

**O‘ZBEKISTON RESPUBLIKASI VA XORIJIY DAVLATLARDA
KIBERXAVFSIZLIKNI TARTIBGA SOLISH QIYOSIY TAHLILI**

Mannonov Asliddin Akbar o‘g‘li

Toshkent Davlat Yuridik Universiteti
Magistratura bosqichi Kiber huquqi mutaxassisligi
asliddinmannonov0980@gmail.com

Annotatsiya. Zamonaviy dunyoda kiberxavfsizlik davlat xavfsizligining muhim tarkibiy qismi sifatida qaralmoqda. Ushbu maqola O‘zbekiston Respublikasi va xorijiy davlatlar (AQSh, Yevropa Ittifoqi, Rossiya, Xitoy) kiberxavfsizlikni tartibga solish tizimlarini qiyosiy tahlil qilishga bag‘ishlangan. Tadqiqotda qiyosiy-huquqiy tahlil usulidan foydalanib, normativ-huquqiy hujjatlar, amaliy yondashuvlar va institutsional tuzilmalar o‘rganildi.

Kalit so‘zlar: kiberxavfsizlik, qonunchilik, O‘zbekiston, xorijiy davlatlar, qiyosiy tahlil, ITU, ISO.

**СРАВНИТЕЛЬНЫЙ АНАЛИЗ РЕГУЛИРОВАНИЯ
КИБЕРБЕЗОПАСНОСТИ В РЕСПУБЛИКЕ УЗБЕКИСТАН И
ЗАРУБЕЖНЫХ СТРАНАХ**

Маннонов Аслиддин Акбар угли

Ташкентский государственный юридический университет
Степень магистра в области киберправа
asliddinmannonov0980@gmail.com

Аннотация. В современном мире кибербезопасность считается важной составляющей национальной безопасности. Статья посвящена сравнительному анализу систем регулирования кибербезопасности Республики Узбекистан и зарубежных стран (США, Евросоюза, России, Китая). В исследовании использован метод сравнительно-правового анализа для изучения нормативных правовых документов, практических подходов и институциональных структур.

Ключевые слова: кибербезопасность, законодательство, Узбекистан, зарубежные страны, сравнительный анализ, ITU, ISO.

**COMPARATIVE ANALYSIS OF CYBERSECURITY
REGULATION IN THE REPUBLIC OF UZBEKISTAN AND FOREIGN
STATES**

Mannonov Asliddin Akbar ugli

Tashkent State University of Law

Master's degree in Cyber Law

asliddinmannonov0980@gmail.com

Annotation. In the modern world, cybersecurity is considered an important component of state security. This article is devoted to a comparative analysis of the cybersecurity regulatory systems of the Republic of Uzbekistan and foreign countries (USA, European Union, Russia, China). The study studied regulatory legal acts, practical approaches and institutional structures using the method of comparative legal analysis.

Keywords: cybersecurity, legislation, Uzbekistan, foreign countries, comparative analysis, ITU, ISO.

Kirish. Zamonaviy dunyoda axborot texnologiyalarining jadal rivojlanishi iqtisodiy, ijtimoiy va siyosiy jarayonlarni tubdan o'zgartirib, raqamli makonni hayotning ajralmas qismiga aylantirdi. Biroq, ushbu taraqqiyot kiberxavfsizlikka oid yangi tahdidlarni keltirib chiqardi. Kiberhujumlarning ko'payishi, shaxsiy va davlat ma'lumotlarining xavf ostida qolishi, shuningdek, muhim raqamli infratuzilmalarga qaratilgan xatarlar davlatlar oldida kiberxavfsizlikni ta'minlash masalasini dolzarb vazifaga aylantirmoqda. Xalqaro tashkilotlar ma'lumotlariga ko'ra, kiberjinoyatlarning global iqtisodiyotga yetkazayotgan zarari yil sayin o'sib bormoqda, bu esa huquqiy va institutsional choralar samaradorligini oshirish zarurligini ta'kidlaydi.

