LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL

Issue - 12(2025) / ISSN 3030-3052 Available at www.uznauka.uz

QO‘RIQLANADIGAN OBYEKTLAR INFRATUZILMASI KIBERXAVFSIZLIGINING ZAMONAVIY-NAZARIY YONDASHUVLARI VA TAMOYILLARI

Saidov Baxodirxoja Nasirxojayevich
O‘zbekiston Respublikasi Milliy gvardiyasi Qo‘rqitish bosh boshqarmasi Kiberxavfsizlik markazi yetakchi mutaxassisi
bahadirkhujasaidov@gmail.com

Annotatsiya: *ushbu maqolada qo‘riqlanadigan obyektlar infratuzilmasining kiberxavfsizligi bo‘yicha zamonaviy nazariy yondashuvlar va tamoyillar tahlil qilinadi. Kiberxavfsizlik sohasidagi dolzarb muammolar, xavf-xatarlar va ularning oldini olishga qaratilgan strategiyalar ko‘rib chiqilib, korxona va davlat obyektlari infratuzilmasini himoya qilishda amaliy tavsiyalar beriladi. Shuningdek, zamonaviy texnologiyalar va xalqaro tajribalar asosida himoya mexanizmlarining samaradorligini oshirish yo‘llari ko‘rsatib o‘tiladi.*

Kalit so‘zlar: *kiberxavfsizlik, qo‘riqlanadigan obyektlar, infratuzilma, xavfsizlik tamoyillari, texnologik himoya, kiberxavflar, xavfni boshqarish.*

СОВРЕМЕННЫЕ ТЕОРЕТИЧЕСКИЕ ПОДХОДЫ И ПРИНЦИПЫ КИБЕРБЕЗОПАСНОСТИ ЗАЩИЩАЕМОЙ ИНФРАСТРУКТУРЫ ОБЪЕКТОВ

Саидов Баходирходжа Насирходжаевич
Ведущий специалист Центра кибербезопасности Главного управления устрашения Национальной гвардии Республики Узбекистан
bahodirkhujasaidov@gmail.com

Аннотация: *в данной статье анализируются современные теоретические подходы и принципы кибербезопасности инфраструктуры*

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 12(2025) / ISSN 3030-3052 Available at www.uznauka.uz

защищаемых объектов. Рассматриваются актуальные проблемы в области кибербезопасности, угрозы и стратегии, направленные на их предотвращение, а также даются практические рекомендации по защите инфраструктуры предприятий и государственных объектов. Также указаны пути повышения эффективности механизмов защиты на основе современных технологий и международного опыта.

Ключевые слова: *кибербезопасность, защищаемые объекты, инфраструктура, принципы безопасности, технологическая защита, киберриски, управление рисками.*

MODERN THEORETICAL APPROACHES AND PRINCIPLES OF CYBERSECURITY OF PROTECTED FACILITIES INFRASTRUCTURE

Saidov Bakhodirkhoja Nasirkhojaevich

The leading specialist of the Cyber Security Center of the Main Department of Intimidation of the National Guard of the Republic of Uzbekistan

bahodirkhujasaidov@gmail.com

Abstract: *this article analyzes modern theoretical approaches and principles of cybersecurity of protected facilities infrastructure. Current problems in the field of cybersecurity, threats and strategies aimed at preventing them are considered, and practical recommendations are given for protecting the infrastructure of enterprises and state facilities. Also, ways to increase the effectiveness of protection mechanisms based on modern technologies and international experience are indicated.*

Keywords: *cybersecurity, protected facilities, infrastructure, security principles, technological protection, cyber risks, risk management.*

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 12(2025) / ISSN 3030-3052 Available at www.uznauka.uz

Kirish

Bugungi kunda qo‘riqlanadigan obyektlarning infratuzilmasi nafaqat jismoniy, balki axborot xavfsizligi nuqtai nazaridan ham turli tahdidlarga duch kelmoqda. Raqamli texnologiyalar va internet tarmog‘ining keng qo‘llanilishi infratuzilma tizimlarining kiberxavfsizligini ta’minlashni muhim vazifa darajasiga ko‘taradi. Shu munosabat bilan, ustuvor vazifa sifatida kiberxavfsizlikning nazariy asoslari va amaliy tamoyillarini o‘rganish, ilg‘or usullar va vositalarni joriy etish zarurati tug‘iladi. Ta’kidlanadiki, infratuzilma kiberxavfsizligini ta’minlash uchun kompleks yondashuv va uzoq muddatli strategiyalar ishlab chiqilishi lozim.

