KIBERXAVFSIZLIK SOHASIDA DAVLAT-XUSUSIY SHERIKCHILIKNI RIVOJLANTIRISHNING STRATEGIK YO‘NALISHLARI

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

Annotatsiya. Ushbu maqolada kiberxavfsizlik sohasida davlat-xususiy sherikchilikni rivojlantirishning strategik yo‘nalishlarini o‘rganishga bag‘ishlanadi. Maqolada kiberxavfsizlik sohasida davlat-xususiy sherikchilikni rivojlantirishning strategik yo‘nalishlarining imkoniyatlarini o‘rganishga alohida e’tibor qaratiladi. Maqolada axborot xavfsizligini ta’minlashda davlat va xususiy sektorning o‘zaro hamkorligi samaradorligini oshirishga yo‘naltirilgan kiberxavfsizlik sohasida DXShni huquqiy tartibga solishni takomillashtirish bo‘yicha tavsiyalar beriladi.

Аннотация. В данной статье посвящено изучению стратегических направлений развития государственно-частного партнёрства в сфере кибербезопасности. Особое внимание уделяется возможностям развития государственно-частного партнёрства в данной сфере. В статье приведены рекомендации по совершенствованию правового регулирования ГЧП в сфере кибербезопасности, направленные на повышение эффективности взаимодействия государства и частного сектора в обеспечении информационной безопасности.

Annotation. This article is devoted to the study of strategic directions for the development of public-private partnership in the field of cybersecurity. Special attention is given to the potential opportunities for advancing such partnerships in this area. The article provides recommendations for improving the legal regulation of public-private partnership in cybersecurity, aimed at enhancing the effectiveness of cooperation between the public and private sectors in ensuring information security.

Raqamli asrda kiberxavfsizlik milliy xavfsizlik, iqtisodiy taraqqiyot va fuqarolarning davlat tizimlariga bo‘lgan ishonchini ta’minlashda muhim omilga aylangan. Tahdidlar murakkab va puxta uyushtirilgan shaklga ega bo‘lib borar ekan, davlat organlari ularni yolg‘iz hal eta olmaydi. Davlat-xususiy sheriklik modeli xususiy sektorning texnik salohiyati, innovatsion imkoniyatlari va resurslaridan foydalangan holda milliy kiberbarqarorlikni mustahkamlashning samarali usuli hisoblanadi. Raqamlashtirish sur’atlari yuqori bo‘lgan O‘zbekiston uchun kiberxavfsizlik sohasida DXShni yo‘lga qo‘yish va rivojlantirish dolzarb va strategik ahamiyatga ega. Xususiy hamkorlar davlatlarga xalqaro hamkorlikni amalga oshirishda yordam berib, axborot texnologiyalari jinoyatchiligiga qarshi kurashda transchegaraviy hamkorlikka o‘z hissasini qo‘shmoqda. Bunday hamkorlikning

maqsadi kiberxavflarga qarshi kurashda samaradorlikni oshirish, ma’lumot va tajriba almashinuvini ta’minlash, hamda kiberhujumlar yuz berganda harakatlarni muvofiqlashtirish mexanizmlarini yaratishdan iborat. Davlat-xususiy hamkorlik, shuningdek, axborot tizimlarini himoya qilish bo‘yicha yangi texnologiyalar va uslublarni ishlab chiqishga ham xizmat qilishi mumkin. Umuman olganda, davlat va xususiy tuzilmalar o‘rtasida hamkorlik aloqalarini o‘rnatish kiberjinoyatchilikka qarshi kurashda muhim qadam hisoblanadi. Faqatgina birgalikdagi harakatlar orqali axborot tizimlarini himoya qilish va kiberhujumlarning oldini olishda maksimal samaradorlikka erishish mumkin.

Axborot texnologiyalari jinoyatchiligiga qarshi kurashish uchun davlat-xususiy hamkorlikni yo‘lga qo‘yish zarurati bir qancha sabablarga asoslanadi, jumladan:

mazkur sohada sodir etilayotgan jinoyatlar sonining keskin o‘sib borayotganligi.

huquqni muhofaza qiluvchi organlarda axborot texnologiyalari sohasi o‘ziga xos xususiyatlarini hisobga olgan holda samarali kasbiy faoliyat yurita oladigan malakali mutaxassislarning yetishmasligi.

huquqni muhofaza qiluvchi organ xodimlarining maxsus vositalar va dasturiy ta’minot bilan texnik jihozlanish darajasining yetarli emasligi[1].

