KIBERXAVFSIZLIK SOHASIDA DAVLAT-XUSUSIY SHERIKCHILIKNI RIVOJLANTIRISHNING HUQUQIY MUAMMOLARI VA ULARNI BARTARAF ETISH YO‘LLARI

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

Annotatsiya. Mazkur maqolada O‘zbekiston Respublikasida kiberxavfsizlik sohasida davlat-xususiy sherikchiligining (DXSH) samarali rivojlanishiga to‘sqinlik qilayotgan huquqiy muammolar tahlil qilinadi hamda xorijiy davlatlar (AQSh, Buyuk Britaniya, Singapur) tajribasi bilan qiyosiy-huquqiy tahlil asosida amaldagi qonunchilikning asosiy kamchiliklari aniqlanadi va ularni bartaraf etishning aniq yo‘llari taklif etiladi. Bunda, xususan, ixtisoslashtirilgan tartibga solishning yo‘qligi, xavf-xatarlar va mas’uliyatni taqsimlash, axborot maxfiyligini ta’minlash, xususiy sheriklarni tanlash mezonlari, intellektual mulkni tartibga solish va nazorat mexanizmlari kabi masalalarga alohida e’tibor qaratiladi. Shuningdek, O‘zbekistonda kiberxavfsizlik sohasida DXSHning huquqiy bazasini takomillashtirish bo‘yicha amaliy tavsiyalar taqdim etiladi.

Kalit so‘zlar: davlat-xususiy sherikchiligi, kiberxavfsizlik, huquqiy tartibga solish, qiyosiy-huquqiy tahlil, O‘zbekiston, xorijiy tajriba, huquqiy muammolar, bartaraf etish yo‘llari.

Аннотация. В статье анализируются правовые проблемы, препятствующие эффективному развитию государственно-частного партнерства (ГЧП) в сфере кибербезопасности в Республике Узбекистан, и на основе сравнительно-правового анализа с опытом зарубежных стран (США, Великобритания, Сингапур) выявляются ключевые недостатки действующего законодательства и предлагаются конкретные пути их преодоления, с особым вниманием к вопросам отсутствия специализированного регулирования, распределения рисков и ответственности, обеспечения конфиденциальности информации, критериев отбора частных партнеров, регулирования интеллектуальной собственности и механизмов контроля, а также

представлены практические рекомендации по совершенствованию правовой базы ГЧП в сфере кибербезопасности в Узбекистане.

Ключевые слова: государственно-частное партнерство, кибербезопасность, правовое регулирование, сравнительно-правовой анализ, Узбекистан, зарубежный опыт, правовые проблемы, пути преодоления.

Kirish. Zamonaviy dunyoda kiberxavfsizlik strategik ahamiyat kasb etib, davlat, iqtisodiyot va jamiyatning barqaror rivojlanishining ajralmas sharti hisoblanadi. Kiber tahdidlarning dinamik xususiyatini va himoya vositalarini doimiy takomillashtirish zarurligini hisobga olgan holda, davlat-xususiy sherikchiligi (DXSH) davlat va xususiy sektorning sa'y-harakatlari va resurslarini birlashtirish uchun istiqbolli mexanizm sifatida namoyon bo'ladi. Biroq, yaqqol afzalliklariga qaramay, kiberxavfsizlik sohasida DXSHning rivojlanishi bir qator huquqiy muammolarga duch kelmoqda. Mazkur maqola IMRAD (Kirish, Metodlar, Natijalar va Muhokama) metodologiyasi asosida xorijiy va o'zbekiston tajribasini hisobga olgan holda ushbu muammolarni tahlil qilishga hamda ularni bartaraf etish yo'llarini taklif qilishga bag'ishlangan.

