ZAMONAVIY HUQUQSHUNOSLIKNING AKTUAL MUAMMOLARI

XIII-RESPUBLIKA ILMIY-AMALIY KONFERENSIYA

YAKUNLARI BO'YICHA ILMIY ISHLAR TO'PLAMI

Issue - 2(2025) Available at www.uznauka.uz

FUQAROLIK HUQUQIDA INSHOOTLAR INFRATUZILMASI KIBERHAVFSIZLIGINING NAZARIY ASOSLARI

Saidov Baxodirxo‘ja Nosirxo‘jayevich

O‘zbekiston Respublikasi Milliy gvardiyasi Qo‘rqilash bosh boshqarmasi Kiberxavfsizlik markazi yetakchi mutaxassisi

bahodirxujasaidov@gmail.com

Annotatsiya: *ushbu maqolada fuqarolik huquqi kontekstida kiberxavfsizlikning nazariy asoslarini o‘rganiladi. Raqamli texnologiyalarning jadal rivojlanishi bilan infratuzilma tizimlari kibertahdidlarga tobora zaiflashib bormoqda va bu xavflarni bartaraf etish uchun keng qamrovli huquqiy bazani talab qiladi. Maqolada nazorat qiluvchi organlarning roli va kiberxavfsizlik choralarini kuchaytirishda davlat va xususiy sektor o‘rtasidagi hamkorlikning ahamiyati muhokama qilinadi. Natijalar infratuzilma institutlarini kibertahdidlardan himoya qiluvchi va fuqarolik qonunchiligi standartlariga rioya etilishini ta’minlovchi mustahkam huquqiy strategiyalarni ishlab chiqishga kompleks yondashuv zarurligini ta’kidlaydi.*

Kalit so‘zlar: *kiberxavfsizlik, fuqarolik huquqi, infratuzilmani himoya qilish, huquqiy asoslar, ma’lumotlarni himoya qilish, risklarni boshqarish.*

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ ИНФРАСТРУКТУРЫ УКАЗАНИЯ В ГРАЖДАНСКОМ ПРАВЕ

Саидов Баходирходжа Насирходжаевич

Ведущий специалист Центра кибербезопасности Главного управления устрашения Национальной гвардии Республики Узбекистан

bahodirkhujasaidov@gmail.com

ZAMONAVIY HUQUQSHUNOSLIKNING AKTUAL MUAMMOLARI

XIII-RESPUBLIKA ILMIY-AMALIY KONFERENSIYA

YAKUNLARI BO'YICHA ILMIY ISHLAR TO'PLAMI

Issue - 2(2025) Available at www.uznauka.uz

Аннотация: *в данной статье исследуются теоретические основы кибербезопасности в контексте гражданского права. В условиях быстрого развития цифровых технологий инфраструктурные системы становятся все более уязвимыми для киберугроз и требуют комплексной правовой базы для устранения этих рисков. В статье рассматривается роль регулирующих органов и важность сотрудничества государственного и частного секторов в усилении мер кибербезопасности. Результаты подчеркивают необходимость комплексного подхода к разработке надежных правовых стратегий, которые защищают инфраструктурные учреждения от киберугроз и обеспечивают соблюдение стандартов гражданского права.*

Ключевые слова: *кибербезопасность, гражданское право, защита инфраструктуры, правовая база, защита данных, управление рисками.*

THEORETICAL BASICS OF CYBER SECURITY OF INFRASTRUCTURE INSTRUCTIONS IN CIVIL LAW

Saidov Bakhodirkhoja Nasirkhojaevich

The leading specialist of the Cyber Security Center of the Main Department of Intimidation of the National Guard of the Republic of Uzbekistan

bahodirkhujasaidov@gmail.com

Abstract: *this article explores the theoretical foundations of cyber security in the context of civil law. With the rapid development of digital technologies, infrastructure systems are becoming increasingly vulnerable to cyber threats and require a comprehensive legal framework to address these risks. The*

article discusses the role of regulatory bodies and the importance of cooperation between the public and private sectors in strengthening cyber security measures. The findings highlight the need for a comprehensive approach to developing robust legal strategies that protect infrastructure institutions from cyber threats and ensure compliance with civil law standards.

