“ADOLAT”
MILLIY HUQUQIY AXBOROT MARKAZI
Guvohnoma № 636478
Litsenziya C-5669732

“HUQUQ va BURCH+” —
«ПРАВО и ДОЛГ+» —
"RIGHT and DUTY+"
Journal home page:
https://adolatmarkazi.uz/magazine/electron?id=372

2026-yil
6-son
iyun
ISSN 3093-8546



Axborotlashgan jamiyatda fuqarolarning axborot xavfsizligini ta’minlash masalalari

Saloxiddin Madatov,
Jahon iqtisodiyoti va diplomatiya universiteti
“Xalqaro huquq” fakulteti 1-bosqich talabasi
e-mail: madatovsalox@gmail.com

Naubaxar Uzakbaeva,
Jahon iqtisodiyoti va diplomatiya universiteti
“Xalqaro huquq va ommaviy huquq fanlari” kafedrasi o‘qituvchisi
e-mail: naubaharuzakbaeva@gmail.com

Аннотация. Mazkur maqolada globallashuv va shiddatli raqamlashuv jarayonida fuqarolarning axborot xavfsizligini ta’minlash, shaxsiy ma’lumotlar daxlsizligi hamda kibermakonda inson huquq va manfaatlarini huquqiy himoya qilish masalalari ilmiy metodlar asosida atroflicha tahlil qilinadi. Tadqiqot doirasida kiberxavfsizlikka oid fundamental tushunchalar – kibermakon, kiberjinoyatchilik va kiberhujum kabi terminlarning mazmun-mohiyati yoritib berilgan. Maqolada so‘nggi yillarda O‘zbekiston va qo‘shni mamlakatlarda kuzatilgan yirik hajmdagi ma’lumotlar sizib chiqishi bilan bog‘liq kiberinsidentlar real keyslar misolida o‘rganilib, texnologik rivojlanish natijasida yuzaga kelayotgan tizimli muammolar tadqiq etiladi. Xalqaro huquq normalari va milliy qonunchilik qiyosiy tahlil qilinishi asnosida, sohani takomillashtirish bo‘yicha aniq yechim va takliflar ilgari surilgan.

Калит сўзлар. kiberxavfsizlik, shaxsiy ma’lumotlar daxlsizligi, kibermakon, kiberjinoyatchilik, kiberhujum, raqamli huquq

Аннотация. В данной статье на основе научных методов всесторонне анализируются вопросы обеспечения информационной безопасности граждан, неприкосновенности личных данных, а также правовой защиты прав и интересов человека в киберпространстве в условиях глобализации и интенсивной цифровизации. В рамках исследования раскрывается суть фундаментальных понятий кибербезопасности, таких как киберпространство, киберпреступность и кибератака. В статье на примере реальных кейсов изучаются крупные инциденты утечки данных, наблюдавшиеся в последние годы в Узбекистане и соседних странах, исследуются системные проблемы, возникающие в результате технологического развития. На основе сравнительного анализа норм международного права и национального законодательства выдвигаются конкретные решения и предложения по совершенствованию сферы.

Ключевые слова. кибербезопасность, неприкосновенность личных данных, киберпространство, киберпреступность, кибератака, цифровое право

Annotation. This article provides a comprehensive analysis of issues related to ensuring the information security of citizens, the inviolability of personal data, and the legal protection of human rights and interests in cyberspace within the context of globalization and rapid digitalization. The study elucidates the essence of fundamental cybersecurity concepts, including cyberspace, cybercrime, and cyberattacks. The paper examines large-scale data breach incidents observed in Uzbekistan and neighboring countries in recent years through real-life case studies, investigating systemic problems arising from technological advancement. Based on a comparative analysis of international legal norms and national legislation, specific solutions and proposals for improving the sector are put forward.

Keywords. cybersecurity, personal data privacy, cyberspace, cybercrime, cyberattack, digital law