Kompyuter jinoyatchiligiga qarshi kurashni samaraliroq tashkil etish maqsadida xalqaro tashkilotlar, masalan, Interpol, Evropol va boshqa tuzilmalar kiber va texnologik sohalarda imkoniyatlarga ega bo‘lgan hamkorlarni jalb etishi lozim. Shu bois, xalqaro tashkilotlar tobora ko‘proq xususiy sektor kompaniyalarini o‘z faoliyatiga jalb qilmoqda. Masalan, Interpol dunyo bo‘ylab hamkorlar bilan ishlaydi, ular orqali yuzaga kelayotgan kiberxavflar haqida ma’lumot almashadi, a’zo davlatlarning huquqni muhofaza qiluvchi organlariga yordam ko‘rsatish uchun yangi vositalarni ishlab chiqadi, hamda kiberjinoyatchilik va kiberxavfsizlik sohasidagi ko‘nikma va tajriba bilan o‘rtoqlashadi. Interpol axborot xavfsizligi yo‘nalishida qator xalqaro va mintaqaviy tashkilotlar bilan yaqin hamkorlik qiladi[2]. Bundan tashqari, axborot texnologiyalari va bank sohasi rivoji bilan shug‘ullanuvchi turli xususiy kompaniyalar va tashkilotlar ham bunday hamkorlar qatoriga kiradi. “Kasperskiy laboratoriyasi” – bu 1997-yildan buyon axborot xavfsizligi bilan shug‘ullanib kelayotgan xalqaro kompaniya. U muhim axborot infratuzilmalari, korxonalar, davlat tashkilotlari va aholining xavfsizligini ta’minlash borasida katta tajribaga ega. Kompaniyaning asosiy vazifalari turli qurilmalarni himoya qilish uchun zamonaviy vositalarni ishlab chiqish va axborot texnologiyalari jinoyatchiligiga qarshi kurashish bo‘yicha yechimlar yaratishdan iborat. Hozirda “Kasperskiy

[1] Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности: субъекты и тенденции эволюции: дис. … докт. полит. наук. – М., 2019. – С. 156-157

[2] Рыжов В.Б. Информационная безопасность в государствах Европейского Союза: к постановке проблемы // Представительная власть: XXI век: законодательство, комментарии, проблемы. 2018. № 4 (163). – С. 8-12.

laboratoriyasi” butun dunyo bo‘ylab taxminan 270 ming korporativ mijoz va 400 million foydalanuvchi xavfsizligini ta’minlamoqda. Bundan tashqari, kompaniya xalqaro huquqni muhofaza qiluvchi tashkilotlar bilan hamkorlik qilib, zararli dasturlar bo‘yicha texnik maslahatlar va ekspert tahlilini taqdim etadi.

