

KIBERXAVFSIZLIK VA KRIPTOLOGIYANING IJTIMOIIY HAYOTDAGI MUAMMOLARI HAMDA HUQUQIY YECHIMLARI

I.A.Ismailov

Farg'ona davlat universiteti

Falsafa fanlari bo'yicha falsafa doktori (PhD)

Abdusalilova Nasibaxon Farhod qizi

Farg'ona davlat universiteti talabasi

Аннотация

Mazkur maqolada zamonaviy axborot texnologiyalari rivojlanishi sharoitida kiberxavfsizlik va kriptologiyaning jamiyat hayotidagi ahamiyati, mavjud muammolari hamda ularning huquqiy yechimlari tahlil qilinadi. Shuningdek, kiberjinoyatchilik, shaxsiy ma'lumotlarni himoya qilish, axborot xavfsizligini ta'minlash va xalqaro hamkorlik masalalari yoritilgan.

Kalit so'zlar: kiberxavfsizlik, kriptologiya, axborot xavfsizligi, kiberjinoyat, shaxsiy ma'lumotlar, internet xavfsizligi, raqamli texnologiyalar, huquqiy himoya.

Аннотация

В данной статье анализируются значение кибербезопасности и криптологии в условиях развития современных информационных технологий, существующие проблемы в общественной жизни, а также их правовые решения. Кроме того, рассматриваются вопросы киберпреступности, защиты персональных данных, обеспечения информационной безопасности и международного сотрудничества.

Ключевые слова: кибербезопасность, криптология, информационная безопасность, киберпреступность, персональные данные, интернет-безопасность, цифровые технологии, правовая защита.

Kirish

O'zbekiston Respublikasi Prezidenti Shavkat Mirziyoyev ta'kidlaganidek, "raqamli texnologiyalarni rivojlantirish va axborot xavfsizligini ta'minlash Yangi O'zbekiston taraqqiyotining muhim shartlaridan biri hisoblanadi"¹. Bu esa kiberxavfsizlik masalasining davlat siyosati darajasidagi dolzarb ahamiyatga ega ekanligini ko'rsatadi.

Shavkat Mirziyoyev o'z ma'ruzalarida yoshlarni axborot xurujlaridan himoya qilish², internet tarmog'ida xavfsiz muhitni shakllantirish va raqamli savodxonlikni oshirish masalalariga alohida e'tibor qaratib kelmoqda. Bu kiberxavfsizlik va

¹ O'zbekiston Respublikasi Prezidenti Sh.Mirziyoyevning 2018 yil 9 yanvardagi "Axborot-kommunikatsiya texnologiyalarini rivojlantirish va xavfsizligini ta'minlash"ga bag'ishlangan yig'ilishi // Prezident rasmiy veb-sayti. President.uz

² O'zbekiston Respublikasi Prezidenti Sh.Mirziyoyevning "Raqamli O'zbekiston – 2030" strategiyasini amalga oshirish bo'yicha videoselektor yig'ilishi // Kun.uz, 2021 йил 10 сентябрь. [Kun.uz](https://kun.uz) мақоласи

kriptologiya sohasini ilmiy-amaliy jihatdan tadqiq etishning dolzarbligini yanada oshiradi.

Kiberxavfsizlik va kriptologiya bilan bog'liq muammolarni yanada chuqurroq tahlil qilganda, raqamli jamiyat rivoji bilan birga yangi xavf turlari ham paydo bo'layotganini ko'rish mumkin. Masalan, so'nggi yillarda sun'iy intellekt asosidagi texnologiyalar keng qo'llanila boshladi va bu o'z navbatida yangi turdagi kiber tahdidlarni yuzaga keltirdi. Sun'iy intellekt yordamida avtomatlashtirilgan hujumlar, soxta axborotlar (deepfake) yaratish, foydalanuvchilarni aldash yanada osonlashdi. Bu esa jamiyatda axborot ishonchliligiga putur yetkazib, ijtimoiy beqarorlikka sabab bo'lishi mumkin.

