DAVLAT-XUSUSIY SHERIKCHILIK VA KIBERXAVFSIZLIK SOHASIDAGI QONUNCHILIK TAHLILI

Eshmuradov Najmiddin G‘aybullo o‘g‘li
Toshkent davlat yuridik universiteti magistranti
najmiddineshmuradov99@gmail.com

Annotatsiya. *Tezis O‘zbekistonda davlat-xususiy sheriklik (DXSh) va kiberxavfsizlik sohasidagi huquqiy asoslarni tahlil qiladi. “Kiberxavfsizlik to‘g‘risida”gi Qonun (2022) va “Davlat-xususiy sheriklik to‘g‘risida”gi Qonun (2019) asosida ikki soha o‘rtasidagi huquqiy bog‘lanishning yetishmasligi, xususiy sektor ishtiroki uchun aniq mexanizm va rag‘batlarning yo‘qligi asosiy muammo sifatida ko‘rsatiladi. Xalqaro tajribaga (Janubiy Koreya, Buyuk Britaniya, Qozog‘iston) asoslanib, quyidagi takliflar berilgan: kiberxavfsizlik bo‘yicha DXSh milliy konsepsiyasini qabul qilish; DXSh qonuniga maxsus bob kiritish; xususiy sheriklar uchun litsenziya, sertifikatlash va imtiyoz mexanizmlarini joriy etish. Raqamli xavfsizlikni mustahkamlash uchun davlat va xususiy sektor o‘rtasida huquqiy integratsiya zarur.*

Аннотация. *Статья анализирует правовые основы государственно-частного партнерства (ГЧП) и кибербезопасности в Узбекистане. На основе Закона «О кибербезопасности» (2022) и Закона «О государственно-частном партнерстве» (2019) выявлено отсутствие правовой связи между двумя сферами, недостаток четких механизмов и стимулов для участия частного сектора как основная проблема. С опорой на международный опыт (Южная Корея, Великобритания, Казахстан) предложено: принятие национальной концепции ГЧП в сфере*

кибербезопасности; внесение специальной главы в Закон о ГЧП; введение лицензирования, сертификации и льготных механизмов для частных партнеров. Для укрепления цифровой безопасности необходима правовая интеграция государства и частного сектора.

Annotation. *The article analyzes the legal framework of public-private partnership (PPP) and cybersecurity in Uzbekistan. Based on the Law "On Cybersecurity" (2022) and the Law "On Public-Private Partnership" (2019), the main issue identified is the lack of legal linkage between the two areas, as well as the absence of clear mechanisms and incentives for private sector participation. Drawing on international experience (South Korea, United Kingdom, Kazakhstan), the following proposals are made: adoption of a national PPP concept in cybersecurity; inclusion of a dedicated chapter in the PPP Law; introduction of licensing, certification, and incentive mechanisms for private partners. Legal integration between the state and private sector is essential to strengthen digital security.*

Raqamli iqtisodiyot va jamiyatning jadal raqamlashtirilishi sharoitida kiberxavfsizlik masalalari ustuvor ahamiyat kasb etmoqda. Raqamli transformatsiya jamiyat va iqtisodiyotning barcha sohalarini qamrab olgan bir paytda, kiberxavfsizlikni samarali ta'minlash tizimini yaratish muhim zaruratga aylandi. Davlat resurslarining chegaralanganligi sharoitida davlat-xususiy sheriklik kiberxavfsizlik loyihalarini amalga oshirishda xususiy kapital, texnologiyalar va tajribani jalb qilishning samarali vositasiga aylanmoqda. Ammo bunday hamkorlik faqat aniq va mukammal huquqiy asos mavjud bo‘lsa, barqaror va samarali bo‘ladi. So‘nggi yillarda O‘zbekiston davlat-xususiy sheriklik va kiberxavfsizlik sohalarida normativ-huquqiy

asoslarni shakllantirishda jiddiy siljishlarga erishdi. Shu bois, ushbu masala bo‘yicha huquqiy tahlil olib borish dolzarb hisoblanadi.