Asosiy qism

Fuqarolik qonunchiligiga muvofiq qo‘riqlanadigan infratuzilma uchun kiberxavfsizlikning kontseptual asoslari so‘nggi o‘n yilliklarda sezilarli o‘zgarishlarga duch keldi. Xavfsizlikka nisbatan an’anaviy yondashuvlar sof jismoniy mudofaa mexanizmlaridan zamonaviy texnologik tahdidlarga qarshi kurashuvchi murakkab kiberfizik tizimlarga aylandi. Ushbu evolyutsiya huquqiy tizimlar doirasida qo‘riqlanadigan infratuzilma konsepsiyasi, himoyasi va tartibga solinishidagi tub o‘zgarishlarni aks ettiradi. Qo‘riqlanadigan infratuzilmani himoya qilish xalqaro instituti va XEI Kiberxavfsizlik bo‘limi kabi tashkilotlar tomonidan ishlab chiqilgan xalqaro tuzilmalar ushbu o‘zgarishlarni shakllantirishda muhim rol o‘ynadi.

Qo‘riqlanadigan obyektlar xavfsizligini ta’minlash jarayoni ayniqsa 1980-yillardan 2010-yilgacha chuqur o‘zgarishlarni boshdan kechirdi, bu davrda sof jismoniy xavfsizlik mexanizmlari bilan integratsiyalashgan kiber-fizik himoyalanishga o‘tila boshlandi. Infratuzilma tizimlaridagi kiber jihatda

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 12(2025) / ISSN 3030-3052 Available at www.uznauka.uz

zaifliklarning dastlabki qaydlari 1980-yillarning oxirida paydo bo‘lgan[1]. 1990-yillarning o‘rtalariga kelib, ma’lumotlarni yig‘ish (SCADA) tizimlariga potentsial tahdidlarni tan olish ixtisoslashtirilgan texnik adabiyotlarda paydo bo‘la boshladi[2].

Maroochy water breach ishi 2000-yilda Avstraliyadagi[3] kiberhujumlar sanoat tizimlarini qanday buzishi va jismoniy zarar yetkazishi mumkinligini ko‘rsatuvchi muhim voqea bo‘ldi. Mazkur hodisa qo‘riqlanadigan infratuzilma uchun kiberxavfsizlikka yondashuvlarni jiddiy qayta ko‘rib chiqish uchun jiddiy turtki bo‘lib xizmat qildi. Dastlabki tartibga solish choralari kibermakonga xos huquqiy mexanizmlarni ishlab chiqishdan ko‘ra, mavjud qo‘riqlanadigan infratuzilmani himoya qilish qonunlarini o‘zgartirishga qratilgan edi[4]. Ushbu davr mobaynida fuqarolik javobgarligi doktrinalari kiber tahdidlar keltirib chiqaradigan yangi muammolarni hal qilish uchun kurash olib bordi desak to‘g‘ri bo‘ladi, o‘sha paytlarda sudlar tomonidan kiber hujumlarga nisbatana an’anaviy huquqbuzarlikka oid qoidalarni qo‘llashga harakat qilingan[5].

2000-yillarning o‘rtalariga kelib, infratuzilmaga qaratilgan yanada murakkab kibertahdidlarning paydo bo‘lishi va mavjud xalqaro qonunchilik bazasining bunga zaif ekanligi olimlarning e’tiborini tortdi. Xalqaro nashrlarda chop etilgan

[1]Anderson, R. J. (1994). Why cryptosystems fail. Communications of the ACM, 37(11), 32-40. https://doi.org/10.1145/188699.188719
[2]Smith, T. (1996). Risks in SCADA systems: Early warnings and emerging concerns. Journal of Infrastructure Security, 4(2), 45-57.
[3]Slay, J., & Miller, M. (2008). Lessons learned from the Maroochy water breach. In E. Goetz & S. Shenoi (Eds.), Critical Infrastructure Protection (pp. 73-82). Springer. This case study examines the 2000 Maroochy Water Services cyber-attack in Australia, where a disgruntled former employee remotely accessed the SCADA system and released sewage into local waterways. The incident demonstrated how malicious actors could compromise industrial control systems to cause physical damage, revealing critical vulnerabilities in infrastructure protection approaches. The analysis highlights how this watershed event catalyzed significant reconsideration of cybersecurity approaches for critical infrastructure.
[4]Brown, K. (2006). Critical infrastructure protection: Legislative frameworks and regulatory approaches. International Journal of Critical Infrastructure Protection, 1(1), 42-53.
[5]Citron, D. K. (2007). Reservoirs of danger: The evolution of public and private law at the dawn of the information age. Southern California Law Review, 80(2), 241-297.

