfsizlik to‘g‘risida”gi Qonun talablari bilan uyg‘unlashtirgan holda qo‘llash O‘zbekistonda muhim axborot infratuzilmasi obyektlarining barqarorligini oshirishga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR:

1. Johnson T.A. (ed.). Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare. – Boca Raton: CRC Press, Taylor & Francis Group, 2015. – ISBN 978-1-4822-3923-2.
2. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.0. – Gaithersburg: NIST, 2014.
3. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. – Gaithersburg: NIST, 2024.
4. The White House. Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience. – Washington, 2013.
5. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni. 15.04.2022-yil, O‘RQ-764-son.
6. O‘zbekiston Respublikasi Prezidentining “«Raqamli O‘zbekiston – 2030» strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida”gi Farmoni. 05.10.2020-yil, PF-6079-son.
7. Falliere N., O Murchu L., Chien E. W32.Stuxnet Dossier. Version 1.4. – Symantec Security Response, 2011.
8. Pederson P., Dudenhoefter D., Hartley S., Permann M. Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research. – Idaho Falls: Idaho National Laboratory, 2006.