Metodologiya. Mazkur tadqiqot doirasida quyidagi metodlar qo'llanildi: normativ-huquqiy hujjatlarni tahlil qilish (O'zbekiston Respublikasining kiberxavfsizlik va DXSH sohasini tartibga soluvchi qonunchiligi, shuningdek, xorijiy davlatlarning (AQSh, Buyuk Britaniya, Singapur) tegishli normativ hujjatlari o'rganildi); qiyosiy-huquqiy tahlil (turli yurisdiksiyalarda kiberxavfsizlik sohasidagi DXSHning huquqiy mexanizmlarini solishtirish orqali eng yaxshi amaliyotlar va potentsial muammolar aniqlandi); ilmiy nashrlarni tahlil qilish (DXSH va kiberxavfsizlik masalalari bo'yicha mahalliy va xorijiy olimlarning ilmiy ishlari tadqiq etildi); case study (turli mamlakatlarda kiberxavfsizlik sohasida DXSH loyihalarini amalga oshirishning amaliy misollari ko'rib chiqildi); va ekspert intervyulari (O'zbekistonda kiberxavfsizlikni ta'minlashda ishtirok etayotgan davlat organlari va xususiy kompaniyalar vakillari bilan suhbatlar o'tkazildi).

Natijalar. Kiberxavfsizlik sohasida DXSHning normativ-huquqiy bazasi va qo'llanilishini tahlil qilish quyidagi asosiy huquqiy muammolarni aniqladi: kiberxavfsizlik sohasida DXSH bo'yicha ixtisoslashtirilgan qonunchilikning yo'qligi (O'zbekiston

Respublikasida shuningdek, boshqa bir qator mamlakatlarda ham aynan kiberxavfsizlik sohasidagi DXSHning o‘ziga xos xususiyatlarini tartibga soluvchi alohida qonun mavjud emas va DXSH to‘g‘risidagi umumiy qonunchilik normalari axborotning yuqori darajada maxfiyligi, tahdidlarga tezkor javob berish zaruriyati va tez texnologik rivojlanish bilan bog‘liq bo‘lgan ushbu sohaning o‘ziga xosligini to‘liq hisobga olmaydi); xavf-xatarlar va mas’uliyatni taqsimlash muammolari (kiberxavfsizlik loyihalarida davlat va xususiy sheriklar o‘rtasida xavf-xatar va mas’uliyatning optimal balansini aniqlash murakkab vazifa bo‘lib, noaniq taqsimot loyihani samarasiz boshqarishga va xususiy sektorning qiziqishining pasayishiga olib kelishi mumkin, masalan, DXSH doirasida qayta ishlanadigan maxfiy ma’lumotlarning sizib chiqishi uchun javobgarlik masalasi aniq huquqiy tartibga solishni talab qiladi); maxfiylikni ta’minlash va axborotni himoya qilish masalalari (davlat tomonidan xususiy sherikka cheklangan foydalanishdagi axborotni berish uning maxfiyligini ta’minlash va ruxsatsiz kirishdan himoya qilish bo‘yicha ishonchli huquqiy mexanizmlarni talab qiladi va shaxsiy ma’lumotlar va davlat sirlarini himoya qilish bo‘yicha mavjud normalar kiberxavfsizlik sohasidagi DXSH doirasidagi o‘ziga xos munosabatlarni tartibga solish uchun yetarli bo‘lmasligi mumkin); xususiy sheriklarni tanlash mezonlarini aniqlashdagi qiyinchiliklar (kiberxavfsizlik sohasida zaruriy texnik va ekspert bilimlariga ega bo‘lgan kompetentli va ishonchli xususiy sherikni tanlash DXSH loyihasining muvaffaqiyati uchun juda muhimdir va aniq va shaffof tanlash mezonlarining yo‘qligi davlat mablag‘laridan samarasiz foydalanishga va kiberxavfsizlik sohasidagi xavflarning oshishiga olib kelishi mumkin); intellektual mulkni tartibga solish muammolari (DXSH doirasida kiberxavfsizlik sohasida yangi texnologiyalar va yechimlar yaratilishi mumkin va intellektual mulk masalalarini huquqiy tartibga solish, jumladan, yaratilgan ob’ektlarga bo‘lgan huquqlarni aniqlash va ulardan foydalanish tartibi batafsil ishlab chiqilishini talab qiladi); hamda nazorat va audit masalalarining yetarli darajada tartibga solinmaganligi (xususiy sherikning faoliyati ustidan samarali nazorat va kiberxavfsizlik sohasidagi amalga oshirilgan DXSH loyihalarining auditi ularning davlat maqsadlari va vazifalariga muvofiqligini ta’minlash uchun zaruriy shartlardir va nazorat va auditning huquqiy mexanizmlari aniq belgilanishi hamda shaffoflik va hisobdorlikni ta’minlashi kerak).