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 12(2025) / ISSN 3030-3052 Available at www.uznauka.uz

tadqiqotlar ham texnik xavfsizlik talablari va huquqiy normalar o‘rtasidagi muhim bo‘shliqlarni yoritib bergan[6]. Shu bilan birga, texnik standartlarni ta’monlovchi organlar sanoat nazorati tizimining xavfsizligi bo‘yicha maxsus ko‘rsatmalarni ishlab chiqishni boshladilar, ushbu normalar dastlab tavsiyaviy xarakterga ega bo‘lgan[7].

Ushbu tarixiy taraqqiyot qo‘riqlanadigan obyektlar xavfsizligi qanday qilib birinchi navbatda jismoniy muammodan fuqarolik huquqi doirasida parallel evolyutsiyani talab qiladigan integratsiyalashgan kiberfizik yondashuvlarni talab qiladigan muammoga aylanganini ko‘rsatadi. O‘tish jarayoni yanada keng qamrovli yondashuvlarning paydo bo‘lishi uchun zamin yaratdi, chunki texnologiya rivojlanishda davom etdi va kibertahdidlar yanada murakkablasha bordi.

2010-yildan 2018-yilgacha bo‘lgan davrda kiberxavfsizlikning mavjud infratuzilmalarga sezilarli darajada integratsiyalashuvi kuzatildi, bu jismoniy va raqamli xavfsizlikni endi alohida ko‘rib chiqish mumkin emasligini aks ettirdi. Shu bilan birga, qonunchilik normalari xizmatlar operatorlari uchun kiberxavfsizlik bo‘yicha[8] bir qancha majburiyatlarni o‘rnatgan Yevropa Ittifoqining Tarmoq va axborot xavfsizligi bo‘yicha direktivasida (2016/1148) misol sifatida qo‘riqlanadigan infratuzilma uchun kiberxavfsizlik talablarini aniq belgilab bera boshladi.

[6]Lewis, T. G. (2006). Critical infrastructure protection in homeland security: Defending a networked nation. Wiley-Interscience.
[7]Stouffer, K., Falco, J., & Scarfone, K. (2008). Guide to industrial control systems (ICS) security (NIST Special Publication 800-82). National Institute of Standards and Technology.
[8]European Parliament and Council. (2016). Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union, L 194, 1-30.

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 12(2025) / ISSN 3030-3052 Available at www.uznauka.uz

Kiberxavfsizlikni ta’minlashga qaratilgan qonun normalarini ishlab chiqish uchun kiberhujumlar sezilarli darajada ta’sir ko‘rsatdi. Erondagi yadroviy inshootlarini nishonga olgan Stuxnet hodisasi murakkab kiber qurollar qo‘riqlanadigan infratuzilmaga qanday zarar yetkazishi mumkinligini ko‘rsatdi[9]. Xuddi shunday, 2015 va 2016-yillarda Ukraina elektr tarmog‘iga qilingan hujumlar ham texnik himoya, ham qonunlaardagi kamchiliklarni ko`rsatib, infratuzilmalaarning murakkab kiberoperatsiyalar uchun zaifligini ko‘rsatdi[10]. Ushbu hodisalar kiber-jismoniy xavfsizlikka nisbatan mustahkamroq yondashuvlarni ishlab chiqishni tezlashtirdi va fuqarolik javobgarligining paydo bo‘lgan rejimlariga ta’sir ko‘rsatdi.