Axborot xavfsizligi bizning raqamli davrimizda muhim masala hisoblanadi. Axborot xavfsizligi bozorida tajribasiz holda xalqaro huquqni muhofaza qiluvchi organlarning kiberjinoyatlarni tergov qilishdagi harakatlari – bu amalda amalga oshmaydigan orzu xolos. Shu sababli, bunday hamkorlik kiberjinoyatchilikka qarshi global kurash uchun zarurdir. Bundan tashqari, hamkorlik doirasida “Kasperskiy laboratoriyasi” Evropolga kiberjinoyatlarni tergov qilishda ekspertlik yordamini ko‘rsatadi, shuningdek, Yevropa Ittifoqi huquqni muhofaza qiluvchi organlari xodimlarini tayyorlash va malakasini oshirishda ko‘maklashadi. “Kasperskiy laboratoriyasi” va Evropol o‘rtasidagi hamkorlik kiberjinoyatchilikka qarshi kurashda muhim qadamlardan biri bo‘lib, internetdagi foydalanuvchilar manfaatlarini samaraliroq himoya qilish imkonini beradi. Ayniqsa, “Kasperskiy laboratoriyasi” nafaqat Interpol, Evropol kabi xalqaro tashkilotlar bilan, balki turli mamlakatlardagi huquqni muhofaza qiluvchi organlar bilan ham hamkorlik qiladi. Jumladan: Rossiya, AQSh, Buyuk Britaniya, Germaniya va boshqalar. Kompaniya, shuningdek, kiberxavfsizlik sohasida faoliyat yurituvchi davlat va xususiy tashkilotlar bilan yaqindan hamkorlik qiladi, hamda ushbu yo‘nalishda ishlovchi mutaxassislar uchun o‘quv dasturlari va treninglar o‘tkazadi. Bularning barchasi “Kasperskiy laboratoriyasi”ni kiberxavfsizlik sohasida yetakchi kompaniyaga aylantiradi va global miqyosda kiberxavflarga qarshi samarali kurashishga xizmat qiladi[3]. Bunday tadbirlar nafaqat tajriba va bilim almashish imkonini beradi, balki xalqaro miqyosda kiberxavflarga qarshi harakatlarni muvofiqlashtirishga ham yordam beradi. Bundan tashqari, “Sberbank” ham o‘zining kiberxavfsizlik tizimini faol rivojlantirmoqda va mijozlari hamda biznes hamkorlarini kiberhujumlardan himoya qilish uchun innovatsion texnologiyalarni joriy etmoqda. Shunday qilib, “Kasperskiy laboratoriyasi” kabi kompaniyalar va “Sberbank” kabi yirik moliyaviy institutlarning ekspertlik ko‘magi xalqaro darajadagi kiberxavflarga qarshi kurashda muhim omil hisoblanadi[4]. Ular nafaqat zararli dasturlar va botnetlarni aniqlash va zararsizlantirishga yordam beradi, balki yangi tahdidlarga qarshi himoya qilish uchun innovatsion texnologiyalarni ishlab chiqadi.

Avvalo, O‘zbekistonda kiberxavfsizlik va DXSh sohasidagi huquqiy hamda institutsional bazaning normativ-huquqiy asoslariga to‘xtaladigan bo‘lsak,

[3] The Kaspersky Industrial CyberSecurity Platform https://www.kaspersky.com/enterprisesecurity/industrial-cybersecurity

[4] INTERPOL strengthens cooperation with Kaspersky Lab in global fight against cybercrime. https://www.interpol.int/News-and-Events/News/2014/INTERPOL-strengthens-cooperation-with-Kaspersky-Lab-in-global-fight-against-cybercrime

O‘zbekiston kiberxavfsizlik va davlat-xususiy sheriklik yo‘nalishida bir qator muhim qonunchilik hujjatlarini qabul qilgan:

“Davlat-xususiy sheriklik to‘g‘risida”gi Qonun – DXShning umumiy huquqiy asoslarini belgilaydi, unda sheriklik shakllari, jarayonlari va ishtirokchi subyektlar roli ko‘rsatilgan.

“Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun hamda “Kiberxavfsizlik to‘g‘risida”gi Qonun – ma’lumotlarni himoya qilish va kiberhodisalarga javob berish bo‘yicha majburiyatlarni belgilaydi, bunda xususiy sektor ishtiroki ehtimoli mavjud[5].

Prezidentning 2020-yil 5-oktabrdagi PF-6079-sonli Farmoni – raqamli iqtisodiyot va elektron hukumatni rivojlantirish choralarini ko‘zda tutadi, xususiy sektorning raqamli xavfsizlikdagi rolini rag‘batlantiradi.

Kiberxavfsizlik konsepsiyasi (2020–2023-yillar) – milliy strategik hujjat bo‘lib, xalqaro hamkorlik va xususiy sektor ishtirokini nazarda tutadi. Yuqorida ta’kidlab o‘tganimizdek, biroq kiberxavfsizlik bo‘yicha aniq DXSh modelini bevosita tartibga soluvchi maxsus huquqiy hujjat mavjud emas.

