# KIBERXAVFSIZLIK SOHASIDA DAVLAT-XUSUSIY SHERIKCHILIKNI RIVOJLANTIRISHNING INNOVATSION MEXANIZMLARI: XORIJIY TAJRIBA VA O‘ZBEKISTON QONUNCHILIGI ASOSIDA TAHLIL

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

**Annotatsiya.** Mazkur maqolada kiberxavfsizlikni ta’minlashda davlat-xususiy sherikchilik (DXSh) mexanizmlarining innovatsion shakllari tahlil qilingan. AQSH, Estoniya, Singapur, Isroil kabi ilg‘or davlatlarning tajribalari asosida O‘zbekiston uchun mos model tavsiya etilgan. Shuningdek, O‘zbekiston qonunchiligidagi mavjud muammolar va ularni bartaraf etish yo‘llari ko‘rib chiqilgan.

**Kalit so‘zlar:** kiberxavfsizlik, davlat-xususiy sherikchilik(DXSh), innovatsion mexanizmlar, O‘zbekiston qonunchiligi, xalqaro tajriba, axborot xavfsizligi

**Аннотация.** В данной статье проанализированы инновационные формы механизмов государственно-частного партнёрства (ГЧП) в обеспечении кибербезопасности. На основе опыта передовых стран, таких как США, Эстония, Сингапур и Израиль, предложена адаптированная модель для Узбекистана. Также рассмотрены существующие проблемы в законодательстве Узбекистана и пути их устранения.

**Ключевые слова:** кибербезопасность, государственно-частное партнёрство, инновационные механизмы, законодательство Узбекистана, международный опыт, ГЧП, информационная безопасность

**Annotation.** This article analyzes innovative forms of public-private partnership (PPP) mechanisms in ensuring cybersecurity. Based on the experiences of leading countries such as the USA, Estonia, Singapore, and Israel, a suitable model for Uzbekistan is proposed. The article also examines existing issues in Uzbekistan's legislation and suggests ways to address them.

**Keywords:** cybersecurity, public-private partnership, innovative mechanisms, Uzbekistan legislation, international experience, PPP, information security

**Kirish.** Bugungi globallashuv va raqamli texnologiyalar rivojlanayotgan bir davrda, kiberxavfsizlik masalasi davlatlar uchun strategik xavfsizlik muammosiga aylangan. Axborot texnologiyalarining tezkor rivojlanishi nafaqat yangi imkoniyatlarni yaratmoqda, balki kiberxavflarni ham kuchaytirmoqda. Hozirgi kunda davlat organlari, moliyaviy institutlar, sog‘liqni saqlash tizimi, energetika va boshqa muhim infratuzilmalar tobora ko‘proq raqamlashtirilmoqda, bu esa ularni kiberhujumlarga nisbatan zaif holatga keltirmoqda. Kiberxavfsizlik infratuzilmasini yaratish va mustahkamlash esa katta mablag‘ va yuqori malakali kadrlar talab qiladi. Aynan shu jihatdan davlat-xususiy sherikchilik (DXSh) modeli zamonaviy muammolarga zamonaviy yechim sifatida qaralmoqda.

DXSh – bu davlat va xususiy sektorning resurslarini, bilim va tajribasini birlashtirib, ijtimoiy va iqtisodiy loyihalarni amalga oshirishga xizmat qiluvchi mexanizmdir. Kiberxavfsizlik sohasida esa bu sheriklik davlatning regulyatorlik roli va xususiy sektorning innovatsion yechimlar ishlab chiqishdagi moslashuvchanligini birlashtiradi. Ushbu maqolada kiberxavfsizlik sohasida DXSh modelining mohiyati, xorijiy va mahalliy tajribalari, qonunchilik asoslari, mavjud muammolar va istiqbolli takliflar yoritiladi.

Kiberxavfsizlik sohasi tobora kengayib borar ekan, bu boradagi global tahdidlar ham o‘zgarib bormoqda. Hozirgi paytda APT (Advanced Persistent Threats), ransomware, phishing, DDoS hujumlar kabi murakkab va uzoq muddatli kiberhujumlar ko‘plab davlatlar, kompaniyalar va fuqarolarning axborot xavfsizligiga tahdid solmoqda. Xalqaro miqyosda tashkil etilayotgan hukumatlararo axborot xavfsizligi tashkilotlari, masalan ITU (International Telecommunication Union) va ENISA (European Union Agency for Cybersecurity) orqali davlatlar o‘zaro tajriba almashmoqda, biroq milliy darajada ushbu tahdidlarni bartaraf etish uchun mahalliy resurslar va imkoniyatlardan samarali foydalanish zarur.