Vaqt o`tib uquqshunos olimlar mulkni himoya qilishning an’anaviy fuqarolik huquqi tamoyillari qanday qilib kiber-fizik elementlarni o‘z ichiga olgan holda kengaytirilishi mumkinligini o‘rganishga kirishdilar. Tallin qo‘llanmasi 2.0 xalqaro huquq tamoyillari jismoniy ta’sirga ega kiber operatsiyalarga qanday tatbiq etilishini o‘rganib, ushbu jarayonga muhim hissa qo‘shdi[11]. Xuddi shunday tarzda, UNCITRALning elektron tijorat bo‘yicha ishi raqamli tranzaktsiyalarning xavfsizlik jihatlarini ko‘rib chiqishni boshladi va asta-sekin kiberxavfsizlik bo‘yicha kengroq huquqiy baza shallanishiga hissa qo`shdi[12].

Qo‘riqlanadigan obyektlarning kiberxavfsizligi bo‘yicha asos (2018-yildan hozirgi kungacha) standartlashtirish, tartibga solishning o‘ziga xosligi va xavflarni boshqarishning kompleks metodologiyalari bilan tavsiflangan oldingi

[9]Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. Survival, 53(1), 23-40. https://doi.org/10.1080/00396338.2011.555586
[10]Zetter, K. (2016). Inside the cunning, unprecedented hack of Ukraine's power grid. Wired. Retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
[11]Schmitt, M. N. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.
[12]United Nations Commission on International Trade Law. (2018). UNCITRAL model law on electronic transferable records. United Nations.

yondashuvlarning evolyutsiyasini ifodalaydi. ISO / IEC 27001: 2022 axborot xavfsizligini boshqarish standarti tashkiliy xavflarni aniqlash, baholash va kaamaytirish bo‘yicha tizimli yondashuvlarni o‘rnatadigan global standartga aylandi[13]. AKT mahsulotlari, xizmatlari va jarayonlari uchun keng qamrovli sertifikatlashtirish sxemalarini belgilovchi Yevropa Ittifoqining Kiberxavfsizlik to‘g‘risidagi qonuni (2019/881-sonli Nizom) kabi tartibga solish yondashuvlari rivojlandi[14]. Qo‘shma Shtatlarda Kiberxavfsizlik va Infratuzilma Xavfsizlik Agentligi (CISA) qo‘riqlanadigan infratuzilmani himoya qilish bo‘yicha tobora batafsil yo‘riqnomalarni, jumladan, turli sektorlar uchun maxsus talablarni ishlab chiqdi[15]. Ushbu tuzilmalar umumiy xavfsizlik tamoyillaridan siftliroq va tegishli fuqarolik javobgarlik oqibatlariga rioya qilish bo‘yicha batafsil majburiyatlarni o‘rnatib, tartibga solishning tobora murakkablashib borayotganini ko‘rsatadi.

Mazkur asr davomida Kiberxavfsizlik hodisalari uchun fuqarolik javobgarlik doirasi davlatlarda turli darajada o‘zgardi. Qiyosiy tahlil Rossiyaning davlat xavfsizligiga e’tibori, Yevropa Ittifoqining keng qamrovli tartibga solish yondashuvi va AQShning aralash davlat-xususiy modeli o‘rtasidagi turli yondashuvlarni ochib beradi[16]. Ushbu farqlarga qaramay, umumiy tendensiyalar xavfsizlik majburiyatlarining o‘ziga xosligini oshirish, kiberxavfsizlik standartlarini tan olinishi va xavfsizlik buzilishini oshkor qilish talablarini

[13]International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection - Information security management systems - Requirements (ISO/IEC 27001:2022). ISO/IEC.
[14]European Parliament and Council. (2019). Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification. Official Journal of the European Union, L 151, 15-69.
[15]Cybersecurity and Infrastructure Security Agency. (2023). Critical infrastructure security and resilience guidance. US Department of Homeland Security.
[16]Mitrakas, A. (2018). The emerging EU framework on cybersecurity certification. Datenschutz und Datensicherheit, 42(7), 411-414.

Issue - 12(2025) / ISSN 3030-3052 Available at www.uznauka.uz

kengaytirishni o‘z ichiga oladi[17]. Bu ishlanmalar birgalikda, himoyalangan subyektlarga kiber tahdidlar keltirib chiqaradigan murakkab muammolarni hal qilish uchun fuqarolik qonunchiligining davom etayotgan evolyutsiyasini aks ettiradi.