Yana bir dolzarb muammo — raqamli suverenitet masalasidir. Davlatlar o'z axborot makonini himoya qilishga intilmoqda, chunki tashqi kiberhujumlar siyosiy va iqtisodiy barqarorlikka tahdid solishi mumkin. Shu sababli ayrim davlatlar milliy serverlar, yopiq tarmoqlar va ichki nazorat tizimlarini joriy etmoqda. Biroq bu jarayon ba'zida internet erkinligining cheklanishiga ham olib kelishi mumkin, bu esa inson huquqlari bilan bog'liq muammolarni yuzaga keltiradi.

O'rganilganlik darajasi

Kiberxavfsizlik va kriptologiya masalalari so'nggi yillarda xalqaro va milliy miqyosda keng tadqiq etilmoqda. Ayniqsa, raqamli texnologiyalarning jadal rivojlanishi natijasida axborot xavfsizligi, shaxsiy ma'lumotlarni muhofaza qilish, kiberjinoyatchilikka qarshi kurashish va elektron dalillardan foydalanish kabi masalalar ilmiy tadqiqotlarning muhim yo'nalishiga aylandi.

Xalqaro tadqiqotlarda kiberxavfsizlik davlat xavfsizligining tarkibiy qismi sifatida baholanib, kibermakondagi tahdidlarning transmilliy xususiyati alohida ta'kidlanadi³. Shuningdek, kriptologiya sohasida zamonaviy shifrlash algoritmlari, kvant kriptografiyasi va raqamli identifikatsiya tizimlarining huquqiy-axloqiy jihatlari keng tahlil qilingan⁴.

O'zbekistonda ham axborot xavfsizligi sohasida muayyan ilmiy va huquqiy asoslar shakllangan bo'lib, "Axborotlashtirish to'g'risida"gi Qonun, "Shaxsiy ma'lumotlar to'g'risida"gi Qonun, "Elektron hukumat to'g'risida"gi Qonun hamda Jinoyat kodeksida kiberjinoyatchilikka qarshi huquqiy mexanizmlar belgilangan⁵. Mahalliy tadqiqotlarda asosan axborot xavfsizligini ta'minlash, elektron davlat xizmatlari xavfsizligi, internet tarmog'ida shaxs huquqlarini himoya qilish va raqamli madaniyatni rivojlantirish masalalari yoritilgan⁶.

Shu bilan birga, kiberxavfsizlik va kriptologiya ijtimoiy hayotga ta'siri, kibernetika, deepfake texnologiyalari, sun'iy intellekt asosidagi kibertahdidlar va

³ William Stallings. *Cryptography and Network Security: Principles and Practice*. — Pearson Education, 2017.

⁴ Bruce Schneier. *Applied Cryptography*. — John Wiley & Sons, 2015.

⁵ O'zbekiston Respublikasining "Shaxsiy ma'lumotlar to'g'risida"gi Qonuni // Qonunchilik ma'lumotlari milliy bazasi.

⁶ Abduqodirov A.A. *Axborot xavfsizligi va kiberxavfsizlik asoslari*. — Toshkent: "Fan va texnologiya", 2021.

raqamli suverenitet muammolari yetarlicha kompleks tadqiq etilmagan. Mazkur maqola ana shu jihatlarni huquqiy va ijtimoiy nuqtai nazardan tahlil qilishi bilan ahamiyatlidir.

Tadqiqot metodologiyasi

Maqolani tayyorlashda umumilmiy va maxsus ilmiy tadqiqot usullaridan foydalanildi. Jumladan:

Tizimli tahlil usuli orqali kiberxavfsizlik va kriptologiya sohasidagi muammolarning o'zaro bog'liq jihatlari o'rganildi;

Qiyosiy-huquqiy tahlil usuli yordamida milliy va xalqaro qonunchilik normalari taqqoslandi;

Mantiqiy tahlil usuli asosida kiberjinoyatchilik, raqamli tahdidlar va huquqiy yechimlar o'rtasidagi sabab-oqibat munosabatlari yoritildi;

Sotsiologik yondashuv orqali raqamli madaniyat, internetdan foydalanish odatlari va inson omilining kiberxavfsizlikka ta'siri tahlil qilindi;

Prognostik usul vositasida sun'iy intellekt va kvant texnologiyalari rivojlanishi bilan bog'liq kelajakdagi kibertahdidlar baholandi.