Shu nuqtai nazardan, O‘zbekiston kabi rivojlanayotgan davlatlar uchun davlat va xususiy sektorni o‘zaro integratsiya qilish orqali milliy xavfsizlikni mustahkamlash ustuvor vazifalardan biri sanaladi. Ayniqsa, xalqaro moliyaviy tashkilotlar tomonidan ham DXSh mexanizmlariga katta e’tibor qaratilmoqda. Jahon banki, Yevropa tiklanish va taraqqiyot banki (EBRD) kabi moliyaviy institutlar tomonidan DXSh loyihalariga mablag‘ ajratish yo‘lga qo‘yilgan. Demak, O‘zbekistonning raqamli transformatsiya sari yo‘nalgan strategik siyosatida DXSh asosida kiberxavfsizlikni rivojlantirish innovatsion yondashuv sifatida qaralmoqda.

**Metodologiya**. Tadqiqot metodologiyasi sifatida huquqiy hujjatlarni tahlil qilish, komparativ (qiyosiy) tahlil, kontent-analiz va tizimli yondashuvlar qo‘llanildi. Tahlil qilish jarayonida kontent-analiz orqali O‘zbekiston Milliy qonunchilik bazasi (lex.uz) va xorijiy davlatlarning kiberxavfsizlik bo‘yicha strategiyalari o‘rganildi. Qonunchilik hujjatlari matnida DXShga oid qoidalar, ularning sohalar bo‘yicha taqsimoti va amaliyotdagi ko‘rinishlari sistematik tarzda tahlil qilindi. Shuningdek, AQSH, Estoniya, Buyuk Britaniya va Singapur kabi ilg‘or mamlakatlar tajribasi tahlil qilindi. Ushbu davlatlarda kiberxavfsizlikni ta’minlashda DXSh modeli qanday qo‘llanilayotgani, qanday qonunchilik asoslari mavjudligi va qanday institutlar faoliyat yuritayotgani o‘rganildi. Ma’lumotlar to‘plashda ochiq manbalar (hukumat saytlar, xalqaro tashkilotlar hisobotlari, tahliliy markazlar ma’lumotlari) va ilmiy maqolalardan foydalanildi. Olingan ma’lumotlar asosida mavjud muammolar, imkoniyatlar va istiqbollar aniqlanib, tahliliy xulosalar chiqarildi. Tadqiqotda, shuningdek, SWOT tahlil yondashuvi asosida O‘zbekistonda kiberxavfsizlik sohasidagi DXSh imkoniyatlari va tahdidlari baholandi. Kuchli tomonlar sifatida hukumatning raqamli transformatsiyaga qaratilgan siyosati, AKT sohasidagi kadrlar salohiyati va xalqaro hamkorlik mavjudligi belgilandi. Zaif tomonlar esa – moliyaviy resurslarning cheklanganligi, qonunchilikdagi noaniqliklar va institutsional muvofiqlashtirish muammolaridan iborat.

**Natijalar.** Tahlil natijalari quyidagi asosiy yo‘nalishlar bo‘yicha aniqlandi:

Xalqaro tajriba: AQSHda Homeland Security va NIST (National Institute of Standards and Technology) kabi institutlar DXSh asosida xususiy kompaniyalar bilan hamkorlikda milliy kiberxavfsizlik strategiyalarini ishlab chiqadi. Estoniya, dunyoda birinchi raqamli davlat sifatida, “e-Estonia” dasturi orqali butun davlat boshqaruvini raqamlashtirishga erishgan va kiberxavfsizlikda xususiy sektor bilan yaqin hamkorlikda ishlaydi. Buyuk Britaniyada National Cyber Security Centre (NCSC) xususiy kompaniyalar bilan birgalikda tahdidlar monitoringi, xavfsizlik bo‘yicha treninglar va maslahat xizmatlari ko‘rsatadi.

O‘zbekiston tajribasiga to‘xtaladigan bo‘lsak, 2019-yilda qabul qilingan DXSh to‘g‘risidagi Qonun umumiy asoslarni belgilaydi, biroq kiberxavfsizlik sohasiga alohida e’tibor qaratilmagan. UZCERT (Computer Emergency Response Team) kiberxavfga qarshi markaz sifatida faoliyat yuritsa-da, uning xususiy sektor bilan o‘zaro aloqalari cheklangan. Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi tomonidan “Raqamli O‘zbekiston – 2030” strategiyasi doirasida ba’zi DXSh loyihalari amalga oshirilmoqda.