O‘zbekistonda davlat-xususiy sheriklikning qonunchilik asoslari 2022-yil 15-aprelda qabul qilingan O‘zbekiston Respublikasi “Kiberxavfsizlik to‘g‘risida”gi Qonuni, O‘zbekiston Respublikasi Prezidentining 2020-yil 15-iyunda qabul qilingan “O‘zbekiston Respublikasi axborot tizimlari va resurslarini himoya qilish davlat tizimini joriy etish chora-tadbirlari to‘g‘risida”gi PF-6007-sonli farmoni, O‘zbekiston Respublikasi Prezidentining 2020-yil 15-iyunda qabul qilingan “O‘zbekiston Respublikasida kiberxavfsizlikni ta’minlash tizimini yanada takomillashtirish chora-tadbirlari to‘g‘risida”gi PQ-4751-sonli qarori[1], O‘zbekiston Respublikasi Davlat xavfsizlik xizmati raisining 3458-sonli buyrug‘i asosida 2023-yil 22-sentabrda qabul qilingan “O‘zbekiston Respublikasi kiberxavfsizlik va muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlash darajasini baholash tartibi to‘g‘risida”gi Nizomi hamda boshqa qonunchilik hujjatlaridan iborat.

Kiberxavfsizlik masalalarini tartibga soluvchi asosiy huquqiy hujjat – bu 2022-yil 15-aprelda qabul qilingan O‘zbekiston Respublikasi “Kiberxavfsizlik to‘g‘risida”gi qonuni hisoblanadi. Ushbu qonun birinchi bor **kibermakonda shaxs, jamiyat va davlat manfaatlarini himoya qilish**ni davlat siyosatining ustuvor yo‘nalishi sifatida e’tirof etadi. Asosiy tushunchalar, subyektlar va ularning huquq-mansubligi aniqlashtirilgan. Mazkur qonun, shuningdek, xalqaro shartnomalarga ochiqlik prinsipini mustahkamlab, **xalqaro sheriklik va huquqiy moslashuvchanlik**ka asoslangan yondashuvni ilgari suradi. Mazkur qonun zamonaviy texnologik tahdidlarga qarshi milliy himoya mexanizmini yaratishda **konstitutsiyaviy**

[1] O‘zbekiston Respublikasi qonunchilik ma’lumotlari milliy bazasi https://lex.uz/uz/

himoya asosida yuritilgan. Biroq u yerda davlatning roliga nisbatan haddan tashqari markazlashtirilgan yondashuv hukmron. Mazkur qonunning turli moddalarida (masalan, 11-13-moddalarda) kiberxavfsizlik bo‘yicha asosiy vakolatlar **Davlat xavfsizlik xizmatiga** biriktirilgan. Biroq **xususiy sektorning ishtiroki** alohida va aniq tartibga solinmagan. Vakolatli organlarga axborot tizimlarida tekshiruv, monitoring, texnik vositalardan foydalanish vakolati berilgan, lekin davlat-xususiy sheriklik shakllarida bu qanday qo‘llanishi haqida aniq mexanizmlar mavjud emas. Xususiy sektor – ayniqsa IT kompaniyalar – kiberxavfsizlikda innovatsiya va texnik vositalarni joriy etishda muhim o‘rin egallaydi. Biroq qonunda ular uchun aniq **imtiyozli sharoitlar**, sheriklik mexanizmlari va **xatarni taqsimlash** tartiblari yo‘q.

O‘zbekiston Respublikasi “Kiberxavfsizlik to‘g‘risida”gi **qonundagi imkoniyatlar asosida** davlat-xususiy sheriklik **mexanizmlarini rivojlantirish zarurati mavjud.** Mazkur qonunning **11-modda**sida davlat dasturlarini ishlab chiqish va amalga oshirish vakolati bor. Ushbu dasturlar doirasida xususiy subyektlar ishtirokini rag‘batlantirish mumkin. Mazkur qonunning **14-16-modda**larida esa, axborot tizimlarini muhofaza qilishda davlat va tashkilotlar kiberhimoya vositalaridan foydalanishi mumkinligi ko‘rsatilgan. Mazkur qonunning **28-modda**sida muhim axborot infratuzilmasi subyektlariga choralar ishlab chiqish va amalga oshirish huquqi berilgan[2]. Mazkur qonun davlat-xususiy sheriklik tamoyillariga ochiqlik bildirmasada, mavjud normativ asoslar orqali ularni rivojlantirish mumkin. Buning uchun **kiberxavfsizlik sohasida** davlat-xususiy sheriklik**ning alohida modeli** ishlab chiqilishi lozim (masalan, security-as-a-service, audit, monitoring xizmatlari orqali). Bundan