Tadqiqotning nazariy asosini axborot xavfsizligiga oid milliy qonunchilik hujjatlari, xalqaro tashkilotlar materiallari, ilmiy maqolalar va zamonaviy kiberxavfsizlik konsepsiyalari tashkil etdi.

O'rganishlarimiz shuni ko'rsatadiki, Raqamli iqtisodiyot rivojlanishi bilan elektron tijorat va onlayn to'lov tizimlari kengaymoqda. Bu esa moliyaviy firibgarliklarning yangi shakllarini paydo qilmoqda. Masalan, bank kartalari ma'lumotlarini o'g'irlash, soxta to'lov sahifalari orqali pul yechib olish kabi jinoyatlar keng tarqalgan. Bu holat nafaqat alohida shaxslar, balki yirik biznes subyektlariga ham zarar yetkazadi.

Shuningdek, "inson omili" bilan bog'liq muammolar ham muhim hisoblanadi. Ko'pincha kiberhujumlar texnik zaiflikdan emas, balki insonlarning ehtiyotsizligi yoki bilim yetishmasligi sababli amalga oshiriladi. Oddiy parollar qo'llash, noma'lum havolalarni ochish, shubhali fayllarni yuklab olish kabi holatlar xavfsizlik tizimini zaiflashtiradi. Demak, texnologiya qanchalik rivojlangan bo'lmasin, inson omili doimo asosiy xavf manbalaridan biri bo'lib qoladi.

Kriptologiya nuqtai nazaridan esa yana bir muammo — bu shifrlash texnologiyalarining noto'g'ri yoki noqonuniy maqsadlarda qo'llanishidir. Jinoyatchilar ham kuchli shifrlashdan foydalanib, o'z faoliyatini yashirishga harakat qilmoqda. Bu esa huquqni muhofaza qiluvchi organlar uchun qo'shimcha qiyinchiliklar tug'diradi. Shu sababli ayrim davlatlar shifrlashni tartibga solish yoki nazorat qilishga intilmoqda, lekin bu masalada xavfsizlik va shaxsiy erkinlik o'rtasida muvozanatni topish oson emas.

Huquqiy yechimlar tizimida yana bir muhim yo'nalish — bu raqamli dalillarni to'plash va ulardan sud jarayonlarida foydalanish masalasidir. Kiberjinoyatlarni tergov qilishda elektron izlar, log fayllar, IP manzillar kabi ma'lumotlar muhim rol o'ynaydi. Biroq ularni to'g'ri yig'ish, saqlash va sudda isbot sifatida qo'llash uchun aniq protsessual qoidalar talab etiladi.

Bundan tashqari, davlat va xususiy sektor o'rtasidagi hamkorlikni rivojlantirish ham muhim hisoblanadi. Ko'plab kiberinfratuzilmalar xususiy kompaniyalar qo'lida bo'lganligi sababli, ularning davlat bilan hamkorligi xavfsizlikni ta'minlashda hal qiluvchi ahamiyatga ega. Axborot almashinuvi, birgalikda xavfsizlik choralari ishlab chiqish va tezkor javob berish tizimlari bu borada samarali natija beradi.

Ta'lim tizimida ham kiberxavfsizlikka alohida e'tibor qaratilishi lozim. Maktabdan boshlab o'quvchilarga internetdan xavfsiz foydalanish, shaxsiy ma'lumotlarni himoya qilish, kiber tahdidlardan himoyalanih usullari o'rgatilishi zarur. Oliy ta'limda esa chuqur texnik bilimlar bilan bir qatorda huquqiy va etik masalalar ham o'qitilishi kerak.