Keywords: *cyber security, civil law, infrastructure protection, legal framework, data protection, risk management.*

KIRISH

Kiber jinoyat haqiqiy hayotdagi jinoyatga o‘xshaydi. Farqi shundaki, u faqat virtual makonda yaratilgan. Biroq, bu haqiqiy hayotga ta’sir qilishi ma’lum. O‘zbekistonda raqamlashtirish ishlari o‘z samarasini berdi va ko‘plab ish joylarida ma’lumotlarni raqamli formatga o‘tkazish bo‘yicha faol ish olib borilmoqda. Bu esa odamlarning hayotini ancha yengillashtirdi: pul o‘tkazmasini amalga oshirish uchun davlat xizmatlari markazida navbatda turish va bankga borish shart emas. Ammo soddalashtirish bilan kiberjinoyatchilar tomonidan yangi tahdid paydo bo‘ldi. Bu tahdid kibertahdid deb ataladi. O‘zbekiston Respublikasida ham shu kungacha “Kiberxafvsizlik” masalasi bo‘yicha qonun hujjatlari yetarli darajada emas edi. Chunku bu tushuncha va bu kabi jinoyatlar yaqin o‘tgan yillarda juda avj olib ketdi. Shu sababli O‘zbekiston Respublikasida kiberxavfsizlik sohasidagi munosabatlarni tartibga solish, kiberjinoyatlarni oldini olish, kiberhujumdan himoyalanish maqsadida Oliy Majlis tomonidan “Kiberxafvsizlik to‘g‘risida”gi O‘zbekiston Respublikasi qonuni qabul qilindi. Jadal rivojlanayotgan texnologik taraqqiyot va raqamli infratuzilmaga tobora ortib borayotgan bir davrda

kiberxavfsizlikning ahamiyati shunchaki texnik qiyinchiliklardan oshib, dolzarb huquqiy muammoga aylandi. Shaharlar va davlatlar aqlli texnologiyalarni transport tizimlari, energiya tarmoqlari va aloqa tarmoqlari kabi muhim infratuzilmalariga integratsiyalashgani sari kibertahdidlar bilan bog‘liq zaifliklar eksponensial ravishda oshib bordi. Ushbu evolyutsiya fuqarolik huquqi doirasida kiberxavfsizlikning murakkabliklarini hal qilish uchun keng qamrovli huquqiy bazalarning shoshilinch zarurligini ta’kidlaydi. Ushbu maqola infratuzilma institutlarida qo‘llaniladigan kiberxavfsizlikning nazariy asoslarini o‘rganish, mavjud fuqarolik huquqi tamoyillarini kiberxavflardan himoya qilish uchun qanday moslashtirilishi mumkinligini o‘rganishga qaratilgan.[1]

ASOSIY QISM

Kibertahdid - bu ijtimoiy tarmoqlardagi shaxsiy sahifani buzishdan tortib katta ma’lumotlarni o‘g‘irlashgacha bo‘lgan har qanday noqonuniy faoliyat hisoblanadi. Kiberjinoyatchilar maxsus virus dasturlari yordamida mobil telefon yoki kompyuter kabi har qanday qurilmaga buzib kirishi mumkin. Agar foydalanuvchi litsenziyasiz dasturni o‘rnata va zararli virusli shubhali saytlardan fayllarni yuklab olsa, jinoyatchilar uchun ma’lumotlaringizni olish qiyin bo‘lmaydi. Bunday hujumlar shaxsiy hisoblarda ham, shaxsiy brendlarda ham amalga oshirilishi mumkin. Bunga asosan jamoat arboblari ta’sir qiladi. Kiberjinoyatchilar ko‘pincha yirik kompaniyalarga hujum qilishadi. U yerdan ular mijozlar ma’lumotlar bazalarini yoki boshqa ma’lumotlarni o‘g‘irlashadi va keyin o‘z maqsadlari uchun foydalanadilar. Boshqa kiberfiribgarlar tajribasiz