[2] O‘zbekiston Respublikasi “Kiberxavfsizlik to‘g‘risida”gi Qonuni, 15.04.2022 yildagi O‘RQ-764-son https://lex.uz/uz/docs/-5960604

tashqari, davlat-xususiy sheriklikning huquqiy asosini takomillashtirish zarur, ya’ni xususiy sheriklar huquqlari va javobgarliklari, xizmatlar sertifikatlari va litsenziyalash tartibi, maxfiylik va ma’lumotlardan foydalanish chegaralari belgilanishi kerak.

“Kiberxavfsizlik to‘g‘risida”gi qonunning ijobiy va salbiy jihatlari:

Ijobiy jihatlar	**Salbiy jihatlar**
Kiberxavfsizlikning asosiy tushunchalari va tamoyillari aniqlangan	DXSh mexanizmlari aniq tartibga solinmagan
Davlat siyosati, vakolatli organ va ularning majburiyatlari aniq belgilangan	Vakolatli organlar vakolati haddan ortiq kengaytirilgan
Xalqaro hamkorlikka ochiqlik tamoyili belgilangan	Xususiy sektor bilan sheriklik yondashuvi yetarlicha aks ettirilmagan

O‘zbekiston davlat-xususiy sheriklikni huquqiy jihatdan tan olgan asosiy hujjat bu – 2019-yil 10-maydagi “Davlat-xususiy sheriklik to‘g‘risida”gi Qonun hisoblanadi. Ushbu qonun davlat-xususiy sheriklik tushunchasi, tamoyillari, ishtirokchilari (davlat va xususiy sheriklar), ularning huquq va majburiyatlari, loyihani tayyorlash, tanlov tartibi va amalga oshirish bosqichlarini belgilaydi. Ayniqsa, shaffoflik, bahslashuv asosida sherik tanlash, kamsitmaslik, korrupsiyaga yo‘l qo‘ymaslik tamoyillari ustuvorlik qiladi. Xususiy tashabbuslar (innovatsion takliflar) uchun qonuniy asos mavjud. davlat-xususiy sheriklik bo‘yicha yagona vakolatli organ – Davlat-xususiy sheriklikni rivojlantirish agentligi (Moliya vazirligi huzurida) faoliyat yuritadi.

Davlat-xususiy sheriklik **va kiberxavfsizlik sohasi o‘zaro aloqasida amaliy zarurat shuki,** Kiberxavfsizlik sohasida zamonaviy texnologik vositalarni ishlab chiqish, monitoring qilish, xavfsiz tarmoqlar yaratish va ularni ekspluatatsiya qilishda xususiy sektorning ishtiroki zarur. Lekin “Kiberxavfsizlik to‘g‘risida”gi Qonunda davlat-xususiy sheriklik mexanizmlari alohida qayd etilmagan. Ammo buning **huquqiy imkoniyati ham mavjud.** “Davlat-xususiy sheriklik to‘g‘risida”gi Qonunga muvofiq **Texnologik infratuzilma, IT xizmatlari, monitoring platformalari** davlat-xususiy sheriklik obyektlari sifatida tan olinadi. davlat-xususiy sheriklik loyihasini **davlat yoki xususiy tashabbuskor** tomonidan ilgari surish mumkin. Kiberxavfsizlik sohasidagi loyiha tashabbuslari ushbu qonun asosida **xususiy taklif** ko‘rinishida rasmiylashtirilsa bo‘ladi.

Tahliliy mulohazalar va aniqlangan muammolar

Asosiy yo‘nalish	**Holat**	**Muammo**
Normativ asos	DXSh qonuni universal, lekin kiberxavfsizlikda qo‘llanilmayapti	Soha bo‘yicha maxsus DXSh normalari yo‘q
Ishtirokchilar	Kiberxavfsizlikda davlat subyektlari ko‘p, xususiy subyektlar cheklangan	Rollarning chegaralari belgilab berilmagan
Mexanizm	DXSh qonuni tashabbuslarni nazarda tutadi	“Kiberxavfsizlik to‘g‘risida”gi Qonunda DXShga alohida modul mavjud emas

Qonunga ko‘ra, davlat-xususiy sheriklik – bu davlat va xususiy sherik o‘rtasida muayyan muddatga tuziladigan, infratuzilmani moliyalashtirish, qurish, qayta qurish, boshqarish yoki texnik xizmat ko‘rsatish bo‘yicha sheriklikdir[3]. Qonun ijrosini ta’minlash uchun Iqtisodiyot va moliya vazirligi huzuridagi davlat-xususiy sheriklikni rivojlantirish agentligi mas’ul etib belgilanadi.