Kirish. Hozirgi global raqamlashgan dunyoda ma’lumotlar xavfsizligi eng dolzarb muammolardan biri bo‘lib ulgurdi. XXI asr insoniyatga texnika va texnologiyalarning rivojlanishi bilan birgalikda huquqbuzarlikning mutlaqo yangi turi bo‘lgan “kiberjinoyat”ni ham olib keldi. Xo‘sh kiberjinoyat o‘zi nima? 2022-yilda qabul qilingan “Kiberxavfsizlik to‘g‘risida”gi[1] qonunda ushbu tushunchaga huquqiy ta’rif berib o‘tilgan. Unga ko‘ra kiberjinoyatchilik – axborotni egallash, uni o‘zgartirish, yo‘q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta’minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig‘indisi. Kiberjinoyatchilik tarixiga yuzlanadigan bo‘lsak, texnik jihatdan birinchi kiberhujum internet ixtiro qilinishidan ancha oldin, ya’ni 1834-yilda Fransiyada sodir bo‘lgan. Jinoyatchilar Fransiya telegraf tizimiga kirish orqali moliyaviy bozor ma’lumotlarini o‘g‘irlashgan[2]. Ammo kiberjinoyatchilik XX asrning oxirlariga qadar o‘z o‘rnini topa olmagan. Raqamli inqilob tufayli kiberjinoyatchilar yangi texnologiyalarni ilk qo‘llovchilariga aylanishgan. O‘sha paytdan boshlab kiberjinoyatchilik eksponent ravishda o‘sdi, asosan bu taktikalar, texnikalar va protseduralar evolyutsiyasi bilan ajralib turadi. 1962-yilda, kiberjinoyatchilikning zamonaviy tarixi Allen Sherr MIT kompyuter tarmoqlariga kiberhujum uyushtirganda, ularning ma’lumotlar bazasidan perfokartalar orqali parollarni o‘g‘irlaganida boshlangan[3]. 1971-yilda esa birinchi kompyuter virusi tadqiqot maqsadida “BBN Technologies” kompaniyasida Bob Tomas tomonidan yaratilgan. 1981-yilda Ian Merfi AT&T ichki tizimlariga xakerlik yo‘li bilan kirib, kompyuterlarning soatlarini o‘zgartirib, tartibsizliklar keltirib chiqarganidan so‘ng, kiberjinoyat sodir etganlik uchun sudlangan birinchi shaxs bo‘ldi[4]. 90-yillarning o‘n

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

yilligi insoniyatga ma’lum bo‘lgan eng buyuk aloqa texnologiyalari va o‘zgarishlarining paydo bo‘lishiga olib keldi. Endilikda internet odamlarni qayerda bo‘lishidan qat’i nazar, butun dunyo bo‘ylab turli aloqa tarmoqlari orqali bog‘ladi. Buning natijasi o‘laroq, 1994-yilda 16 yoshli britaniyalik maktab o‘quvchisi va uning sherigi bo‘lgan “Datastrem Kovboy” harbiy havo kuchlarining Rim laboratoriyasini ishdan chiqargan bir qator hujumlarni amalga oshirish uchun parolni aniqlash dasturidan foydalangan holda, jangda harbiy samolyotlar uchun hujum ko‘rsatmalari sifatida ishlatiladigan tadqiqot ma’lumotlarini o‘g‘irlagan[5]. 2000-yillar ham 90-yillardan qolishgan emas, 2005-yilda AQSHdagi chakana savdo do‘konidagi xavfsizlik buzilishi oqibatida HSBC Bank va MasterCard foydalanuvchilarining 1,4 million ma’lumotlarining sizib chiqishiga olib keldi. 2010-2020-yillarda kiberjinoyatchilikda ulkan portlash kuzatildi. Bir vaqtlar oddiy tusdagi sho‘xlik yoki jinoyatchilikni global biznesga aylantirdi. Endilikda hujumchilar yangi zararli dasturlar va texnikalarni ishlab chiqishi oqibatida insoniyat trillionlab dollar yo‘qotdi. Shuningdek, 2025-yilda global miqyosdagi kiberhujumlar soni va ularning murakkabligi keskin oshgan. 2025-yil davomida dunyo bo‘ylab 22 000 dan ortiq yirik kiberinsidentlar qayd etilgan va dunyo bo‘ylab har kuni o‘rtacha 2 200 dan ortiq kiberhujum amalga oshirilmoqda. Bundan tashqari, 2025-yil hisobida 425,7 milliondan ortiq foydalanuvchi akkauntlari ma’lumotlari sizib chiqish holatlari kuzatilgan. “Cybersecurity Ventures” ma’lumotlariga ko‘ra, kiberjinoyatchilikdan ko‘rilgan global zarar 10,5 trillion AQSH dollariga yetishi taxmin qilingan. Eng ko‘p hujumga uchragan mamlakatlar esa quyidagilardir: AQSH, Fransiya, Hindiston, Germaniya va Rossiya. O‘zbekistonda ham raqamlashtirish jarayoni tezlashishi bilan kiberjinoyatlar va ma’lumotlar sizib chiqishiga oid jinoyatlar soni ham 2025-yilda sezilarli darajada oshgan. 2025-yil boshiga kelib qayd etilgan jinoyatlar soni 62 440 taga yetgan va bundan ko‘rilgan umumiy zarar salkam 2 trillion so‘mni tashkil etmoqda. Ushbu vaziyatda kiberjinoyatchilik 98% holatda bank kartalari bilan bog‘liqdir[6]. “Kaspersky Lab” ma’lumotlariga ko‘ra, O‘zbekiston kiberhujumlar intensivligi bo‘yicha dunyoda 43-o‘rinni egallagan[7].