[1] Andress, J. (2014). The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Syngress.

foydalanuvchilardan pul undirishlari, karta yegasining ruxsatisiz pul o‘tkazishlari va ba’zan hatto onlayn xaridlarni ham amalga oshirishlari mumkin. Securing Sam ma’lumotlariga ko‘ra, IP kameralar uy tarmoqlarida o‘rnatilgan zaif qurilmalarning 47 foizini tashkil qiladi. Ularga qaratilgan hujumlar juda xavflidir. Eng zaif himoyaga ega qurilmalar orasida ikkinchi o‘rin ma’lumotlarni saqlash qurilmalari hisoblanadi.

Bugungi raqamli asrda kiberxavfsizlik milliy xavfsizlik, iqtisodiy barqarorlik va jamoat xavfsizligining asosi sifatida maydonga chiqdi. Jamoat infratuzilmasi va muhim tizimlarni jadal raqamlashtirish sharoitida ushbu sohalarni tartibga soluvchi huquqiy bazalar kiber tahdidlarning rivojlanayotgan manzarasiga moslashishi kerak. Fuqarolik huquqi infratuzilmani boshqarish bilan shug‘ullanuvchi tashkilotlarning mas'uliyati va majburiyatlarini belgilashda hal qiluvchi rol o‘ynaydi. Kiberxavfsizlik tizimlar, tarmoqlar va ma’lumotlarni xakerlik, viruslar va ma’lumotlar buzilishi kabi kibertahdidlardan himoya qilishga mo‘ljallangan amaliyotlar, texnologiyalar va jarayonlarni anglatadi. Uning ahamiyatini oshirib bo‘lmaydi, ayniqsa muhim infratuzilmaga taalluqli bo‘lgan tarmoqlar, agar buzilgan bo‘lsa, aholi salomatligi, xavfsizligi va iqtisodiy barqarorlik uchun halokatli oqibatlarga olib kelishi mumkin. Ushbu tarmoqlarga kommunal xizmatlar, transport, aloqa va favqulodda vaziyatlarda javob berish tizimlari kiradi. Ushbu sektorlar o‘rtasidagi o‘zaro bog‘liqlik potentsial xavflarni yanada kuchaytiradi va mustahkam kiberxavfsizlik tizimini zarur qiladi.[2]

Xavfsizlik masalasi haqida gapirganda, biz birinchi navbatda “urush” tushunchasini tasavvur qilamiz. Pulemyot ko‘targan ba’zi dahshatga tushgan

[2] Amoroso, E. G., & Amoroso, E. (2012). Cyber attacks: protecting national infrastructure. Elsevier.