Yana bir muhim yo'nalish — bu kiberetika masalasidir. Raqamli muhitda insonlarning o'zini tutishi, boshqalarga nisbatan hurmat bilan munosabatda bo'lishi, axborotdan mas'uliyatli foydalanishi muhim ahamiyatga ega. Kiberbulling, soxta axborot tarqatish, boshqalarning shaxsiy hayotiga aralashish kabi holatlar jamiyatda salbiy muhitni shakllantiradi. Kiberxavfsizlik va kriptologiya zamonaviy axborot jamiyatining eng muhim va dolzarb yo'nalishlaridan biri hisoblanadi. Raqamli texnologiyalar hayotning barcha sohalariga chuqur kirib borganligi sababli axborotlarni himoya qilish, shaxsiy ma'lumotlar xavfsizligini ta'minlash va davlat axborot tizimlarini asrash masalalari tobora muhim ahamiyat kasb etmoqda. Kiberxavfsizlik axborot tizimlari va tarmoqlarni turli tahdidlardan himoya qilishni ifodalasa, kriptologiya esa axborotni shifrlash va uni ruxsatsiz kirishdan saqlash usullarini o'rganadi.

Ijtimoiy hayotdagi asosiy muammolardan biri shaxsiy ma'lumotlarning himoyasizligi hisoblanadi. Internet va ijtimoiy tarmoqlardan foydalanuvchilar o'z ma'lumotlarini turli platformalarda qoldiradi va bu ma'lumotlar ba'zan noqonuniy ravishda o'g'irlanadi yoki tarqatiladi. Bu esa identifikatsiya o'g'irlanishi, firibgarlik va moliyaviy zarar kabi salbiy oqibatlariga olib keladi. Yana bir muammo kiberjinoyatchilikning tez rivojlanishidir. Xakerlik hujumlari, phishing, viruslar va zararli dasturlar nafaqat oddiy foydalanuvchilar, balki yirik tashkilotlar va davlat tizimlariga ham katta zarar yetkazmoqda.

Ijtimoiy tarmoqlarda soxta axborotlarning tarqalishi, kiberbulling va shaxsiy hayotga aralashish holatlari ham dolzarb muammo hisoblanadi. Bu holatlar jamiyatda ishonch muhitini pasaytiradi va insonlarning psixologik holatiga salbiy ta'sir ko'rsatadi. Bundan tashqari, axborot savodxonligining yetarli emasligi ham

muammolardan biri bo'lib, ko'plab foydalanuvchilar kiberxavfsizlik qoidalariga rioya qilmaydi va bu ularni turli tahdidlarga nisbatan zaif qiladi.

Iqtisodiy jihatdan ham kiberxavfsizlik muammolari jiddiy oqibatlariga olib kelmoqda. Bank tizimlari, elektron to'lovlar va biznes platformalarga qilingan hujumlar katta moliyaviy yo'qotishlarga sabab bo'ladi. Davlat axborot tizimlariga qilingan kiberhujumlar esa milliy xavfsizlikka jiddiy tahdid soladi. Shu bilan birga, sun'iy intellekt texnologiyalarining rivojlanishi yangi turdagi xavflarni, jumladan deepfake va avtomatlashtirilgan kiberhujumlarni yuzaga keltirmoqda.

Kriptologiya sohasida esa shifrlash texnologiyalarining noto'g'ri ishlatilishi muammo hisoblanadi. Jinoyatchilar kuchli shifrlashdan foydalanib o'z faoliyatini yashirishga harakat qiladi, bu esa ularni aniqlash va nazorat qilishni qiyinlashtiradi. Bundan tashqari, inson omili ham muhim muammo bo'lib, ko'plab xavfsizlik buzilishlari foydalanuvchilarning ehtiyotsizligi, zaif parollar yoki shubhali havolalarga ishonishi sababli yuzaga keladi.

Ushbu muammolarni hal etishda huquqiy yechimlar muhim o'rin tutadi. Kiberjinoyatchilikka qarshi maxsus qonunlar qabul qilinib, axborot tizimlariga noqonuniy kirish, ma'lumotlarni o'g'irlash va zarar yetkazish uchun javobgarlik belgilangan. Shaxsiy ma'lumotlarni himoya qilishga oid qonunchilik fuqarolarning axborot daxlsizligini ta'minlashga xizmat qiladi. Bundan tashqari, elektron dalillarni sud jarayonida qo'llash va kiberjinoyatlarni tergov qilish bo'yicha huquqiy mexanizmlar ishlab chiqilgan.