Muammolar: Birinchidan, normativ-huquqiy bo‘shliqlar, ya’ni DXSh modelini kiberxavfsizlik sohasida qo‘llash bo‘yicha aniq reglamentlar yo‘q. Ikkinchidan, resurs cheklanganligi, ya’ni davlat budjetidan ajratiladigan mablag‘ yetarli emas. Uchinchidan, ishonch muammosi, ya’ni davlat va xususiy sektor o‘rtasida axborot almashinuvi, maxfiylik va ishonch muammolari mavjud.

Shu bilan birga, tadqiqot shuni ko‘rsatadiki, agar DXSh kiberxavfsizlik yo‘nalishida to‘g‘ri tashkil etilsa, u innovatsion rivojlanish, tezkor yechimlar ishlab chiqish va milliy xavfsizlikni ta’minlashda muhim rol o‘ynashi mumkin.

Davlat-xususiy sherikchilik mexanizmlarining afzalliklariga to‘xtaladigan bo‘lsak, xususiy sektor ilg‘or texnologiyalarni tezda joriy qila oladi hamda nnovatsion yechimlarning davlat xizmatlarida tez joriy qilinishiga zamin yaratadi. Jahon bankining “Public-Private Partnerships in Cybersecurity” nomli hisobotida DXShni “inclusive governance model” deb atab, bunda davlat va xususiy sektor birgalikda

milliy kiberxavfsizlik strategiyasini ishlab chiqish va amalga oshirishda ishtirok etishi kerakligi ta’kidlanadi.

**Xalqaro tajriba tahlili.** AQSH tajribasi: AQSHda kiberxavfsizlik sohasida davlat-xususiy sherikchilik (DXSh) keng ko‘lamda amalga oshirilmoqda. Masalan, CISA (Cybersecurity and Infrastructure Security Agency) tomonidan “Joint Cyber Defense Collaborative (JCDC)” tashabbusi asosida yirik xususiy kompaniyalar, jumladan Amazon, Microsoft, Google va boshqalar bilan hamkorlik qilinadi. Bu platforma orqali kiberhujumlar bo‘yicha real vaqtda axborot almashinuvi amalga oshiriladi. AQSHning NIST (National Institute of Standards and Technology) agentligi tomonidan ishlab chiqilgan kiberxavfsizlik standartlari xususiy sektor uchun tavsiya etiladi, lekin ko‘plab kompaniyalar bu standartlarga amal qiladi.

Estoniya tajribasi: Estoniya Yevropadagi eng raqamlashtirilgan davlatlardan biri bo‘lib, bu yerda “e-Estonia” modeli doirasida kiberxavfsizlik infratuzilmasi davlat-xususiy sherikchilik asosida shakllantirilgan. Xususiy texnologik kompaniyalar, masalan, Guardtime, davlat xizmatlarining ishonchli ishlashini ta’minlashda muhim rol o‘ynaydi. Estoniya kiberxavfsizlik bo‘yicha maxsus qonunchilik asosida davlat-xususiy hamkorlikning shakllari va mas’uliyat doiralari aniq belgilanadi.

Singapur tajribasi: Singapurda Cyber Security Agency (CSA) tomonidan “Safer Cyberspace Masterplan” qabul qilingan bo‘lib, unda DXSh modeli asosida “Threat Intelligence Platform”, “Cybersecurity Labelling Scheme” kabi mexanizmlar joriy qilingan. Singapur hukumati xususiy sektorga subsidiya va grantlar ajratib, yangi texnologiyalarni sinovdan o‘tkazish uchun maxsus muhit yaratgan.

Isroil tajribasi: Isroil dunyoda kiberxavfsizlik startaplari eng ko‘p joylashgan mamlakatlardan biri bo‘lib, bu yerda davlat harbiy sohada to‘plangan tajribani xususiy sektor bilan baham ko‘radi. Isroilning Beer-Sheva shahridagi “CyberSpark” hududi DXSh asosida tashkil etilgan bo‘lib, u yerda universitetlar, mudofaa sanoati va texnologik startaplar bir joyda faoliyat yuritadi. Isroil hukumati DXShni kiberxavfsizlikda innovatsiyalar uchun kalit omil sifatida ko‘radi.