askarlar bostirib kirganday vahima bor. Darhaqiqat, hozir bunday urushlarsiz tinch davr tug‘ilgandek tuyulishi mumkin. Hech kim beshta to‘pponchasini osmaydi, tanklarini gurillatadi, samolyotlari bilan bombardimon qiladi, chegaramizni buzmaydi, aralashmaydi. Ammo bu biz dushmanlardan butunlay ozodmiz, degani emas. Bugun biz tinch-totuv yashayapmiz, ammo qurolsiz jang davom etmoqda. Hozirgi urush oldingi urushdan farq qiladi. Bugungi dunyo axborot urushi davrida yashamoqda Yangi davr kompyuter, axborot va tarmoq “urush”ining asosiy xususiyati shundaki, u orqa va frontga bo‘linmaydi, chegaralari yo‘q. Shu sababli, an’anaviy urushlarga qaraganda kamroq pul sarflansa-da, xavf va oqibatlar juda katta. Sababi, bu urushda inson bolasi tez-tez otib ketadi, shahid bo‘ladi, yarador bo‘ladi, nogiron bo‘lib qolmasa ham, avvalgidan ham xavfliroqdir. Tan yarasini davolasa bo‘ladi, lekin ruh va aqli zaiflarning yaralarini davolash jamiyat uchun juda qimmatga tushishini boshidan tushunishimiz kerak. Zamonaviy axborot texnologiyalari ko‘plab afzallik va afzalliklarga ega. Keling, avval uni sanab o‘tamiz: Birinchidan, tezkorlik, ikkinchidan, iqtisodiy samaradorlik va tejamkorlik, uchinchidan, uzoq masofadan xizmat ko‘rsatish qobiliyati, to‘rtinchidan, axborotni tarqatish va qabul qilishning yaxlitligi, beshinchidan, axborotdan foydalanish imkoniyati, uni iste’mol qilish imkoniyatlarining keng doirasi va boshqalar. Bunday afzallik va afzalliklarga qaramay, axborot texnologiyalari orqali amalga oshirilayotgan turli davlat xizmatlari ham jiddiy xavflarni keltirib chiqaradi. Shu sababli jamiyatda foydali faoliyat ritmini ta’minlash, yuzaga kelishi mumkin bo‘lgan yo‘qotish va zararlarni kamaytirish, investitsiya samaradorligi va tadbirkorlik imkoniyatlarini kengaytirish maqsadida turli axborot tahdidlari va muammolaridan himoyalanish zarurati paydo bo‘ldi. Umuman olganda, biz hozir

shunday murakkab davrda yashayapmizki, axborot tahdidini chetlab o‘tib bo‘lmaydi. Eng muhimi, shaxsiy kompyuteringizdagi muhim ma’lumotlaringiz o‘chirilsa, nafaqat sizga, balki jamoangizga va boshqa tegishli muassasalarga ham ta’sir qiladi, va agar davlat boshqaruv organlaridan biri bunday holatga tushib qolsa, uning barcha tuzilmalari katta qiyinchiliklarga duch keladi. Mamlakatning asosiy muammolarini hal qiladigan avlod qurilmalaridan ma’lumotlarni o‘g‘irlash va o‘chirish hatto favqulodda hodisa deb hisoblanadi. Chunki bunday holat davlat manfaatlariga, milliy xavfsizlikka, mustaqillik va muxtoriyatga jiddiy zarar yetkazadi. Shuning uchun ma’lumot ishning normalligini muvofiqlashtiruvchi asosiy kapital, shuningdek, ma’lum bir tashkilotning qimmatli mulki va jihozlari hisoblanadi, shuning uchun uni himoya qilish kerak. Ilgari biz ma’lumotlarni qog‘ozga yozib, saqlagan va boshqalarga tarqatganmiz. Hozirgi kunda kompyuterlar va internet tarmoqlaridan keng foydalanish uni elektron, onlayn resurs sifatida saqlash va tarqatish imkonini berdi. Bugungi axborot tizimi juda murakkab va sintetik, shuning uchun u ba’zan inson omilidan tashqari tahdidlarni keltirib chiqaradi. Internet zamonaviy dunyo davlatlarining aloqa va aloqa vositasi bo‘lgani uchun millionlab katta va kichik tizimlar o‘zaro ro‘yxatdan o‘tgan va unga ulangan. Natijada ko‘p vaqt va mablag‘ tejalgan bo‘lsa-da, jinoyatchilarga jinoiy yo‘l bilan daromad olish imkonini ham beradi. Shuningdek, vayronagarchilikka olib keladigan zararli dasturlar Internetda keng tarqalmoqda. Internetda milliy chegaralar va cheklovlar mavjud emasligi sababli, axborot xavfsizligi muammosi nafaqat guruh, mintaqa, qit’a yoki alohida davlat muammosidir. Darhaqiqat, bu global muammoga aylandi. Kompyuter va axborot-tarmoq urushining oqibatlariga kelsak, bu tabiiy ofatdan kam emas. Buni hatto