Xalqaro hamkorlik ham juda muhim ahamiyatga ega, chunki kiberjinoyatlar ko'pincha davlat chegaralarini tan olmaydi. Shu sababli davlatlar o'rtasida axborot almashinuvi, qo'shma tergovlar va umumiy xavfsizlik standartlarini joriy etish zarur hisoblanadi. Ta'lim tizimida kiberxavfsizlik bo'yicha bilimlarni oshirish, aholining axborot savodxonligini kuchaytirish va kiberetika qoidalarini targ'ib qilish ham muhim profilaktik chora hisoblanadi. Kiberxavfsizlik va kriptologiya masalalari bugungi kunda faqat texnik soha doirasida emas, balki global ijtimoiy jarayonlarning muhim qismi sifatida ham qaralmoqda. Raqamli texnologiyalar tez rivojlanib borayotgan bir paytda yangi turdagi tahdidlar ham paydo bo'lmoqda va bu jamiyat hayotiga bevosita ta'sir ko'rsatmoqda.

Kiberxavfsizlikdagi muhim muammolardan biri — raqamli identifikatsiya tizimlarining zaifligi hisoblanadi. Ko'plab xizmatlar onlayn rejimga o'tgani sababli, foydalanuvchilarning shaxsini aniqlash va himoya qilish tizimlari doim ham yetarli darajada ishonchli emas. Bu esa noqonuniy kirish va akkauntlarni buzish holatlariga olib keladi.

Yana bir dolzarb muammo — ma'lumotlar bazalarining markazlashgan holda saqlanishidir. Katta hajmdagi ma'lumotlar bir joyda saqlanganda, ular kiberhujumlar

uchun asosiy nishonga aylanadi. Agar bunday tizimlar buzilsa, millionlab foydalanuvchilar ma'lumotlari xavf ostida qoladi.

Kriptologiya sohasida esa kvant hisoblash texnologiyalarining rivojlanishi yangi muammo sifatida ko'rilmoqda. Kelajakda kvant kompyuterlar mavjud shifrlash algoritmlarini buzishi mumkinligi sababli, yangi turdagi kriptografik tizimlarni yaratish zarurati tug'ilmoqda.

Ijtimoiy jihatdan yana bir muammo — raqamli ishonch inqirozidir. Internetda yolg'on axborotlar, manipulyatsiya va soxta yangiliklarning ko'payishi natijasida odamlar haqiqiy va noto'g'ri axborotni ajratishda qiyinchilikka duch kelmoqda. Bu esa jamiyatda ishonchsizlikni kuchaytiradi.

Bundan tashqari, korporativ kiberxavfsizlik muammosi ham dolzarbdir. Yirik kompaniyalar va tashkilotlar o'z tizimlarini to'liq himoya qila olmasligi natijasida biznes ma'lumotlar sizib chiqishi holatlari ko'paymoqda. Bu esa raqobat va iqtisodiy barqarorlikka salbiy ta'sir ko'rsatadi.

Huquqiy jihatdan esa eng katta muammo — qonunchilikning texnologik rivojlanishdan ortda qolishidir. Kiberjinoyatchilik tez yangilanib boradi, lekin huquqiy normalar har doim ham bu o'zgarishlarga tez moslasha olmaydi. Shu sababli yangi turdagi jinoyatlar huquqiy bo'shliqlardan foydalanishi mumkin.

Shuningdek, raqamli dalillarni xalqaro miqyosda tan olish masalasi ham murakkabdir. Bir davlatda to'plangan elektron dalil boshqa davlat sud tizimida har doim ham to'liq qabul qilinmaydi. Bu esa kiberjinoyatchilarni jazolash jarayonini qiyinlashtiradi.

Profilaktika nuqtai nazaridan esa eng muhim yo'nalishlardan biri — aholining kiberxavfsizlik madaniyatini shakllantirishdir. Foydalanuvchilar kuchli parollar yaratish, ikki bosqichli autentifikatsiya ishlatish va shubhali havolalardan saqlanish kabi oddiy qoidalarga amal qilishi katta xavflarning oldini oladi.