O‘zbekiston Respublikasi “Davlat-xususiy sheriklik to‘g‘risida”gi Qonunining 3-moddasiga ko‘ra, davlat-xususiy sheriklik “davlat organlari va xususiy hamkorlar o‘rtasida ustuvor sohalarda loyihalarni amalga oshirish uchun ma’lum muddatga tuziladigan o‘zaro manfaatli hamkorlik”dir[4]. Qonun davlat-xususiy sheriklikni turli sohalarda qo‘llashni ko‘zda tutadi, biroq unda kiberxavfsizlik sohasi bevosita tilga olinmagan. Bu esa qonunchilik doirasida ushbu sohani qamrab olish zarurligini ko‘rsatadi. Shunga qaramay, qonun umuman davlat-xususiy sheriklik mexanizmlarini belgilab beradi, ammo kiberxavfsizlik singari sektorlar uchun maxsus tartibni ko‘zda tutmaydi. Bu esa aynan kiberxavfsizlik sohasida davlat-xususiy sheriklik loyihalarini amalga oshirishda huquqiy noaniqliklarga olib kelmoqda.

O‘zbekiston kiberxavfsizligini ta’minlashda ishtirok etuvchi asosiy davlat tuzilmalari quyidagilardan iborat: O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi[5], Davlat xavfsizlik xizmati, “Cyber Security Center” kiberxavfsizlik markazi[6], “O‘zbekiston telekommunikatsiya tarmoqlarini

[3] N.I.Tuxtasinov. “O‘zbekistonda davlat-xususiy sheriklik tizimi va kapital bozoridagi asosiy tendensiyalar”.O‘quv qo‘llanma /Tuxtasinov Nurillo Islomjon o‘g‘li – T.:TDYU nashriyoti, 2024.13-14-bet https://library-tsul.uz/ozbekistonda-davlat-xususiy-sheriklik-tizimi-va-kapitalbozoridagiasosiytenden siyalar-tuxtasinov-n-2024/

[4] O‘zbekiston Respublikasi “Davlat-xususiy sheriklik to‘g‘risida”gi Qonuni, 10.05.2019 yildagi O‘RQ-537-son https://lex.uz/ru/docs/-4329270

[5] O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi https://gov.uz/oz/digital

[6] “Cyber Security Center” kiberxavfsizlik markazi https://csec.uz/uz/

boshqarish respublika markazi" DUK va boshqa vakolatli tashkilotlar. O‘zbekiston Respublikasi **Davlat xavfsizlik xizmati** kiberxavfsizlik sohasidagi **vakolatli davlat organdir**. Ushbu organlar normativ huquqiy asoslarni ishlab chiqadi, nazorat, sertifikatlash va monitoring funksiyalarini bajaradi. Biroq, xususiy sektor bilan tizimli va institutsional hamkorlik hali yetarlicha shakllanmagan. Telekommunikatsiya, bank va axborot texnologiyalari sohasidagi kompaniyalar kiberxavfsizlik loyihalarida ishtirok etish salohiyatiga ega. Ammo ularning ishtirokini cheklayotgan asosiy omillar, ya'ni huquqiy mexanizmlarning aniqligi yetarli emasligi, investitsiyalarni qaytarish kafolatlarining yo‘qligi va tender jarayonlarining shaffof emasligidir.