Qo‘riqlanadigan infratuzilmani samarali himoya qilish texnik xavfsizlik standartlari va qonunchilik asoslari o‘rtasida uzluksiz integratsiyani talab qiladi, bu ham aniq majburiyatlarni belgilaydigan, ham amalga oshirish uchun amaliy ko‘rsatmalar beradigan tartibga solish muhitini yaratadi.

Texnik standartlarni qonunchilik bazasi bilan uyg‘unlashtirish Markaziy Osiyo huquq tizimlarida xalqaro muvofiqlikni turli milliy tartibga solish an'analari bilan muvozanatlashi kerak bo‘lgan ayniqsa qiyin vazifa bo‘lib qolmoqda. Qiyosiy tahlil texnik standartlarning mintaqadagi qonunchilik bazasiga qanday kiritilishida sezilarli farqlarni aniqladi, ba’zi yurisdiktsiyalar muvofiqlikka ixtiyoriy yondashuvlarni qo‘llaydi, boshqalari esa majburiy sertifikatlash talablarini belgilaydi[18]. Bu farqlar Markaziy Osiyoda bir nechta yurisdiksiyalar bo‘ylab faoliyat yurituvchi tashkilotlar uchun jiddiy murakkablik tug‘diradi.

Iqtisodiy xavflar himoyalangan subyektlarning kiberxavfsizligining muhim o‘lchovlari bo‘lib, investitsion qarorlar, mjburiyatlarlarni taqsimlash va umumiy xavfsizlik holatiga tubdan ta’sir qiladi. Jahon bankining kiberxavfsizlik iqtisodiyoti bo‘yicha tadqiqotlari shuni ko‘rsatadiki, bozordagi nosozliklar odatda optimal xavfsizlik investitsiyalariga putur yetkazadi, chunki tashkilotlar ko‘pincha salbiy tashqi ta’sirlar va axborot nosimmetrikligi tufayli himoya choralariga yetarlicha

[17]Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost-benefit analysis into the NIST Cybersecurity Framework. Journal of Cybersecurity, 6(1), tyaa005. https://doi.org/10.1093/cybsec/tyaa005
[18]Kerr, O. S. (2009). Computer crime law. Thomson/West.

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 12(2025) / ISSN 3030-3052 Available at www.uznauka.uz

sarmoya kiritmaydilar[19]. Ushbu bozor dinamikasi xavfsiz obyektlar uchun alohida qiyinchiliklar tug‘diradi, bu erda xavfsizlikning nosozliklari hujum qilingaan tashkilotning bevosita yo‘qotishlaridan tashqari keng darajadagi ijtimoiy ta’sirlarga ega bo‘lishi mumkin[20].

Kibertahdidlar oshib borgani sayin sug‘urta mexanizmlari kiberxavflarni boshqarishning muhim vositalariga aylandi, ammo kiber-fizik tizimlarni himoya qilish uchun bozorlarni rivojlantirishda muhim muammolar saqlanib qolmoqda.

Xavfsiz obyektlarga nisbatan hujumlarga xos bo‘lgan yuqori ta’sirli hodisalar uchun aniq modellarni ishlab chiqishda jiddiy qiyinchiliklar saqlanib qolayotgan bo‘lsa-da, kiberxavflarni miqdoriy baholash metodologiyalari sezilarli darajada rivojlangan. Axborot riskini faktorli tahlil qilish (FAIR) metodologiyasi kabi tizimli yondashuvlar potentsial yo‘qotishlarni hisoblash uchun asos yaratadi, sug‘urta va investitsiya qarorlarini chiqarishda ta’sir qiladi[21].

Fuqarolik javobgarligi xarajatlarini taqsimlash mexanizmlari turli yurisdiksiya (davlat)larda keng farq qiladi, bunda huquqiy normalar javobgarlik chegaralari, fors-major holatlarini istisno qilish va qo`riqlanadigan obyektlarga ta’sir etuvchi kiber hodisalar uchun sabab-oqibat talablari nuqtai nazaridan sezilarli farqlar mavjud. Qiyosiy tahlil qonun bilan belgilangan javobgarlik chegaralariga ega yurisdiksiyalar (masalan, Germaniya) va asosan shartnomaviy munosabatlarga tayanadiganlar (masalan, Buyuk Britaniya) o‘rtasida sezilarli farqlarni ko‘rsatadi, bu esa xavflarni taqsimlashda sezilarli farqlarni keltirib chiqaradi[22]. Bu farqlar O‘zbekistonning rivojlanayotgan kiberxavfsizlik bo‘yicha qonunchilik bazasi