atom, yadroviy ommaviy qirg‘in qurollari tahdidi bilan solishtirish mumkin. Biz bilamizki, axborot harbiy qo‘mondonlik uchun havo kabi muhim. Agar hech qanday ma’lumot bo‘lmasa, beshta qurolga ega bo‘lgan hech qanday buyuk jamoa chig‘anoq qila olmaydi. Agar shunday bo‘lsa, kompyuter, axborot va tarmoq tizimidagi xavfsizlik masalasi mudofaa sohasida katta o‘rin egallaydi. Yangi asrda fan va texnika birgalikda taraqqiyotning yuksak marralarini zabt etdi. Muloqot, axborot almashish imkoniyati va tezligi maksimal darajada oshdi, ko‘rinmas bahaybat olam esa imkon qadar kaftimizda “kichraytirildi”. Natijada davlatlararo va millatlararo munosabatlar imkon qadar mustahkamlandi.

Jismoniy shaxslar va tashkilotlar o‘rtasidagi huquqiy munosabatlarni o‘z ichiga olgan fuqarolik qonunchiligi kiberxavfsizlik bilan bog‘liq javobgarlik va ehtiyot bo‘lish majburiyatlarini belgilash asoslarini belgilaydi. Ushbu sohada bir nechta asosiy tushunchalarni, jumladan, beparvolik, qat’iy javobgarlik va g‘amxo‘rlik vazifasini o‘rganish kerak. Ularning har biri kiberxavfsizlikdagi nosozliklar uchun javobgarlikni belgilovchi hal qiluvchi rol o‘ynaydi. Mas'uliyat fuqarolik huquqining asosiy printsipi bo‘lib, kiberxavfsizlikning buzilishi natijasida etkazilgan zarar uchun kim javobgar bo‘lishini belgilaydi. Umuman olganda, javobgarlikni ikki turga bo‘lish mumkin: beparvolik va qat’iy javobgarlik.

1. Beparvolik: Kiberxavfsizlik kontekstida beparvolik tashkilot o‘z tizimlarini kibertahdidlardan himoya qilish uchun oqilona choralar ko‘rmaganida yuzaga keladi. Beparvolikni aniqlash uchun uchta asosiy elementni isbotlash kerak: ehtiyot bo‘lish, majburiyatni buzish va sabablar. Misol uchun, agar muhim infratuzilma provayderi tegishli xavfsizlik choralarini qo‘llashni e’tiborsiz qoldirsa va ma’lumotlar buzilishiga duchor bo‘lsa, zarar ko‘rgan tomonlar tashkilot o‘z

g‘amxo‘rlik majburiyatini buzgan deb da’vo qilishi mumkin, bu esa keyingi zararga olib keladi

2. Kuchaytirilgan javobgarlik: Ba’zi hollarda, tashkilot aybi yoki niyatidan qat’i nazar, kiber hodisalar uchun qat’iy javobgarlikka tortilishi mumkin. Bu, ayniqsa, zarar etkazish xavfi yuqori bo‘lgan sohalarda qo‘llaniladi. Misol uchun, agar energiya provayderi operatsiyalarni to‘xtatib qo‘yadigan va jamoat zarariga olib keladigan kiberhujumga duchor bo‘lsa, qat’iy javobgarlik tashkilotning profilaktika choralaridan qat'i nazar, javobgar bo‘lishini ta’minlashi mumkin.[3]