Bu davlatlarning har biri o‘zining institutsional modeliga ega bo‘lsa-da, ularning umumiy jihati – davlat va xususiy sektor o‘rtasida ishonchli hamkorlik, normativ bazaning aniq belgilangani va strategik yondashuv mavjudligi.

**Muhokama.** Yuqoridagi natijalar asosida bir qator muhim xulosalar chiqarish mumkin. Birinchidan, rivojlangan davlatlar tajribasi shuni ko‘rsatadiki, kiberxavfsizlik masalasi davlat va xususiy sektor o‘rtasidagi faol hamkorliksiz samarali hal etilmaydi. DXSh orqali birgalikda kiberxavfsizlik standartlarini ishlab chiqish, texnologiyalarni sinovdan o‘tkazish, xavfsizlik protokollarini ishlab chiqish va joriy etish, treninglar o‘tkazish kabi muhim vazifalar bajariladi. Ikkinchidan, O‘zbekistonda kiberxavfsizlik va DXSh bo‘yicha alohida aloqador normativ hujjatlarning mavjud emasligi hamda xususiy sektorga ishonch pastligi bu modelni keng qo‘llashga to‘sqinlik qilmoqda. Ayniqsa, xususiy kompaniyalarning hukumat bilan axborot almashishdagi cheklovlar va xavotirlari, ularning ishtirokini cheklaydi. Uchinchidan, yurtimizda yuqori malakali kiberxavfsizlik mutaxassislariga ehtiyoj katta. Bu sohada universitetlar, ilmiy-tadqiqot institutlari va xususiy IT-kompaniyalar o‘rtasida strategik sheriklik zarur. DXSh modeli aynan shu jihatdan innovatsion bilim va texnologiyalar almashinuvini rag‘batlantiradi. To‘rtinchidan, raqamli infratuzilmani himoya qilishda faqat texnik vositalar emas, balki institutsional mexanizmlar, qonunchilik, inson kapitali va ijtimoiy ishonch ham muhim rol o‘ynaydi. DXSh bu komponentlarning o‘zaro uyg‘unligini ta’minlovchi platforma bo‘lib xizmat qilishi mumkin. Shu sababli, DXSh mexanizmlarini kiberxavfsizlik sohasiga moslashtirish, qonunchilikni takomillashtirish, ishonchli axborot almashinuv tizimlarini yaratish hamda xususiy sektorni rag‘batlantirish – bu boradagi asosiy vazifalardandir.

Kiberxavfsizlik bo‘yicha samarali DXShni tashkil etish uchun shaffoflik va hisobdorlik tamoyillari ustuvor bo‘lishi kerak. Maxfiy ma’lumotlar bilan ishlashdagi ishonchni ta’minlash uchun normativ hujjatlarda shartnoma asoslari, ma’lumotlarni himoya qilish bo‘yicha standartlar, va favqulodda vaziyatlarda javobgarlik masalalari aniq belgilanishi kerak. Shuningdek, DXSh subyektlarining huquq va majburiyatlari, moliyaviy risklarni taqsimlash mexanizmlari, loyiha monitoringi va baholash

indikatorlari belgilanmasa, bu mexanizm samarali ishlamaydi. Shu bois xorij tajribasidagi kabi o‘ziga xos “regulatory sandbox”lar tashkil etish va kiberxavfsizlikka doir texnologiyalarni sinovdan o‘tkazish mumkin bo‘lgan platformalarni yo‘lga qo‘yish lozim. Muhokama davomida, shuningdek, davlat-xususiy sherikchilik loyihalarida fuqarolik jamiyati ishtirokini ham ta’minlash masalasi muhim ekani ta’kidlanadi. Bu ochiqlik va jamoatchilik nazoratini kuchaytiradi.