Ta'lim tizimida kiberxavfsizlik va kriptologiya fanlarini chuqur o'qitish ham muhim ahamiyatga ega. Chunki kelajak mutaxassislari faqat texnik bilim emas, balki huquqiy va etik tushunchalarga ham ega bo'lishi kerak.

Xulosa

Tadqiqot natijalari shuni ko'rsatadiki, kiberxavfsizlik va kriptologiya bugungi raqamli jamiyatning strategik ahamiyatga ega sohalaridan biri hisoblanadi. Raqamli texnologiyalarning kengayishi bilan bir qatorda kiberjinoyatchilik, shaxsiy ma'lumotlarning sizib chiqishi, deepfake texnologiyalari, avtomatlashtirilgan kiberhujumlar va axborot manipulyatsiyasi kabi tahdidlar ham ortib bormoqda.

Tahlillar shuni ko'rsatdiki, kiberxavfsizlik muammolarining katta qismi inson omili bilan bog'liq bo'lib, foydalanuvchilarning axborot savodxonligi yetarli emasligi xavf darajasini oshirmoqda. Shuningdek, qonunchilikning texnologik rivojlanishdan ortda qolayotgani ayrim huquqiy bo'shliqlarni yuzaga keltirmoqda.

Kriptologiya sohasida esa zamonaviy shifrlash texnologiyalari axborot muhofazasini kuchaytirsa-da, ularning jinoiy maqsadlarda qo'llanilishi huquqni muhofaza qiluvchi organlar faoliyatini murakkablashtirmoqda. Kvant texnologiyalarining rivojlanishi esa mavjud kriptografik tizimlarni yangilash zaruratini keltirib chiqarmoqda.

Tadqiqot natijalari kiberxavfsizlikni ta'minlash faqat texnik vositalar bilan cheklanmasdan, huquqiy, ijtimoiy va ma'naviy choralarni ham qamrab olishi lozimligini ko'rsatdi.

Tavsiyalar

1. Kiberjinoiyatchilikka qarshi milliy qonunchilikni xalqaro standartlar asosida takomillashtirish zarur.
2. Shaxsiy ma'lumotlarni muhofaza qilish sohasida nazorat mexanizmlarini kuchaytirish maqsadga muvofiq.
3. Davlat va xususiy sektor o'rtasida tezkor axborot almashinuvi tizimini rivojlantirish lozim.
4. Ta'lim muassasalarida kiberxavfsizlik va kriptologiya fanlarini bosqichma-bosqich chuqurlashtirib o'qitish tavsiya etiladi.
5. Aholi o'rtasida raqamli madaniyat va kiberetika qoidalarini targ'ib qilish muhim hisoblanadi.
6. Kvant kriptografiyasi va sun'iy intellekt asosidagi xavfsizlik texnologiyalari bo'yicha ilmiy tadqiqotlarni qo'llab-quvvatlash zarur.
7. Elektron dalillar bilan ishlash bo'yicha yagona protsessual standartlarni ishlab chiqish maqsadga muvofiq.

Foydalanilgan adabiyotlar

1. William Stallings. Cryptography and Network Security: Principles and Practice. — Pearson Education, 2017.
2. Bruce Schneier. Applied Cryptography. — John Wiley & Sons, 2015.
3. O'zbekiston Respublikasining "Shaxsiy ma'lumotlar to'g'risida"gi Qonuni // Qonunchilik ma'lumotlari milliy bazasi.
4. Abduqodirov A.A. Axborot xavfsizligi va kiberxavfsizlik asoslari. — Toshkent: "Fan va texnologiya", 2021.
5. O'zbekiston Respublikasining "Axborotlashtirish to'g'risida"gi Qonuni
6. O'zbekiston Respublikasining "Shaxsiy ma'lumotlar to'g'risida"gi Qonuni
7. O'zbekiston Respublikasining Jinoyat kodeksi Kiberjinoiyatlar (axborot tizimlariga noqonuniy kirish, ma'lumotlarni o'g'irlash) uchun javobgarlikni belgilaydi.
8. "Elektron hukumat to'g'risida"gi Qonun
9. O'zbekiston Respublikasi Raqamli texnologiyalar vazirligi materiallari Kiberxavfsizlik siyosati, raqamli rivojlanish va amaliy tavsiyalar.