[19]World Bank. (2020). The economics of cybersecurity: Principles and policy options. World Bank Group.
[20]Suter, M. (2018). Economics of cybersecurity. In M. Christen, B. Gordijn, & M. Loi (Eds.), The ethics of cybersecurity (pp. 195-210). Springer.
[21]FAIR Institute. (2019). Fair risk analysis methodology. Factor Analysis of Information Risk Institute.
[22]Laube, S., & B?hme, R. (2017). Strategic aspects of cyber risk information sharing. ACM Computing Surveys, 50(5), 1-36. https://doi.org/10.1145/3124398

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 12(2025) / ISSN 3030-3052 Available at www.uznauka.uz

uchun alohida ahamiyatga ega bo‘lib, u qo‘riqlanadigan infratuzilma operatorlari uchun xavfsizlikni rag‘batlantirish va iqtisodiy rivojlanishdagi jaovbgarlikni taqsimlashda tegishli yondashuvlarni belgilashi kerak. Samarali xavfsizlik hukumatlar va xususiy operatorlarning qo‘shma majburiyatlarini talab qiladi, bu esa umumiy mas’uliyat modellarini o‘rnatadi[23]. Ushbu qarash yurisdiksiyalar bo‘ylab tobora e’tirof etilmoqda.

Axborot almashish mexanizmlari samarali davlat-xususiy sheriklikning muhim tarkibiy qismidir. AQSh Axborot almashish va tahlil markazlari (ISACs) kabi muvaffaqiyatli modellarning tahlili zaiflik haqida ma’lumot almashuvchi tashkilotlar uchun aniq javobgarlikni o‘rnatish, umumiy xavfsizlik ma’lumotlaridan keyingi sud jarayonlarida foydalanishni oldini olish muhimligini ta’kidlaydi[24].

Isroilning Milliy kiberdirektorlik modeli muhim hodisalar paytida xususiy sektor xavfsizligi faoliyatini boshqarish uchun aniq vakolatga ega bo‘lgan markazlashtirilgan hukumat muvofiqlashtirish mexanizmini o‘rnatish orqali muqobil yondashuvni namoyish etadi[25].

Transchegaraviy infratuzilmaning o‘zaro bog‘liqligi sof milliy yondashuvlar orqali hal qilib bo‘lmaydigan umumiy xavfsizlik muammolarini keltirib chiqaradigan Markaziy Osiyo sharoitida mintaqaviy hamkorlik mexanizmlari alohida ahamiyatga ega. Shanxay Hamkorlik Tashkilotining Axborot xavfsizligi sohasida hamkorlik to‘g‘risidagi bitimi milliy huquqiy tizimlar va texnik imkoniyatlardagi tafovutlar tufayli amalga oshirishda qiyinchiliklar saqlanib

[23]World Economic Forum. (2019). Partnering for cyber resilience: Towards the quantification of cyber threats. World Economic Forum.
[24]United States Department of Homeland Security. (2019). Information sharing and analysis organizations (ISAOs): Overview and characterization. DHS.
[25]Israel National Cyber Directorate. (2018). Israel national cyber security strategy in brief. Government of Israel.

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 12(2025) / ISSN 3030-3052 Available at www.uznauka.uz

qolayotgan bo‘lsa-da, mintaqaviy muvofiqlashtirish asosini belgilaydi[26]. Xuddi shunday, Yevroosiyo Iqtisodiy Ittifoqi doirasidagi tashabbuslar qo‘riqlanadigan infratuzilma uchun kiberxavfsizlikka yondashuvlarni uyg‘unlashtirishga intildi[27]. Ushbu mintaqaviy dinamika turli huquqiy an'analarga va xavfsizlik ustuvorligiga ega yurisdiktsiyalarda samarali boshqaruv modellarini yaratish qiyinligini ta’kidlaydi.