O‘zbekiston Respublikasi raqamli iqtisodiyotni rivojlantirish va axborot texnologiyalarini keng joriy etish yo‘lida muhim qadamlar tashlamoqda. 2022-yilda qabul qilingan “Kiberxavfsizlik to‘g‘risida”gi Qonun ushbu sohada milliy qonunchilik bazasini shakllantirishga xizmat qildi. Biroq, kiberxavfsizlikni tartibga solishning samaradorligi nafaqat mahalliy qonunchilikning mustahkamligiga, balki global tajribalarga moslashish va xalqaro hamkorlikka ham bog‘liq. Xorijiy davlatlar, xususan, AQSh, Yevropa Ittifoqi, Rossiya va Xitoy kabi yetakchi mamlakatlar kiberxavfsizlik sohasida o‘ziga xos huquqiy va amaliy yondashuvlarni ishlab chiqqan bo‘lib, ularning tajribasi O‘zbekiston uchun foydali saboqlar berishi mumkin. Ushbu maqola O‘zbekiston Respublikasi va xorijiy davlatlarda kiberxavfsizlikni tartibga solishning huquqiy asoslari, institutsional tuzilmalari va amaliy yondashuvlarini qiyosiy tahlil qilishga qaratilgan. Tadqiqotning asosiy maqsadi O‘zbekiston qonunchiligining kuchli va zaif tomonlarini aniqlash, shuningdek, xorijiy davlatlarning ilg‘or tajribalarini o‘rganish orqali milliy kiberxavfsizlik tizimini takomillashtirish bo‘yicha takliflar ishlab chiqishdan iborat. Tadqiqotda quyidagi savollarga javob izlanadi: O‘zbekistonning kiberxavfsizlik qonunchiligi zamonaviy tahdidlarga qanchalik mos keladi? Xorijiy davlatlarning qaysi tajribalari O‘zbekiston uchun qo‘llanilishi mumkin? Ushbu savollar asosida qiyosiy-huquqiy tahlil usuli yordamida har bir mamlakatning normativ-huquqiy bazasi, tashkiliy tuzilmalari va kiberxavfsizlikni ta‘minlashdagi amaliy choralari o‘rganiladi.

Maqola kiberxavfsizlik sohasidagi global va mahalliy muammolarni yoritish bilan birga, O‘zbekiston uchun strategik rivojlanish yo‘nalishlarini belgilashga xizmat qiladi. Tadqiqot natijalari nafaqat ilmiy jamoatchilik, balki

qonun chiqaruvchi organlar va kiberxavfsizlik sohasidagi mutaxassislar uchun ham amaliy ahamiyatga ega bo'ladi.

Metodologiya. Ushbu tadqiqot O'zbekiston Respublikasi va xorijiy davlatlarning kiberxavfsizlikni tartibga solish tizimlarini qiyosiy tahlil qilishga qaratilgan bo'lib, qiyosiy-huquqiy tahlil usuliga asoslanadi. Tadqiqotda normativ-huquqiy hujjatlar, ilmiy adabiyotlar va xalqaro tashkilotlarning hisobotlari asosiy ma'lumot manbalari sifatida foydalanildi. O'zbekistonning kiberxavfsizlik qonunchiligi, shu jumladan "Kiberxavfsizlik to'g'risida"gi Qonun (2022) va tegishli prezident qarorlari tahlil qilindi. Xorijiy davlatlar sifatida AQSh, Yevropa Ittifoqi, Rossiya va Xitoy tanlandi, ularning kiberxavfsizlikka oid qonunlari (masalan, GDPR, NIST Framework, Xitoyning Cybersecurity Law) o'rganildi. Ma'lumotlarni yig'ishda rasmiy davlat saytlari (lex.uz, ec.europa.eu), xalqaro tashkilotlar hisobotlari va ilmiy maqolalardan foydalanildi. Tahlil jarayonida huquqiy bazalar, institutsional tuzilmalar va amaliy yondashuvlar solishtirilib, ularning afzalliklari va kamchiliklari aniqlandi. Tadqiqot O'zbekistonning milliy xususiyatlarini hisobga olgan holda, xorijiy tajribalarni qo'llash imkoniyatlarini baholashga yo'naltirildi. Natijalar O'zbekiston kiberxavfsizlik tizimini takomillashtirish bo'yicha amaliy takliflar ishlab chiqish uchun asos bo'lib xizmat qiladi.