AQSh kiberxavfsizlik sohasida DXSH mexanizmlaridan faol foydalanadi, xususan, davlat va xususiy tashkilotlar o‘rtasida tahdidlar to‘g‘risida axborot almashish dasturlari orqali. AQSh qonunchiligi bunday hamkorlik doirasida taqdim etilayotgan axborot maxfiyligini ta’minlash bo‘yicha maxsus qoidalarni nazarda tutadi; Buyuk Britaniya kiberxavfsizlik sohasida xabardorlikni oshirish va tajriba almashishga qaratilgan turli tashabbuslar orqali DXSHni rivojlantirmoqda va kiberxavfsizlik sohasida standartlashtirish va sertifikatlashtirish masalalariga alohida e’tibor qaratilmoqda; Singapur kiberxavfsizlik sohasida rivojlangan DXSH tizimiga ega bo‘lib, u qo‘shma tadqiqot loyihalari va kompetensiya markazlarini yaratishni o‘z ichiga oladi. Singapur qonunchiligi tez o‘zgaruvchan texnologik sharoitlarga moslashuvchanligi bilan ajralib turadi.

O‘zbekistonda kiberxavfsizlik sohasida DXSH rivojlanishning boshlang‘ich bosqichida bo‘lib, mavjud loyihalar asosan lokal xususiyatga ega va DXSH to‘g‘risidagi umumiy qonunchilik normalari doirasida amalga oshirilmoqda. Ixtisoslashtirilgan huquqiy tartibga solishning yo‘qligi bunday hamkorlikning miqyosini kengaytirish va samaradorligini oshirish uchun ma’lum qiyinchiliklar yaratmoqda.

AQShda hukumat idoralari va xususiy kompaniyalar o‘rtasida kiber tahdidlar to‘g‘risida axborot almashishning yagona platformasini yaratish bo‘yicha loyiha muvaffaqiyatli amalga oshirildi.

Huquqiy muammo: Axborot almashishning aniq protokollari va uni qayta ishlash standartlarining yo‘qligi tizimning samarasizligiga va ma’lumotlarning sizib chiqishiga olib kelishi mumkin edi.

Yechim: Ushbu loyihaning huquqiy bazasi qanday ma’lumot almashinuvga tegishli ekanligini aniq belgilaydi, kirish darajalari va ruxsatsiz ma’lumotlarni oshkor qilish uchun javobgarlik choralarini shuningdek, almashinuv formatlari va protokollari standartlarini o‘rnatadi.

Singapurda davlat va xususiy sektor ekspertlarini birlashtirgan kiberxavfsizlik bo‘yicha qo‘shma markazni yaratish loyihasi amalga oshirildi.

Huquqiy muammo: Hamkorlik doirasida yaratilgan intellektual mulkka egalik qilish masalalaridagi noaniqlik bahslarga olib kelishi va texnologiyalarning keyingi rivojlanishini qiyinlashtirishi mumkin edi.

Yechim: Markazni yaratish bo‘yicha yuridik kelishuv qo‘shma ishlab chiqilgan intellektual mulkka egalik qilish va undan foydalanish masalalarini, shuningdek, markaz xodimlari aybi bilan sodir bo‘lgan kiberxavfsizlik hodisalari yuzasidan javobgarlikni taqsimlash tartibini batafsil tartibga soladi.

Buyuk Britaniyada DXSHga misol sifatida Kiberxavfsizlik milliy markazi (NCSC) va xususiy kompaniyalar o‘rtasidagi “Kiberxavfsizlik bo‘yicha axborot almashish sherikligi” (CiSP) dasturi doirasidagi hamkorlikni keltirish mumkin.

Huquqiy muammo: Davlat va xususiy tashkilotlarda tijorat sirini himoya qilishga bo‘lgan yondashuvlardagi farq qimmatli axborot almashinuviga to‘sqinlik qilishi mumkin edi.