O‘zbekistonda kiberxavfsizlik va DXSh sohasidagi institutsional tuzilmalarni sanab, ularni yoritib o‘tamiz. Asosiy mas’ul tashkilotlar quyidagilardan iborat: Birinchisi, Raqamli texnologiyalar vazirligi huzuridagi Kiberxavfsizlik bo‘yicha davlat markazi – kiberxavfsizlik siyosati, standartlar va monitoring uchun mas’ul hisoblanadi. Ikkinchisi, Kiberxavfsizlikni muvofiqlashtirish bo‘yicha Kengash – vazirliklararo platforma bo‘lib, xususiy sektor vakilligi cheklangan. Uchinchisi “O‘zbektelekom”, “UzCard” va yirik moliyaviy institutlar – amaliy kiberxavfsizlikda faol ishtirok etadi, ammo ular bilan shakllangan DXSh mexanizmlari hozircha mavjud emas.

Xorijiy olimlar nuqtayi nazaridan kiberxavfsizlikdagi DXShni yoritadigan bo‘lsak, AQSh va Yevropa Ittifoqi tajribasida hamkorlikka asoslangan boshqaruv mavjud bo‘lib, ko‘plab xorijiy olimlar, xususan Kshetri (2016) kiberxavfsizlik sohasida “birgalikda boshqarish” modelini qo‘llab-quvvatlaydi. Bunda davlatlar qonunchilik va tartibga solish bazasini yaratadi, xususiy sektor esa innovatsiya, texnik yechimlar va tahdidlar haqidagi ma’lumotlarni taqdim etadi. Axborot almashinuvi tizimlarini yaratish, masalan, AQShdagi Cybersecurity Information Sharing Act (CISA) va Yevropa Ittifoqining NIS2 Direktivasi davlat va xususiy sub’yektlar o‘rtasidagi majburiy hamkorlikni belgilaydi[6]. Dunn-Cavelty (2012) tomonidan ilgari surilgan (Xavfga asoslangan DXSh modeli – Buyuk Britaniya, Avstraliya tajribasi) yondashuvga ko‘ra, xavflar tahlili jarayonida xususiy sektor faol ishtirok etadi, davlat esa milliy miqyosdagi xavf ustuvorliklarini belgilaydi va resurslarni taqsimlaydi. Avstraliyada yaratilgan Critical Infrastructure Centre modeli xususiy subyektlar bilan

[5] O‘zbekiston Respublikasining Qonuni, 02.07.2019 yildagi O‘RQ-547-son https://lex.uz/docs/-4396419
[6] Kshetri, N. (2016). Cybersecurity and International Relations. Journal of International Affairs.

hamkorlikda xavf tahlilini o‘tkazish tajribasini o‘z ichiga oladi[7]. Ushbu yondashuvlar O‘zbekistonda kiberxavfsizlikni boshqarishda davlat va xususiy sektor o‘rtasida roli aniq taqsimlangan, birgalikda boshqaruvga asoslangan modelni joriy etish uchun mustahkam asos bo‘la oladi. Xavfga asoslangan DXSh modeli esa tahdidlarni baholash va resurslarni oqilona taqsimlash orqali milliy xavfsizlikni ta’minlashda muhim rol o‘ynaydi.

O‘zbekistonlik olimlar tomonidan ta’kidlanishicha, “Raqamli O‘zbekiston – 2030” strategiyasi doirasida kiberxavfsizlikda DXShni institutsional asosda rivojlantirish imkoniyatlari yaratilmoqda. Ularning fikricha, DXSh davlatga resurs va mutaxassislik tanqisligini bartaraf etishda yordam beradi. Yangi huquqiy asoslar xususiy sektor uchun jozibador shartlarni ham kafolatlamog‘i lozim.