Asosiy qism. O'zbekiston Respublikasida kiberxavfsizlikni tartibga solish raqamli iqtisodiyotni rivojlantirish va axborot xavfsizligini ta'minlashning muhim yo'nalishi sifatida shakllanmoqda. 2022-yilda qabul qilingan "Kiberxavfsizlik to'g'risida"gi Qonun kiberhujumlarga qarshi kurashish, axborot infratuzilmasini himoya qilish va raqamli makonda xavfsizlikni ta'minlashning huquqiy asoslarini belgilaydi. Ushbu qonunga qo'shimcha ravishda, 2023-yildagi PQ-167-son

Prezident qarori va boshqa normativ-huquqiy hujjatlar axborot xavfsizligini mustahkamlash bo'yicha qo'shimcha chora-tadbirlarni o'z ichiga oladi. Kiberxavfsizlik sohasidagi institutsional tuzilmalar orasida Raqamli texnologiyalar vazirligi va "Kiberxavfsizlik markazi" davlat unitar korxonasi yetakchi o'rin tutadi. "Kiberxavfsizlik markazi" 2019-yil 14-sentabrdagi PQ-4452-son Prezident qaroriga muvofiq tashkil etilgan bo'lib, axborot xavfsizligiga tahdidlarni tahlil qilish, noqonuniy kirishning oldini olish, axborot-kommunikatsiya texnologiyalarini sertifikatlaydigan o'tkazish, davlat axborot tizimlari xavfsizligi siyosatini ishlab chiqishda ko'maklashish va foydalanuvchilarni kiber tahdidlar haqida xabardor qilish kabi vazifalarni bajaradi. Markaz telekommunikatsiyalar operatorlari va huquqni muhofaza qilish organlari bilan hamkorlikda kiberxavfsizlikni ta'minlashga qaratilgan samarali dasturiy-texnik yechimlar bo'yicha tavsiyalar ishlab chiqadi. Amaliy choralar doirasida kiberhujumlarni aniqlash va bartaraf etish tizimlari joriy etilmoqda, ayniqsa muhim axborot infratuzilmasi obyektlari, masalan, davlat axborot tizimlari va bank sektoridagi raqamli platformalar himoyasi ustuvor hisoblanadi. Zamonaviy dasturiy yechimlar va xavfsizlik devorlari orqali raqamli infratuzilmaning barqaror ishlashi ta'minlanmoqda. Biroq, tizim bir qator kamchiliklarga ega. Malakali mutaxassislarning yetishmasligi tezkor va samarali choralar ko'rishni qiyinlashtirsa, xalqaro hamkorlikning cheklanganligi global kiberxavfsizlik standartlarini joriy etishni sekinlashtirmoqda. Bundan tashqari, qonunchilikning yangi tahdidlarga, masalan, sun'iy intellekt asosidagi hujumlar yoki blokcheyn tizimlariga qarshi xatarlarga moslashuvchanligi past bo'lib, bu kiberxavfsizlik tizimining umumiy samaradorligiga ta'sir qiladi. Ushbu muammolar

O'zbekistonning kiberxavfsizlik sohasida xorijiy tajribalarni o'rganish va qo'llash zarurligini ta'kidlaydi.

Xorijiy davlatlarda kiberxavfsizlikni tartibga solish global raqamli tahdidlarga qarshi turishda muhim tajribalarni namoyon qiladi. AQShda kiberxavfsizlik NIST Cybersecurity Framework va CISA (Cybersecurity and Infrastructure Security Agency) qonunlari orqali boshqariladi, bu tizimlar xususiy sektor bilan yaqin hamkorlik va global standartlarni ishlab chiqish imkonini beradi. Yevropa Ittifoqi GDPR (General Data Protection Regulation) va NIS Directive (Network and Information Security) kabi qonunlar orqali shaxsiy ma'lumotlarni himoya qilish va tarmoq xavfsizligini ta'minlaydi, bu esa xalqaro hamkorlikni rivojlantirishga xizmat qiladi. Rossiyada "Axborot xavfsizligi to'g'risida"gi Federal qonun va Roskomnadzor faoliyati kiberxavfsizlikni davlat nazorati ostida olib boradi, bu esa tizimning mustahkamligini ta'minlaydi. Xitoyda 2017-yildagi Cybersecurity Law va Data Security Law raqamli infratuzilmani markazlashgan boshqaruvga asoslaydi, bu esa tezkor choralar ko'rishni osonlashtiradi. Ushbu tizimlarning afzalliklari orasida AQShning xususiy sektor bilan hamkorligi, Yevropa Ittifoqining shaxsiy ma'lumotlarni himoya qilishdagi yuqori standartlari, Rossiyaning davlat nazoratining samaradorligi va Xitoyning markazlashgan boshqaruv tizimi alohida ajralib turadi. Biroq, kamchiliklar sifatida AQShda federal va shtat qonunchiligining murakkabligi, Yevropa Ittifoqida kichik bizneslar uchun qonun talablariga rioya qilishdagi qiyinchiliklar, Rossiyada shaxsiy erkinliklarga qo'yilgan cheklovlar va Xitoyda davlat senzurasining yuqori darajasi kiberxavfsizlik tizimlarining samaradorligiga muayyan darajada ta'sir qiladi.