Bizga ma'lumki, kiberxavfsizlik sohasida davlat-xususiy sheriklikni ta'minlash bo‘yicha qonunchilikda ziddiyatlar va bo‘shliqlar mavjud. davlat-xususiy sheriklik va kiberxavfsizlikni integratsiyalashgan holda tartibga solmaslik davlat-xususiy sheriklik va kiberxavfsizlik bo‘yicha alohida qonunlar mavjud bo‘lsa-da, ular o‘zaro bog‘lanmagan. davlat-xususiy sheriklik to‘g‘risidagi qonunda kiberxavfsizlik sohasi alohida yo‘nalish sifatida ko‘zda tutilmagan. Bu esa xususiy sektorni loyihalarda ishtirok etishga undaydigan aniq huquqiy kafolatlarning yo‘qligiga olib keladi. Xalqaro amaliyotda xususiy sheriklarga soliq imtiyozlari, imtiyozli kreditlar, davlat mulkidan foydalanish huquqi taqdim etiladi. O‘zbekistonda bunday imtiyozlar faqat infratuzilmaviy loyihalar uchun nazarda tutilgan, masalan, O‘zbekiston Respublikasi Prezidentining 2018-yil 20-dekabrda qabul qilingan "O‘zbekiston Respublikasining 2019-yilga mo‘ljallangan Investitsiya dasturini amalga oshirish chora-tadbirlari to‘g‘risida"gi PQ-4067-sonli qarorida, biroq

kiberxavfsizlik sohasida mavjud emas[7]. Xavflarni taqsimlash mexanizmlarining yetishmasligi, ya'ni davlat-xususiy sheriklik loyihalarida risklarning adolatli taqsimlanishi muhim. Kiberxavfsizlikda xavflar (ma'lumotlarning sizib chiqishi, xakerlik hujumlari, texnik nosozliklar) juda yuqori bo'lib, ularning moliyaviy oqibatlari sezilarli. Afsuski, hozirda O'zbekiston qonunchiligida bu xavflarni sug'urtalash yoki zararlarni kompensatsiya qilish bo'yicha alohida mexanizmlar mavjud emas.

Xalqaro tajribaga to'xtaladigan bo'lsak, Janubiy Koreyada Kiberxavfsizlik bo'yicha davlat-xususiy hamkorlik markazi faoliyat yuritadi. Davlat va IT-kompaniyalar o'rtasida real vaqtda axborot almashinuvi, xavfsizlik protokollari muvofiqlashtirilgan[8]. Buyuk Britaniyada Milliy Kiberxavfsizlik Markazi (NCSC) "Cyber Essentials" dasturi orqali xususiy kompaniyalarni davlat siyosatini shakllantirishga jalb qilgan. Bu mexanizm orqali bizneslar sertifikatlangan himoya standartlariga amal qiladi[9]. Qozog'iston "Kiberqalqon" milliy konsepsiyasini qabul qilgan bo'lib, u davlat-xususiy sheriklik mexanizmlarini, jumladan, subsidiyalar, kibermarkazlar va innovatsion xablarni o'z ichiga oladi[10]. Ushbu tajribalar O'zbekistonda ham kiberxavfsizlik sohasida real vaqtda axborot almashinuvi, davlat va biznes o'rtasidagi ishonchli hamkorlikni yo'lga qo'yish zarurligini ko'rsatadi. Bundan tashqari, sertifikatlash, subsidiyalar va innovatsion markazlar orqali davlat-

[7] O'zbekiston Respublikasi Prezidentining 2018-yil 20-dekabrda qabul qilingan "O'zbekiston Respublikasining 2019-yilga mo'ljallangan Investitsiya dasturini amalga oshirish chora-tadbirlari to'g'risida"gi PQ-4067-sonli qarori https://lex.uz/ru/docs/-4117465

[8] Korea Internet & Security Agency (KISA). (2022). Public-Private Cooperation in Cybersecurity. https://www.kisa.or.kr/eng/main.jsp

[9] National Cyber Security Centre (UK). (2023). Cyber Essentials Scheme. https://www.ncsc.gov.uk/cyberessentials

[10] Qozog'iston Respublikasi Raqamli rivojlanish vazirligi. (2021). Kiberqalqon konsepsiyasi. https://digit.gov.kz/ru/articles/kiberwyt

xususiy sheriklikni rag‘batlantirish kiber tahdidlarga qarshi barqaror tizim yaratishga xizmat qiladi.

Yuqoridagi fikrlarni umumlashtirib quyidagilarni taklif qilishimiz mumkin.

Birinchidan, kiberxavfsizlikda davlat-xususiy sheriklikni rivojlantirishga yo‘naltirilgan strategik va normativ hujjatlarni qabul qilish. “Kiberxavfsizlik sohasida davlat-xususiy sheriklikning milliy konsepsiyasi”ni ishlab chiqish va unda: sheriklikning asosiy yo‘nalishlari; tomonlarning huquq va majburiyatlari; xususiy sheriklarni tanlash mezonlari; axborot almashinuv tartibi belgilanishi lozim.