2020-yil boshida internetdagi barcha ma’lumotlar hajmi 44 zettabaytga yetdi. Hisob-kitoblarga ko‘ra, 2025-yilga borib har kuni ishlab chiqariladigan ma’lumotlar hajmi 463 ekzabaytga yetadi. Biroq ekspertlar ommaviy axborot vositalariga bosim o‘tkazilayotganidan xavotirda. Chunki “Radio Television Gonkong” tahririyati prodyuseri 2019-yildagi qo‘zg‘olon haqida reportaj tayyorlash vaqtida yo‘l harakati qoidalarini buzganlikda ayblanib, javobgarlikka tortildi. Bundan tashqari, matbuot erkinligini targ‘ib qiluvchi “Chegara bilmas muxbirlar” xalqaro tashkiloti Gonkong OAV erkinligi bo‘yicha dunyoning 180 mamlakati orasida 80-o‘rinni egallab turgani va natija qoniqarli emasligini anglatishini ma’lum qildi. Mamlakatimizda axborot jamiyatini barpo etish jarayoni sharoitida axborot kommunikatsiya texnologiyalari jamiyat hayotining har qanday sohasining asosiy o‘zagiga aylanib bormoqda. Axborot kommunikatsiya texnologiyalari siyosiy tizimning qon tomirlariga o‘xshab, uning tarkibiy qismlari va elementlarini oziqlantiradi, ularning o‘zaro aloqasi va

[3] Alpcan, T., & Başar, T. (2010). Network security: A decision and game-theoretic approach. Cambridge University Press.

harakatini ta’minlaydi. Boshqacha aytganda, siyosiy tizim va uning tarkibiy qismlarining to‘g‘ri ishlashi bevosita axborotning xolisligi, to‘g‘riligi va o‘z vaqtida yetkazilishiga bog‘liq. Binobarin, har qanday davlatda davlat boshqaruvi shakllaridan qat’i nazar, uning siyosiy tizimining barcha tarkibiy qismlarida (siyosiy institutlar, siyosiy munosabatlar, siyosiy norma va tamoyillar, siyosiy ong va siyosiy madaniyat) axborotning shakllantiruvchi, muvofiqlashtiruvchi, kommunikativ omil sifatidagi o‘rni alohida bo‘ladi va u bundan keyin ham rivojlanib boradi. Chunki axborot texnologiyalari, axborot tarqatishning yangi usullari, jumladan, bugungi kunda O‘zbekistonda rasman ommaviy axborot vositalariga tenglashtirilgan internet tarmog‘i rivojlanishi bilan siyosiy tizimning kommunikativ faoliyati jonlanadi. Davlat hokimiyati va boshqaruvi organlari ham ushbu yangiliklarga qiziqish bildirishdi, buning natijasida “elektron hukumat”, “elektron boshqaruv”, “elektron partiya”, “elektron universitet”, axborot-kommunikatsiya siyosati instituti kabi yangi loyihalar dunyoga keldi. Shu bilan birga, axborotni ishlab chiqarish va tarqatish jarayoni hamda kompyuter texnikasining jadal rivojlanishi davlat boshqaruvi tuzilmasi va mexanizmlariga sezilarli ta’sir ko‘rsatmoqda. Bugungi axborot oqimi doimiy kuchga aylandi, jahon axborot makonining shakllanayotgan sharoitida axborotning jamiyatdagi roli va o‘rni ayniqsa ortib bormoqda. Bu, o‘z navbatida, davlat, jamiyat va shaxslarning axborot xavfsizligini ta’minlash masalalarining murakkablashishiga xizmat qilmoqda.

Ma’lumotlarning buzilishi va shaxsiy daxlsizlikning buzilishi bilan bog‘liq tashvishlar ortib borayotganligi sababli, ma’lumotlarni himoya qilish to‘g‘risidagi qonunlar fuqarolik huquqida muhim o‘rin egalladi. Ushbu qonunlar