Yechim: Ushbu hamkorlikning huquqiy jihatlari axborot almashish shartlari, ma’lumotlarni qayta ishlash tartiblari va xususiy sheriklarning tijorat sirlarini himoya qilish bo‘yicha choralarni belgilaydigan o‘zaro anglashuv memorandumlari bilan tartibga solinadi.

O‘zbekistonda Kiberxavfsizlik davlat markazi va yirik IT-kompaniya o‘rtasida kiberxavfsizlik bo‘yicha qo‘shma o‘quv markazini yaratishning gipotetik misolini keltirish mumkin.

Huquqiy muammo: Xususiy sherikni tanlashning aniq mezonlarining yo‘qligi vakolatsiz tashkilotni tanlashga va davlat mablag‘laridan samarasiz foydalanishga olib kelishi mumkin edi.

Yechim: Bunday sherikchilikni huquqiy rasmiylashtirish ishlab chiqilgan o‘quv materiallariga bo‘lgan huquqlarni, bitiruvchilarni sertifikatlash tartibini va ta’lim xizmatlari sifati uchun javobgarlikni taqsimlashni shuningdek, tajriba, malaka va obro‘ga asoslangan xususiy sherikni tanlashning shaffof va ob’ektiv mezonlarini batafsil belgilashni talab qiladi.

Muhokama. Aniqlangan huquqiy muammolar O‘zbekistonda kiberxavfsizlik sohasida DXSHni tartibga soluvchi normativ-huquqiy bazani takomillashtirish zarurligini ko‘rsatadi. Olimlarning fikricha, xorijiy tajribani hisobga olgan holda, kiberxavfsizlikning o‘ziga xos

xususiyatlarini inobatga olgan holda ixtisoslashtirilgan qonun ishlab chiqish yoki amaldagi DXSH to‘g‘risidagi qonunchilikka o‘zgartirishlar kiritish maqsadga muvofiqdir.

O‘zbekiston Respublikasining “Davlat-xususiy sheriklik to‘g‘risida”gi Qonuniga quyidagi o‘zgartish va qo‘shimchalar kiritish lozim:

- Qonunni kiberxavfsizlik sohasidagi DXSH loyihalarini amalga oshirishning o‘ziga xos xususiyatlarini tartibga soluvchi alohida bob bilan to‘ldirish, bunda ob’ektlarning o‘ziga xosligi, ishtirokchilarga qo‘yiladigan talablar, o‘zaro hamkorlik tartibi va axborot xavfsizligini ta’minlash masalalarini hisobga olish.
- Kritik kiber tahdidlar yuzaga kelgan yoki yuzaga kelish xavfi mavjud bo‘lgan hollarda kiberxavfsizlik sohasidagi DXSH loyihalarini kelishish va amalga oshirishning tezlashtirilgan tartiblarini qo‘llash imkoniyatini nazarda tutish.
- Kiberxavfsizlik sohasidagi loyihalarga jalb etilayotgan xususiy sheriklarning malakasi va tajribasiga alohida talablar o‘rnatish, shu jumladan tegishli litsenziya va sertifikatlarning majburiy ravishda mavjud bo‘lishi.

Quyidagi normativ-huquqiy hujjatlarni ishlab chiqish va tasdiqlash lozim:

- Kiberxavfsizlik sohasidagi DXSH loyihalari uchun xususiy sheriklarni tanlash tartibi to‘g‘risidagi nizomni qabul qilish. Nizom texnik kompetentlik, moliyaviy barqarorlik, kiberxavfsizlik sohasidagi ish tajribasi va ishbilarmonlik obro‘sini hisobga olgan holda baholashning shaffof va ob’ektiv mezonlarini o‘z ichiga oladi.
- Kiberxavfsizlik sohasidagi davlat-xususiy sheriklik to‘g‘risidagi namunaviy bitimni tasdiqlash. Bitim xavf-xatar va mas’uliyatni taqsimlashning unifikatsiyalashgan shartlarini, axborot maxfiyligi va himoyasini ta’minlash tartibini, intellektual mulkka bo‘lgan huquqlarni tartibga solishni hamda nazorat va audit mexanizmlarini o‘z ichiga oladi.
- DXSH loyihalari doirasida xususiy sheriklar tomonidan majburiy ijro etilishi kerak bo‘lgan kiberxavfsizlik sohasidagi texnik reglamentlar va standartlarni ishlab chiqish va tasdiqlash.