Qiyosiy tahlil. O'zbekiston Respublikasi va xorijiy davlatlar (AQSh, Yevropa Ittifoqi, Rossiya, Xitoy) kiberxavfsizlikni tartibga solishda umumiy va

farqli yondashuvlarni namoyon qiladi. Umumiy jihat sifatida, barcha mamlakatlarda kiberxavfsizlik davlat siyosatining ustuvor yoʻnalishi sifatida qaraladi. Bu sohada muhim axborot infratuzilmasini, xususan, davlat axborot tizimlari, bank sektoridagi platformalar va energetika tarmoqlarini himoya qilishga alohida eʼtibor qaratiladi. Kiberxavfsizlikni taʼminlash uchun normativ-huquqiy bazalar ishlab chiqilgan boʻlib, ular kiberhujumlarni aniqlash, oldini olish va ularga qarshi choralar koʻrishni maqsad qiladi. Biroq, tizimlar oʻrtasida sezilarli farqlar mavjud. Oʻzbekistonda kiberxavfsizlik qonunchiligi, masalan, 2022-yildagi “Kiberxavfsizlik toʻgʻrisida”gi Qonun bilan yangi shakllanmoqda va rivojlanish bosqichida turibdi. Xorijiy davlatlarda, ayniqsa AQSh va Yevropa Ittifoqida, koʻp yillik tajribaga asoslangan murakkab huquqiy tizimlar mavjud boʻlib, ular global kiber tahdidlarga moslashgan. Masalan, AQShning NIST Cybersecurity Framework va CISA qonunlari xususiy sektor bilan yaqin hamkorlikka asoslanadi, bu esa innovatsion yechimlar va global standartlarni ishlab chiqishda muhim rol oʻynaydi. Yevropa Ittifoqining GDPR va NIS Directive kabi qonunlari shaxsiy maʼlumotlarni himoya qilishda yuqori standartlarni oʻrnatib, xalqaro hamkorlikni rivojlantiradi. Rossiyada “Axborot xavfsizligi toʻgʻrisida”gi Federal qonun davlat nazoratiga asoslangan boʻlib, markazlashgan boshqaruvni taʼminlaydi. Xitoyning 2017-yildagi Cybersecurity Law va Data Security Law raqamli infratuzilmani qatʼiy davlat boshqaruvi ostida himoya qiladi.

Oʻzbekistonda kiberxavfsizlik tizimi asosan davlat boshqaruviga tayanadi, bu esa tezkor qaror qabul qilishni osonlashtirsa-da, xususiy sektorning ishtiroki va xalqaro hamkorlikning cheklanganligi rivojlanishni sekinlashtiradi. Xorijiy davlatlarda, xususan AQSh va Yevropa Ittifoqida, xususiy sektorning faol ishtiroki va xalqaro tashkilotlar bilan hamkorlik kiberxavfsizlik tizimlarini yanada

moslashuvchan va samarali qiladi. Shaxsiy ma'lumotlarni himoya qilish bo'yicha Yevropa Ittifoqining tajribasi global miqyosda yetakchi hisoblanadi, O'zbekistonda esa bu soha hali rivojlanish bosqichida. Rossiya va Xitoyning markazlashgan tizimlari tezkor choralar ko'rishda afzallik bersa-da, shaxsiy erkinliklar va axborot erkinligiga qo'yilgan cheklovlar tizimning ochiqligini pasaytiradi.

O'zbekiston uchun xorijiy tajribalardan foydalanish kiberxavfsizlik tizimini mustahkamlashda muhim ahamiyatga ega. Yevropa Ittifoqining GDPR asosidagi shaxsiy ma'lumotlarni himoya qilish standartlari O'zbekiston qonunchiligini shaxsiy ma'lumotlar xavfsizligi bo'yicha takomillashtirishda yo'l-yo'riq bo'lishi mumkin. AQShning xususiy sektor bilan hamkorlik tajribasi, xususan, kiberxavfsizlik sohasida startaplar va innovatsion kompaniyalarni jalb qilish modeli, O'zbekistonda xususiy sektor ishtirokini oshirish uchun foydali bo'ladi. Bundan tashqari, ITU va ISO kabi xalqaro tashkilotlar bilan hamkorlikni kengaytirish O'zbekistonni global kiberxavfsizlik standartlariga yaqinlashtiradi va yangi tahdidlarga qarshi kurashda tajriba almashish imkonini beradi. Ushbu tajribalar O'zbekistonning kiberxavfsizlik tizimini zamonaviy talablarga moslashtirish va raqamli iqtisodiyotni xavfsiz rivojlantirishda muhim hissa qo'shadi.