O‘zbekistonlik va xorijlik olimlarning tadqiqotlari asosida kiberxavfsizlikdagi DXShni rivojlantirishning strategik yo‘nalishlari quyidagilardan iborat. Huquqiy va me’yoriy bazani takomillashtirish O‘zbekistonda DXSh qonunida kiberxavfsizlik loyihalarini aniq belgilovchi bandlar mavjud emas. Xorijda – Singapur va AQSh kabi mamlakatlarda Cybersecurity Act DXShni maxsus soha sifatida tartibga soladi[8]. Xavflarni birgalikda boshqarish tizimi – DXSh orqali tarmoqlar bo‘yicha birgalikda xavf tahlili va ustuvorliklarni belgilash, OECD olimlari tomonidan DXShda axborot xavfi almashinuvi tizimlari samarali ekani e’tirof etiladi. Axborot almashinuvi platformalari – biz tomonidan Milliy tahdidlar haqida ma’lumot almashish platformasini yaratish taklif qilingandi, AQShda esa Information Sharing and Analysis Centers (ISACs) bu borada samarali model sanaladi. Investitsiya va innovatsiyaviy sheriklik, ya’ni DXSh orqali AI asosidagi xavfsizlik texnologiyalari, kriptografiya, kiber ta’lim loyihalariga sarmoya jalb qilish, Isroilning Be’er Sheva kiberparki[9] misolida davlat, oliygohlar va IT kompaniyalar hamkorligidagi innovatsion klasterlar samaradorligi tasdiqlangan. Inson kapitalini rivojlantirish, ya’ni DXSh asosida kiberxavfsizlik bo‘yicha oliy ta’lim dasturlarini xususiy sektor bilan birga ishlab chiqish, Estoniyada esa milliy kiberxavfsizlik bo‘yicha mashg‘ulotlar va simulyatsiyalar orqali davlat-xususiy sektordagi kadrlar malakasi oshirilmoqda.

O‘zbekistonda DXShni rivojlantirishning strategik yo‘nalishlarini sanab o‘tadigan bo‘lsak, quyidagi strategik yo‘nalishlar O‘zbekiston sharoitida kiberxavfsizlikdagi DXShni rivojlantirish uchun muhim hisoblanadi. Birinchidan, Kiberxavfsizlikda DXShga oid alohida strategiya ishlab chiqish, ya’ni “Raqamli

[7] Dunn-Cavelty, M. (2013). Public-private partnerships in cybersecurity: Risk-based approaches. Risk Analysis. Threat representations with an impact in the cyber-security discourse. International Studies Review, 15(1), 105-122. https://doi.org/10.1111/misr.12023

[8] Cybersecurity Act 2018 (Singapur). https://sso.agc.gov.sg/Acts-Supp/9-2018/?utm_source

[9] Kabinett beschließt Cyberpark in Beer Sheva zu unterstützen https://www.juedische.at/pages/israelnaher-osten/israels-kabinett-beschliesst-cyberpark-in-beer-sheva-zu-unterstuetzen/

O‘zbekiston – 2030” strategiyasi[10] doirasida kiberxavfsizlik bo‘yicha DXSh alohida bo‘lim sifatida kiritilishi lozim. Har bir ishtirokchi – davlat organlari, IT kompaniyalar, banklar va fuqarolik jamiyati – uchun aniq funksiyalar belgilanishi kerak.

Ikkinchidan, kiberxavfsizlik bo‘yicha Davlat-xususiy sheriklik kengashini tashkil etish lozim. Raqamli texnologiyalar vazirligi huzurida Kiberxavfsizlik bo‘yicha DXSh Kengashi tashkil etilishi kerak. Unga yirik IT kompaniyalar, moliya sektori, ilmiy muassasalar va fuqarolik jamiyati vakillari jalb qilinadi.

Uchinchidan, axborot almashinuvi mexanizmlarini rivojlantirish, bu strategik yo‘nalish orqali tahdidlar to‘g‘risida yuridik jihatdan himoyalangan axborot almashish platformalari yaratiladi. Misol uchun AQShdagi ISAC (Information Sharing and Analysis Centers) modeli[11] asosida bank, transport va telekommunikatsiya tarmoqlari uchun alohida markazlar tashkil qilinadi.

To‘rtinchidan, ilmiy-tadqiqot va innovatsion hamkorlik markazlarini yo‘lga qo‘yish, bu orqali davlat va xususiy sektor hamkorligida Kiberxavfsizlik bo‘yicha Innovatsion laboratoriyalar tashkil etilishi mumkin. Sun’iy intellekt asosidagi tahdidlarni aniqlash, kriptografiya va xavfsiz tarmoq yechimlari ishlab chiqiladi.