Ixtisoslashtirilgan davlat organini yoki ishchi guruhni tashkil etish:

✓ Kiberxavfsizlik sohasidagi DXSH loyihalarini muvofiqlashtirish, qo‘llab-quvvatlash va monitoring qilish uchun mas’ul bo‘lgan ixtisoslashtirilgan davlat organini yoki idoralararo ishchi guruhni tashkil etish imkoniyatini ko‘rib chiqish.

✓ Mazkur organga metodik tavsiyalar ishlab chiqish, loyihalarni ekspertizadan o‘tkazish va bitimlarning ijrosini nazorat qilish bo‘yicha vakolatlar berish.

Xalqaro hamkorlikni rivojlantirish kerak:

- Kiberxavfsizlik sohasida DXSHni huquqiy tartibga solish bo‘yicha xorijiy davlatlarning eng yaxshi amaliyotlarini faol o‘rganish va joriy etish.
- Tajriba almashish va kiberxavfsizlik sohasidagi DXSH loyihalariga investitsiyalarni jalb qilish uchun xorijiy hamkorlar bilan xalqaro bitimlar va o‘zaro anglashuv memorandumlarini tuzish.

Kadrlar malakasi va xabardorligini oshirish zarur:

- Davlat xizmatchilari va xususiy sektor vakillarini kiberxavfsizlik sohasida DXSH loyihalarini huquqiy tartibga solish va amalga oshirish masalalari bo‘yicha o‘qitish va malakasini oshirishni tashkil etish.
- Dolzarb muammolarni muhokama qilish va tajriba almashish uchun muntazam ravishda seminarlar, konferensiyalar va davra suhbatlari o‘tkazish.

Huquq nazariyasi nuqtai nazaridan, kiberxavfsizlik sohasida DXSHni rivojlantirish milliy xavfsizlikni ta’minlashning davlat manfaatlari va xususiy sektorning iqtisodiy manfaatlari o‘rtasida muvozanatni izlashni talab qiladi. Huquqiy tartibga solish xususiy tashabbus va innovatsiyalarni rag‘batlantirishi, shu bilan birga davlat tomonidan tegishli nazorat darajasini ta’minlashi kerak. Shuningdek, kiberxavfsizlik dinamik rivojlanayotgan soha ekanligini hisobga olish zarur, shuning uchun huquqiy normalar yangi texnologiyalar va tahdidlarga yetarlicha moslashuvchan bo‘lishi kerak.

Xulosa. Kiberxavfsizlik sohasida davlat-xususiy sherikchiligini rivojlantirish O‘zbekiston Respublikasi axborot makonining himoya darajasini oshirish uchun istiqbolli yo‘nalish hisoblanadi. Biroq, DXSH salohiyatini samarali ro‘yobga chiqarish uchun ixtisoslashtirilgan qonunchilikni ishlab chiqish, xavf-xatar va mas’uliyatni taqsimlash mexanizmlarini takomillashtirish, axborot maxfiyligi kafolatlarini kuchaytirish, sheriklarni

tanlashning shaffof mezonlarini joriy etish, intellektual mulk masalalarini batafsil tartibga solish va samarali nazorat va audit mexanizmlarini joriy etish shuningdek, ushbu sohada normativ-huquqiy bazani va institutsional mexanizmlarni takomillashtirishga qaratilgan aniq amaliy takliflarni kiritish orqali mavjud huquqiy muammolarni bartaraf etish zarur. Xorijiy tajribani hisobga olish va ushbu muammolarni hal qilishga ilmiy yondashuv kiberxavfsizlik sohasida davlat va xususiy sektorning o‘zaro manfaatli hamkorligini rivojlantirish uchun qulay huquqiy sharoitlar yaratishga imkon beradi.

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. National Cybersecurity Protection Act of 2014, Public Law 113-274.
9. National Cyber Security Strategy (Buyuk Britaniya).
10. Official Secrets Act (Buyuk Britaniya).
11. Computer Misuse Act 1990 (Buyuk Britaniya).
12. Cybersecurity Act 2018 (Singapur).
13. Personal Data Protection Act (PDPA) (Singapur).