Ikkinchidan, “Davlat-xususiy sheriklik to‘g‘risida”gi qonunga maxsus kiberxavfsizlik bobini kiritish. Unda quyidagilar ko‘zda tutilishi kerak: xavfsizlik standartlari; litsenziyalar va sertifikatlar orqali xususiy sheriklar uchun majburiy talablar; axborot maxfiyligini ta’minlash normalari.

Xulosa qiladigan bo‘lsak, O‘zbekistonda davlat-xususiy sheriklik va kiberxavfsizlik sohalaridagi huquqiy tartibga solish rivojlanish bosqichida. Mazkur ikki yo‘nalish o‘rtasida huquqiy bog‘liqlikning yo‘qligi xususiy sektor ishtirokini susaytiradi. Xalqaro tajribani joriy qilish, xususiy investitsiyalarni rag‘batlantirish va aniq-huquqiy mexanizmlarni ishlab chiqish raqamli muhitning xavfsizligini ta’minlashda hal qiluvchi omil bo‘ladi. Bugungi kunda O‘zbekistonning davlat-xususiy sheriklik va kiberxavfsizlik sohasidagi qonunchiligi mustahkam va potensialga boy, biroq ular o‘zaro integratsiyalashmagan. Kiberxavfsizlik sohasini innovatsion rivojlantirish uchun davlat-xususiy sheriklik mexanizmlarini maxsus tartibga solish, xususiy sektorni faolroq jalb qilish, loyihaviy yondashuvni qo‘llash talab etiladi.

Xususiy sektor sheriklari axborot almashinuvi va tahdidlarni tahlil qilishda muhim hissa qo‘sha oladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

Normativ-huquqiy hujjatlar

1. O‘zbekiston Respublikasi Konstitutsiyasi, 01.05.2023.
2. O‘zbekiston Respublikasi “Kiberxavfsizlik to‘g‘risida”gi Qonuni, 15.04.2022 yildagi O‘RQ-764-son.
3. O‘zbekiston Respublikasi “Davlat-xususiy sheriklik to‘g‘risida”gi Qonuni, 10.05.2019 yildagi O‘RQ-537-son.
4. “Raqamli O‘zbekiston – 2030” STRATEGIYASI, O‘zbekiston Respublikasi Prezidentining Farmoni, 05.10.2020 yildagi PF-6079-son.
5. “2022 — 2026-yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risida” O‘zbekiston Respublikasi Prezidentining Farmoni, 28.01.2022 yildagi PF-60-son.
6. “O‘zbekiston Respublikasi muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlash tartibi to‘g‘risidagi” NIZOM, O‘zbekiston Respublikasi Prezidentining qarori, 31.05.2023 yildagi PQ-167-son.
7. “O‘zbekiston Respublikasi kiberxavfsizlik va muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta’minlash darajasini baholash tartibi to‘g‘risidagi” NIZOM, O‘zbekiston Respublikasi davlat xavfsizlik xizmati raisining buyrug‘i, 22.09.2023 yilda ro‘yxatdan o‘tgan, ro‘yxat raqami 3458

Kitob va turkum nashrlari:

1. “Роль государственно-частного партнерства в формировании устойчивой политики кибербезопасности Японии” Низамова М. А. Казанский (Приволжский) федеральный университет.

2. N. I. Tuxtasinov. “O‘zbekistonda davlat-xususiy sheriklik tizimi va kapital bozoridagi asosiy tendensiyalar”.O‘quv qo‘llanma / Tuxtasinov Nurillo Islomjon o‘g‘li – T.:TDYU nashriyoti, 2024 – 120 bet

Internet saytlari

1. https://www.lex.uz/uz/
2. https://www.norma.uz/
3. https://library-tsul.uz/
4. InfraGard – https://www.infragard.org
5. CyberNet EU Project – https://cybernet.eu
6. OAS Cybersecurity Program – https://www.oas.org/en/sms/cicte/cybersecurity.asp
7. National center of Incident readiness and Strategy for Cybersecurity. https://www.nisc.go.jp/eng/index.html