tashkilotlar shaxsiy va maxfiy ma’lumotlarni qanday yig‘ish, saqlash va qayta ishlashni boshqaradi. Ushbu qonunlarning kiberxavfsizlik bilan bog‘liqligi juda katta, chunki aksariyat kibertahdidlar bunday ma’lumotlarni nishonga oladi. Yevropa Ittifoqidagi umumiy ma’lumotlarni himoya qilish to‘g‘risidagi reglament (GDPR) kiberxavfsizlik bilan o‘zaro aloqada bo‘lgan ma’lumotlarni himoya qilish qonunchiligining yorqin namunasi bo‘lib xizmat qiladi. GDPRga muvofiq, tashkilotlar shaxsiy ma’lumotlarni himoya qilish uchun tegishli texnik va tashkiliy chora-tadbirlarni amalga oshirishlari shart. Bunga rioya qilmaslik jiddiy jazolarga olib kelishi mumkin, bu esa tashkilotlarning kiberxavfsizlikning mustahkam amaliyotlariga sarmoya kiritishiga kuchli turtki yaratadi.

Komplayens asoslari tashkilotlarga kiberxavfsizlik bilan bog‘liq qonuniy va tartibga soluvchi talablarga rioya qilishda yordam beradigan boshqaruv tuzilmalari sifatida ishlaydi. Fuqarolik qonunchiligi huquqiy tavakkalchiliklarni yumshatish uchun tashkilotlar rioya qilishlari kerak bo‘lgan qonuniy majburiyatlar orqali rioya qilishning asosiy darajasini belgilaydi.

1. Sanoat standartlari va qoidalari: Turli sohalar o‘zlarining kiberxavfsizlik standartlari va qoidalarini o‘rnatdilar. Masalan, Sog‘liqni saqlash sug‘urtasi portativligi va javobgarligi to‘g‘risidagi qonun (HIPAA) bemor ma’lumotlarini himoya qilish bo‘yicha tibbiyot xodimlariga maxsus talablarni qo‘yadi. Ushbu standartlarga rioya qilmagan tashkilotlar qonuniy oqibatlarga olib kelishi mumkin.

2. Ichki siyosat: Tashqi qoidalarga qo‘shimcha ravishda, tashkilotlarga fuqarolik huquqi tamoyillariga mos keladigan ichki kiberxavfsizlik siyosatini qabul qilish tavsiya etiladi. Ushbu siyosatlar hodisalarga javob berish, xodimlarni

o‘qitish va xavflarni baholash kabi sohalarni qamrab olishi kerak. Kuchli ichki siyosatga ega bo‘lgan tashkilotlar nafaqat kiberxavfsizlik holatini mustahkamlaydi, balki potentsial qonuniy da’volarga qarshi himoyasini ham kuchaytiradi.[4]

Fuqarolik huquqi doirasida kiberxavfsizlikning nazariy asoslari yaxshi yo‘lga qo‘yilgan bo‘lsa-da, ushbu qonunlarni qo‘llashda qiyinchiliklar mavjud. Muhim muammolardan biri texnologik o‘zgarishlarning tez sur'atidir. Kibertahdidlar qo‘rqinchli sur'atda rivojlanib, ko‘pincha qonun chiqaruvchilarning mavjud qonunlarni moslashtirish yoki yangi qoidalarni qabul qilish qobiliyatidan ustun turadi. Ushbu nomutanosiblik huquqiy himoyada bo‘shliqlarni keltirib chiqaradi va tashkilotlarni kiberhujumlarga qarshi himoyasiz qoldiradi. Bundan tashqari, yurisdiksiya masalalari kiberxavfsizlik qonunlarining bajarilishini murakkablashtiradi. Kiberhujumlar dunyoning istalgan joyidan kelib chiqishi mumkin, bu esa qaysi yurisdiktsiya qonunlari qo‘llanilishini aniqlashni qiyinlashtiradi. Ushbu murakkablik tashkilotlarga o‘zlarining huquqiy majburiyatlarini tushunish va potentsial majburiyatlarni boshqarishda qiyinchiliklar tug‘diradi.