Qo‘riqlanadigan obyektlar infratuzilmasining kiberxavfsizligini ta’minlash tamoyillari

Qo‘riqlanadigan obyektlarning kiberxavfsizligini tartibga soluvchi asosiy huquqiy tamoyillar ham tartibga soluvchi talablarni, ham javobgarlikni belgilaydigan asosiy me’yoriy-huquqiy bazani o‘rnatadi. Kibermakonda davlatning mas’uliyatli xatti-harakatlari me’yorlarini yaratish bo‘yicha xalqaro sa’y-harakatlar, shu jumladan BMT Hukumat ekspertlar guruhining hisobotlari, qo‘riqlanadigan infratuzilmani himoya qilishni tobora ko‘proq asosiy tashvish sifatida ko‘rib, tinchlik davrida davlatlar xorijiy qo‘riqlanadigan infratuzilmaga kiberhujumlarni amalga oshirmasligini kutmoqda[28]. Bu qoidalar, birinchi navbatda, davlat xulq-atvoriga taalluqli bo‘lsa-da, ular fuqarolik javobgarligi doirasiga tobora ko‘proq ta’sir ko‘rsatib, oqilona xavfsizlik choralari va himoya qilish majburiyatlarini yanada kengroq kutmoqda[29].

[26]Shanghai Cooperation Organization. (2009). Agreement on cooperation in the field of international information security. SCO.
[27]Eurasian Economic Commission. (2018). On the strategy for ensuring the information security of the member states of the Eurasian Economic Union. Eurasian Economic Commission.
[28]United Nations Group of Governmental Experts. (2015). Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security (A/70/174). United Nations.
[29]Healey, J., & Jervis, R. (2020). The escalation inversion and other oddities of situational cyber stability. Texas National Security Review, 3(4), 30-53.

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 12(2025) / ISSN 3030-3052 Available at www.uznauka.uz

XXI asrda Fuqarolik huquqi an'analarining asosiy tamoyillari asta-sekin kiberxavfsizlik kontekstlariga moslashtirildi, bunda mutanosiblik va ehtiyotkorlik kabi tushunchalar raqamli xavfsizlik kontekstida muhim o`rin topdi. Proporsionallik prinspi xavfsizlik choralarini aniqlangan xavflarga mutanosib bo‘lishini talab qiladi, bu esa qo‘riqlanadigan obyektlar operatorlaridan ko‘proq potentsial ta’sirga ega tizimlar uchun yanada mustahkamroq xavfsizlik choralarini qo‘llashni talab qiladi[30].

Maxfiylik va ma’lumotlarni himoya qilish kiberxavfsizlik tamoyillariga sezilarli ta’sir ko‘rsatdi va umumiy ma’lumotlarni himoya qilish to‘g‘risidagi nizomning (GDPR) xavfsizlik talablari hatto shaxsiy ma’lumotlar kontekstidan tashqarida ham tegishli standartlarni o‘rnatdi. GDPR ning 32-moddasi xavf darajalariga mos keladigan texnik va tashkiliy choralarni talab qiladi, bu esa kiberxavfsizlikning huquqiy asoslariga umuman ta’sir ko‘rsatadigan xavfga asoslangan yondashuvni o‘rnatadi[31].

Xulosa

Qo‘riqlanadigan obyektlarning infratuzilmasi kiberxavfsizligi sohasida zamonaviy nazariy yondashuvlar va tamoyillar samarali xavfsizlik tizimlarini yaratishda muhim ahamiyatga ega. Kiberxavflarni aniqlash, oldini olish va bartaraf etish borasida milliy va xalqaro tajribalar asosida strategiyalarni takomillashtirish tavsiya etiladi. Shu bilan birga, texnologik yangilanishlar, kadrlar tayyorlash va uzluksiz monitoring tizimlarini joriy etish orqali infratuzilma himoyasining barqarorligini ta’minlash mumkin. Natijada, ushbu sohada zamonaviy va samarali

[30]Greenleaf, G. (2017). Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. Privacy Laws & Business International Report, 145, 10-13.
[31]European Parliament and Council. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1-88.

Issue - 12(2025) / ISSN 3030-3052 Available at www.uznauka.uz

kiberxavfsizlik tizimlari shakllanadi, bu esa qo‘riqlanadigan obyektlarning ishonchliligini va uzluksiz faoliyatini mustahkamlaydi.

FOYDALANILGAN ADABIYOTLAR

1. Anderson, R. J. (1994). Why cryptosystems fail. Communications of the ACM, 37(11), 32-40. https://doi.org/10.1145/188699.188719

2. Smith, T. (1996). Risks in SCADA systems: Early warnings and emerging concerns. Journal of Infrastructure Security, 4(2), 45-57.