O‘zbekistonda DXSh amaliyotlari: O‘zbekistonda davlat-xususiy sherikchilik sohasida umumiy huquqiy asos 2019-yilda qabul qilingan “Davlat-xususiy sheriklik to‘g‘risida”gi Qonun bilan shakllantirilgan. Kiberxavfsizlik sohasiga bu qonun to‘g‘ridan-to‘g‘ri taalluqli bo‘lmasa-da, unda AKT yo‘nalishidagi loyihalar uchun imkoniyatlar mavjud. Misol sifatida, “Xavfsiz shahar” loyihasini ko‘rsatish mumkin. Bu loyihada videokuzatuv tizimlari, transport monitoring tizimlari va sun’iy intellekt asosida ishlovchi xavfsizlik platformalari joriy etilgan. Loyihada xususiy texnologik kompaniyalar infratuzilmani yetkazib bergan va texnik xizmat ko‘rsatmoqda. Bu DXShning noformal ko‘rinishidir. Shuningdek, 2022-yildan boshlab Raqamli texnologiyalar vazirligi huzurida “Cybersecurity Center” tashkil qilindi va u yerda ham xususiy sektor bilan hamkorlikda treninglar, sertifikatlash va axborot almashinuvi yo‘lga qo‘yilgan. Bu DXSh uchun muhim poydevor sanaladi.

Qonunchilik tahlili – O‘zbekiston va xorij: O‘zbekistonda kiberxavfsizlik bilan bog‘liq huquqiy asoslar quyidagilar: “Elektron hukumat to‘g‘risida”gi Qonun; “Axborotlashtirish to‘g‘risida”gi Qonun; “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi Qonun; “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun; “Kiberxavfsizlik to‘g‘risida”gi Qonun (15.04.2022 yildagi O‘RQ-764-son).

Xorijiy huquqiy modellar bilan taqqoslanganda, O‘zbekiston qonunchiligi hali yangi bosqichda ekanini ko‘rish mumkin. Masalan: AQSHda NIST tomonidan ishlab chiqilgan “Cybersecurity Framework” mavjud bo‘lib, unda xususiy sektor ishtiroki rasmiylashtirilgan. Yevropa Ittifoqida GDPR doirasida xususiy kompaniyalarning axborot himoyasi bo‘yicha aniq mas’uliyatlari va javobgarlik doiralari belgilangan. Singapurda esa “Cybersecurity Act” asosida tan olingan “critical information

infrastructure” obyektlari ro‘yxati yuritiladi va ularga nisbatan qat’iy xavfsizlik talablari qo‘yiladi. O‘zbekistonda esa bu boradagi segmentatsiya hali zaif, ammo DXSh doirasida shunday infratuzilmalarni aniqlash va sertifikatlash tizimi joriy qilinishi kutilmoqda.

**Xulosa.** Yuqoridagi tahlillarga asoslanib, quyidagi xulosalarga kelish mumkin, kiberxavfsizlik sohasida DXSh modeli muhim innovatsion vosita bo‘lib, davlat va xususiy sektor resurslarini birlashtirishga xizmat qiladi. Rivojlangan davlatlar tajribasi shuni ko‘rsatadiki, DXSh nafaqat moliyaviy, balki bilim, tajriba va texnologik hamkorlik imkoniyatlarini ham yaratadi. O‘zbekistonda mavjud qonunchilik bazasi DXShni umumiy asosda belgilagan bo‘lsa-da, kiberxavfsizlik sohasida uni amalda qo‘llash uchun maxsus normativ hujjatlar ishlab chiqilishi zarur. Xususiy sektorni jalb qilishda ishonch muhitini yaratish, ma’lumotlar maxfiyligi va xavfsizligini ta’minlash bo‘yicha kafolatlar zarur. Innovatsion sheriklik platformalarini yaratish, grantlar va soliq imtiyozlari orqali xususiy kompaniyalarni rag‘batlantirish – istiqbolli yo‘nalishlardandir.

Shu asosda quyidagi takliflar ilgari surishimiz mumkin:

Birinchisi, kiberxavfsizlik sohasida DXSh uchun maxsus qonunchilik bazasini yaratish;

Ikkinchisi, xususiy sektor vakillari bilan muntazam strategik uchrashuvlar va hamkorlik mexanizmlarini ishlab chiqish;

Uchinchisi, ilmiy-tadqiqot institutlari, universitetlar va IT-kompaniyalar o‘rtasida hamkorlik platformasini yaratish;

To‘rtinchisi, davlat-xususiy sheriklik asosida raqamli suverenitet va ma’lumotlar xavfsizligi bo‘yicha kodeks ishlab chiqish;

Beshinchisi, Raqamli tahdidlarni monitoring qilish uchun markazlashtirilgan “Cyber Threat Intelligence Platform” yaratish.

Bu takliflar amalga oshirilsa, O‘zbekistonning kiberxavfsizlik infratuzilmasi yanada barqaror, zamonaviy va innovatsion asosda rivojlanadi.