Kiberxavfsizlik qonunchiligiga xos bo‘lgan muammolarni hal qilish uchun ko‘p qirrali yondashuv zarur. Manfaatdor tomonlar, jumladan, davlat idoralari, xususiy sektor tashkilotlari va huquq sohasi mutaxassislari o‘zgaruvchan texnologiyalar va tahdidlarga moslashish uchun yetarli darajada tezkor bo‘lgan keng qamrovli huquqiy bazani ishlab chiqish uchun hamkorlik qilishi kerak.

[4] Brands, S. (2000). Rethinking public key infrastructures and digital certificates: building in privacy. Mit Press.

1. Qonunchilikni isloh qilish: qonunchilikni uzluksiz isloh qilish texnologik taraqqiyot bilan hamnafas turish uchun zarur. Siyosatchilar mavjud qonunlarni yangilash va raqamli landshaft voqeligini aks ettiruvchi yangi qoidalarni yaratish uchun kiberxavfsizlik bo‘yicha ekspertlar va sanoat rahbarlari bilan hamkorlik qilishlari kerak.

2. Davlat-xususiy sheriklik: Davlat va xususiy sektor o‘rtasidagi hamkorlik kiberxavfsizlik bo‘yicha yanada samarali choralar ko‘rishga olib kelishi mumkin. Axborot almashish tashabbuslari tashkilotlarga bir-birining tajribasidan o‘rganish va potentsial tahdidlarga qarshi himoyasini kuchaytirishga yordam beradi.

3. Ta’lim: Tashkilotlar o‘rtasida kiberxavfsizlik xatarlari va qonuniy majburiyatlari haqida xabardorlikni oshirish juda muhimdir. O‘quv dasturlarini amalga oshirish faol choralar va qonunlar va qoidalarga rioya qilishni ta’kidlaydigan kiberxavfsizlik madaniyatini rivojlantirishi mumkin.

XULOSA

Bugungi kunda “Kiberxafvsizlik to‘g‘risida”gi O‘zbekiston Respublikasi qonunini amalga oshirishga alohida e’tibor qaratilmoqda. Cybershield - axborot xavfsizligi sohasida davlat organlari tomonidan amalga oshiriladigan chora-tadbirlar, apparat-dasturiy ta’minot tizimlari va loyihalari majmuidir. Mazkur dastur doirasida axborot-kommunikatsiya texnologiyalaridan xavfsiz foydalanishga qaratilgan chora-tadbirlar belgilangan. Infratuzilma institutlariga qarshi kibertahdidlarning ortib borayotgan chastotasi va murakkabligi kiberxavfsizlikni qamrab oluvchi mustahkam fuqarolik qonunchiligi bazasi zarurligini ta’kidlaydi. Ushbu maqola fuqarolik huquqi kontekstida

kiberxavfsizlikning nazariy asoslarini bayon qilib, javobgarlik, risklarni boshqarish va ma’lumotlarni himoya qilish kabi asosiy tamoyillarni yoritib beradi. Infratuzilma tizimlari rivojlanishda davom etar ekan, ularni boshqaradigan huquqiy yondashuvlar ham paydo bo‘ladigan xavflarni yumshatishda samarali bo‘lishini ta’minlashi kerak. Bundan tashqari, kiberxavfsizlik choralarini kuchaytiruvchi yaxlit strategiyalarni ishlab chiqish uchun davlat organlari, xususiy sektor sub'ektlari va yuridik amaliyotchilar o‘rtasidagi hamkorlikni rivojlantirish muhim ahamiyatga ega.

FOYDALANILGAN ADABIYOTLAR

1. Andress, J. (2014). The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Syngress.
2. Amoroso, E. G., & Amoroso, E. (2012). Cyber attacks: protecting national infrastructure. Elsevier.
3. Alpcan, T., & Başar, T. (2010). Network security: A decision and game-theoretic approach. Cambridge University Press.
4. Brands, S. (2000). Rethinking public key infrastructures and digital certificates: building in privacy. Mit Press.