Beshinchidan, kadrlar tayyorlashda davlat-xususiy sheriklikni kuchaytirish, ya’ni IT kompaniyalar bilan hamkorlikda kiberxavfsizlik akademiyalari tashkil etish lozim. Bu orqali davlat organlari va xususiy kompaniyalar o‘rtasida stajirovkalar va amaliyot dasturlari yo‘lga qo‘yiladi.

Oltinchidan, Startaplar uchun kiberxavfsizlik “regulyator sandbox”larini yaratish, bu bilan kiberxavfsizlik startaplari o‘z mahsulotlarini sinovdan o‘tkazishi uchun regulyator qulayliklari bilan tajriba maydonlari (sandbox) yaratiladi. Milliy xavfsizlik bilan bog‘liq IT yechimlarga soliq imtiyozlari taqdim etiladi.

Yettinchidan, davlat xaridlari orqali DXShni rag‘batlantirish, bu orqali kiberxavfsizlik xizmatlari va infratuzilmasi strategik davlat xaridlari ro‘yxatiga kiritiladi. Davlat buyurtmachilari tomonidan milliy xavfsizlik standartlariga mos bo‘lgan mahsulotlar talabi joriy qilinadi.

Ushbu strategik yo‘nalishlarni amalga oshirishda mavjud muammolar va to‘siqlar mavjud. DXShni kiberxavfsizlikda rivojlantirishda quyidagi muammolar yechimini topish zarur. Avvalo, huquqiy noaniqlik, ya’ni ma’lumotlar egaligi va javobgarlik masalasi aniq belgilanmagan. Ikkinchisi, ishonch muammosi, ya’ni davlat va xususiy sektor o‘rtasida axborot almashish borasida yetarlicha ishonch mavjud emas. Uchinchisi, xususiy sektor salohiyatining cheklanganligi, ya’ni ko‘plab mahalliy IT kompaniyalar texnologik va moliyaviy jihatdan hali tayyor emas. To‘rtinchisi, hududiy nomutanosiblik, ya’ni Toshkent tashqarisidagi hududlarda

[10] O‘zbekiston Respublikasi Prezidentining Farmoni, 05.10.2020 yildagi PF-6079-son https://lex.uz/ru/docs/-5030957

[11] The ISAC (Information Sharing and Analysis Centers) model in the USA https://www.nationalisacs.org/

raqamli infratuzilma zaif. Bu tajribalar shuni ko‘rsatadiki, DXSh muvaffaqiyati uchun ishonch, aniq rollar, yuridik aniqlik va hamkorlikka tayyorlik muhim ahamiyatga ega.

Xulosa qiladigan bo‘lsak, kiberxavfsizlikda davlat-xususiy sheriklik O‘zbekiston uchun nafaqat zaruriy himoya mexanizmi, balki raqamli iqtisodiyotda ishonchli va xavfsiz rivojlanish kafolatidir. DXSh asosida yondashuv O‘zbekistonning xalqaro IT bozoridagi raqobatbardoshligini oshiradi, davlat sektorining barqarorligini ta’minlaydi va xususiy sektorga investitsion ishonchni mustahkamlaydi. Agar ushbu strategiyalar tizimli ravishda amalga oshirilsa, O‘zbekiston nafaqat mintaqada, balki keng xalqaro miqyosda kiberxavfsizlik bo‘yicha ilg‘or davlatlardan biriga aylanishi mumkin.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

I. 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

II. Kitob va turkum nashrlari:

1. “Роль государственно-частного партнерства в формировании устойчивой политики кибербезопасности Японии” Низамова М. А. Казанский (Приволжский) федеральный университет.
2. “Development of public-private partnership to counter crime in the sphere of information technologies” Samogin Artem Aergeevich, Zelenaya Ekaterina Elekseevna, Russian Technological University.
3. Public-private partnerships on cybercrime regional perspectives best practices, challendes, and opportunities from the Americas, Africa and Asia.

4. 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

III. 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
8. Japan Computer Emergency Response Team Coordination Center. URL: https://www.jpcert.or.jp/about/
9. INTERPOL strengthens cooperation with Kaspersky Lab in global fight gainst cybercrime. https://www.interpol.int/News-andEvents/News/2014/INTERPOL-strengthens-cooperation-with-Kaspersky-Lab-in-global-fight-against-cybercrime