Yakuniy xulosalardan biri sifatida, DXSh asosidagi yondashuv nafaqat texnologik yechimlar, balki strategik boshqaruv, moliyaviy barqarorlik va milliy xavfsizlikni ta’minlashga xizmat qiladi. Kelgusida quyidagi tavsiyalarni amalga oshirish muhim hisoblanadi, ya`ni DXSh asosidagi kiberxavfsizlik infratuzilmasini moliyaviy va institutsional jihatdan qo‘llab-quvvatlash uchun milliy fond tashkil etish, O‘zbekiston Respublikasi Prezidenti huzuridagi Strategik islohotlar agentligi ko‘magida maxsus “Cyber PPP Taskforce” tashkil etish, hamda Xalqaro donor tashkilotlar bilan sheriklik asosida grant asosidagi startap loyihalariga kiberxavfsizlik inkubatorlarini yo‘lga qo‘yish. Xulosa qilib aytganda, kiberxavfsizlikda DXSh modeli O‘zbekiston uchun nafaqat zarurat, balki innovatsion imkoniyatdir.

Bundan tashqari, O‘zbekistonda kiberxavfsizlik bo‘yicha davlat-xususiy sherikchilikni institutsional darajada rivojlantirish uchun alohida DXSh agentligi tashkil etish zarur. Ushbu agentlik davlat va xususiy sektor o‘rtasida vositachilikni amalga oshiradi. Xavfsizlik infratuzilmasining muhim qismlarini – internet provayderlar, moliyaviy texnologiyalar, raqamli to‘lov tizimlari – “tan olingan strategik infratuzilma” deb belgilab, ularga nisbatan DXSh asosida sertifikatlash tizimi joriy etish kerak. Xorijiy tajribalarga asoslanib, “sandbox” tizimini joriy etish orqali innovatsion texnologiyalarni real muhitda sinovdan o‘tkazishga imkon beruvchi platforma yaratish lozim. Raqamli tahdidlarni monitoring qilish uchun markazlashtirilgan “Cyber Threat Intelligence Platform” yaratish zarur. Bu platformada xususiy sektor vakillari ham axborot almashinuvida ishtirok etadi. Davlat xaridlari doirasida kiberxavfsizlik yechimlarini ishlab chiquvchi startaplar uchun imtiyozli yo‘nalishlar belgilanishi mumkin.

O‘zbekiston sharoitida kiberxavfsizlikni kuchaytirish va xalqaro standartlarga mos infratuzilma yaratishda davlat-xususiy sherikchilik eng maqbul va innovatsion yo‘nalishdir. DXSh modeli orqali davlat resurslaridan oqilona foydalanish, xususiy sektordan ilg‘or texnologiyalarni jalb etish, hamda umumiy xavfsizlik madaniyatini shakllantirish imkoniyati yaratiladi.

## FOYDALANILGAN ADABIYOTLAR RO‘YXATI

### O‘zbekiston Respublikasi qonunlari va normativ-huquqiy hujjatlari:

1. “Davlat-xususiy sheriklik to‘g‘risida”gi Qonun .
2. “Elektron hukumat to‘g‘risida”gi Qonun.
3. “Axborotlashtirish to‘g‘risida”gi Qonun.
4. “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi Qonun.
5. “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun.
6. “Kiberxavfsizlik to‘g‘risida”gi Qonun.
7. “Raqamli O‘zbekiston – 2030” strategiyasi.

### Xorijiy davlatlarning kiberxavfsizlik strategiyalari va qonunchiligi hamda Xalqaro tashkilotlar hisobotlari va materiallari:

8. Jahon bankining “Public-Private Partnerships in Cybersecurity” hisoboti.
9. ITU (International Telecommunication Union) materiallari.
10. ENISA (European Union Agency for Cybersecurity) materiallari.
11. EBRD (Yevropa tiklanish va taraqqiyot banki) hisobotlari.
12. AQSHning Milliy kiberxavfsizlik strategiyasi.
13. NIST (National Institute of Standards and Technology) Cybersecurity Framework.
14. Estoniyaning “e-Estonia” dasturi va kiberxavfsizlik bo‘yicha qonunchiligi.
15. Buyuk Britaniyaning National Cyber Security Centre (NCSC) materiallari.
16. Singapurning “Safer Cyberspace Masterplan” va Cybersecurity Act.
17. Isroilning kiberxavfsizlik bo‘yicha milliy strategiyasi.
18. Yevropa Ittifoqining GDPR (General Data Protection Regulation).