Jadval 1

Kiberxavfsizlik sohasidagi qiyosiy tahlil natijalari

Davlat	Umumiy jihatlar	Farqlar	O'zbekiston uchun foydali tajribalar
O'zbekiston	Kiberxavf	Qonunchil	-

on	sizlik davlat siyosatining muhim qismi, infratuzilma himoyasi ustuvor.	ik yangi, davlat boshqaruvi ustun, xususiy sektor ishtiroki cheklangan.	
AQSh	Kiberxavf sizlik davlat siyosatining muhim qismi, infratuzilma himoyasi ustuvor.	Ko'p yillik tajriba, xususiy sektor ishtiroki katta, global standartlar ishlab chiqish.	Xususiy sektor bilan hamkorlik modeli.
Yevropa Ittifoqi	Kiberxavf sizlik davlat siyosatining muhim qismi, infratuzilma himoyasi ustuvor.	Shaxsiy ma'lumotlarni himoya qilishda ilg'or, xalqaro hamkorlik kuchli.	GDPR asosidagi shaxsiy ma'lumotlarni himoya qilish standartlari.
Rossiya	Kiberxavf sizlik davlat siyosatining muhim qismi, infratuzilma himoyasi ustuvor.	Davlat nazorati kuchli, shaxsiy erkinliklarga cheklovlar mavjud.	-
Xitoy	Kiberxavf sizlik davlat	Markazlas hgan boshqaruv,	-

	siyosatining muhim qismi, infratuzilma himoyasi ustuvor.	davlat senzurasining yuqori darajasi.	
Xalqaro hamkorlik	-	-	ITU, ISO bilan hamkorlikni kengaytirish.

Xulosa. Ushbu tadqiqot O‘zbekiston Respublikasi va xorijiy davlatlar (AQSh, Yevropa Ittifoqi, Rossiya, Xitoy) kiberxavfsizlikni tartibga solish tizimlarini qiyosiy tahlil qildi. O‘zbekistonda kiberxavfsizlik qonunchiligi rivojlanish bosqichida bo‘lib, davlat boshqaruvi asosida muhim axborot infratuzilmasini himoya qilishga qaratilgan. Xorijiy davlatlarda esa ko‘p yillik tajribaga asoslangan tizimlar, xususiyl sektor ishtiroki va xalqaro hamkorlik kiberxavfsizlikni yanada samarali qiladi. Yevropa Ittifoqining shaxsiy ma’lumotlarni himoya qilish tajribasi va AQShning xususiyl sektor bilan hamkorligi O‘zbekiston uchun muhim saboqlar beradi. Tadqiqot shuni ko‘rsatdiki, O‘zbekiston kiberxavfsizlik tizimini mustahkamlash uchun qonunchilikni takomillashtirishi, xalqaro hamkorlikni kengaytirishi va xususiyl sektor ishtirokini oshirishi zarur. Ushbu choralar zamonaviy kiber tahdidlarga qarshi turish va raqamli iqtisodiyotni xavfsiz rivojlantirishda muhim ahamiyatga ega bo‘ladi.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasining Qonuni, 15.04.2022 yildagi O‘RQ-764-son.
2. O‘zbekiston Respublikasi davlat xavfsizlik xizmati raisining buyrug‘i, 22.09.2023 yilda ro‘yxatdan o‘tgan, ro‘yxat raqami 3458.

3. O‘zbekiston Respublikasi Prezidentining qarori, 14.09.2019 yildagi PQ-4452-son.
4. Постановление Правления Центрального банка Республики Узбекистан, зарегистрировано 25.04.2023 г., рег. номер 3429.
5. European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
6. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
7. H.R.3359 - 115th Congress (2017-2018): Cybersecurity and Infrastructure Security Agency Act of 2018. (2018, ноябрь 16). <https://www.congress.gov/bill/115th-congress/house-bill/3359>.
8. Federal Law of the Russian Federation No. 149-FZ “On Information, Information Technologies and Information Protection”. (2006). Russian Federation Official Gazette. http://www.consultant.ru/document/cons_doc_LAW_61798/.