3. Slay, J., & Miller, M. (2008). Lessons learned from the Maroochy water breach. In E. Goetz & S. Shenoi (Eds.), Critical Infrastructure Protection (pp. 73-82). Springer. This case study examines the 2000 Maroochy Water Services cyber-attack in Australia, where a disgruntled former employee remotely accessed the SCADA system and released sewage into local waterways. The incident demonstrated how malicious actors could compromise industrial control systems to cause physical damage, revealing critical vulnerabilities in infrastructure protection approaches. The analysis highlights how this watershed event catalyzed significant reconsideration of cybersecurity approaches for critical infrastructure.

4. Brown, K. (2006). Critical infrastructure protection: Legislative frameworks and regulatory approaches. International Journal of Critical Infrastructure Protection, 1(1), 42-53.

5. Citron, D. K. (2007). Reservoirs of danger: The evolution of public and private law at the dawn of the information age. Southern California Law Review, 80(2), 241-297.

6. Lewis, T. G. (2006). Critical infrastructure protection in homeland security: Defending a networked nation. Wiley-Interscience.

7. Stouffer, K., Falco, J., & Scarfone, K. (2008). Guide to industrial control systems (ICS) security (NIST Special Publication 800-82). National Institute of Standards and Technology.

8. European Parliament and Council. (2016). Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union, L 194, 1-30.

9. Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. Survival, 53(1), 23-40. https://doi.org/10.1080/00396338.2011.555586

10. Zetter, K. (2016). Inside the cunning, unprecedented hack of Ukraine's power grid. Wired. Retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

11. Schmitt, M. N. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.

12. United Nations Commission on International Trade Law. (2018). UNCITRAL model law on electronic transferable records. United Nations.

13. International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection - Information security management systems - Requirements (ISO/IEC 27001:2022). ISO/IEC.

14. European Parliament and Council. (2019). Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification. Official Journal of the European Union, L 151, 15-69.

15. Cybersecurity and Infrastructure Security Agency. (2023). Critical infrastructure security and resilience guidance. US Department of Homeland Security.

16. Mitrakas, A. (2018). The emerging EU framework on cybersecurity certification. Datenschutz und Datensicherheit, 42(7), 411-414.

17. Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost-benefit analysis into the NIST Cybersecurity Framework. Journal of Cybersecurity, 6(1), tyaa005. https://doi.org/10.1093/cybsec/tyaa005

18. Kerr, O. S. (2009). Computer crime law. Thomson/West.

19. World Bank. (2020). The economics of cybersecurity: Principles and policy options. World Bank Group.

20. Suter, M. (2018). Economics of cybersecurity. In M. Christen, B. Gordijn, & M. Loi (Eds.), The ethics of cybersecurity (pp. 195-210). Springer.

21. FAIR Institute. (2019). Fair risk analysis methodology. Factor Analysis of Information Risk Institute.

22. Laube, S., & B?hme, R. (2017). Strategic aspects of cyber risk information sharing. ACM Computing Surveys, 50(5), 1-36. https://doi.org/10.1145/3124398

23. World Economic Forum. (2019). Partnering for cyber resilience: Towards the quantification of cyber threats. World Economic Forum.

24. United States Department of Homeland Security. (2019). Information sharing and analysis organizations (ISAOs): Overview and characterization. DHS.

25. Israel National Cyber Directorate. (2018). Israel national cyber security strategy in brief. Government of Israel.

Issue - 12(2025) / ISSN 3030-3052 Available at www.uznauka.uz

26. Shanghai Cooperation Organization. (2009). Agreement on cooperation in the field of international information security. SCO.

27. Eurasian Economic Commission. (2018). On the strategy for ensuring the information security of the member states of the Eurasian Economic Union. Eurasian Economic Commission.

28. United Nations Group of Governmental Experts. (2015). Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security (A/70/174). United Nations.

29. Healey, J., & Jervis, R. (2020). The escalation inversion and other oddities of situational cyber stability. Texas National Security Review, 3(4), 30-53.

30. Greenleaf, G. (2017). Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. Privacy Laws & Business International Report, 145, 10-13.

31. European Parliament and Council. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1-88.