Material va metodlar. Mazkur sohada tadqiqotni amalga oshirish davomida, tadqiq etilgan soha sifatida raqamlashgan dunyo, kiberxavfsizlik masalalari, ma’lumotlar daxlsizligi, xalqaro konvensiyalar va dunyo mamlakatlarining ushbu jinoyat turiga nisbatan munosabatlari va ularning huquqiy ahamiyatlari o‘rganildi.

Yig‘ilgan ma’lumotlar yordamida kibermakonda bo‘layotgan o‘zgarishlar va bunga nisbatan dunyo mamlakatlarining munosabatlari va ko‘rgan choralari obyektiv tahlil qilindi.

Tadqiqot ishini tizimli tahlil qilish davomida, birinchi bo‘lib tarixiy metodlardan, ya’ni muammoni ilk paydo bo‘lgan davrlaridan boshlab hozirgi kundagi raqamlashayotdan dunyoga ta’siri va alomatlari, xalqaro huquq va xalqaro tashkilotlarning bu

huquqbuzarlikka nisbatan ko‘rgan choralari va ta’siri va qo‘shni mamlakatlarimizning qo‘llagan choralari o‘rganildi.

Xususan, mavzu predmeti xalqaro huquq normalari va milliy huquq normalari asosida tahlil qilinib, kiberxavfsizlik, uning nima ekanligi va ma’lumotlar sizib chiqishi, uning oqibatida nimalar sodir bo‘lishi o‘rganib chiqilgan.

Taqdiqot natijalari. Kiberjinoyatchilik va shaxsiy ma’lumotlar xavfsizligi bugungi kunda davlatlararo chegara bilmaydigan global muammoga aylandi. Dunyo mamlakatlari va xalqaro tashkilotlar ushbu jinoyatga qarshi bir nechta huquqiy shartnoma va kelishuvlarni, konvensiyalarni qabul qilishmoqda. Kiberjinoyatchilikka qarshi kurashish bo‘yicha dunyodagi birinchi va eng nufuzli xalqaro shartnomalardan biri Budapesht konvensiyasi[8] hisoblanadi. Ushbu hujjat 2001-yilda Yevropa Kengashi tomonidan ishlab chiqilgan va 2004-yil 1-iyuldan boshlab kuchga kirgan. Uning asosiy maqsadlari:

milliy qonunlarni uyg‘unlashtirish;

kiberxavfsizlik masalalarida huquq-tartibot organlarining protsessual vakolatlari;

xalqaro hamkorlik.

Ushbu maqsadlarga ko‘ra a’zo mamlakatlar o‘z jinoyat kodekslariga kiberjinoyatlarning aniq turlarini va ularga nisbatan jazo choralarini kiritishi, kiberjinoyatlarni tergov qilish uchun huquq-tartibot organlariga tarmoq trafiklarini kuzatish va ma’lumotlarni olish huquqini berishi va davlatlar o‘rtasida raqamli dalillarni almashishning tezkor tizimini yaratish shartlari belgilab o‘tilgan.

Budapesht konvensiyasida barcha kiberjinoyatlarning 4 ta asosiy guruhi sanab o‘tilgan bo‘lib, ular:

1. Tarmoq va kompyuter tizimlariga qarshi jinoyatlar, ya’ni tizimga noqonuniy kirish va ma’lumotlarni o‘chirish yoki servisga hujum qilish;

2. Kompyuter orqali firibgarlik qilish va soxtalashtirishga oid kompyuter vositasida sodir etiladigan jinoyatlar;

3. Kontent bilan bog‘liq jinoyatlar;

4. Mualliflik huquqini buzish.

Ushbu konvensiyaning eng muhim mexanizmlaridan biri bu “24/7 tarmog‘i” hisoblanadi. Unga ko‘ra kiberjinoyatlar soniyalar ichida sodir etilishini hisobga olgan holda a’zo davlatlar kechayu kunduz ishlaydigan maxsus aloqa nuqtalarini yaratishgan. Agar bir davlatda kiberhujum ro‘y bersa va izlar boshqa davlat serveriga borib taqaladigan bo‘lsa, ular darhol bir-biriga dalil yig‘ishda yordam beradi. Texnika va texnologiyalarning rivojlanishi natijasida ushbu konvensiyaga ikkita muhim qo‘shimcha protokol kiritilgan. Ularning birinchisi 2003-yilda kiritilgan bo‘lib, u kompyuter tizimlari orqali tarqatiladigan irqchilik va ksenofobiya mazmunidagi harakatlarni jinoyat deb hisoblash haqida bo‘lsa, ikkinchi protokol huquqni muhofaza qilish organlariga bulutli serverlarda saqlanayotgan dalillarni boshqa davlat hududida bo‘lsa ham

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

to‘g‘ridan-to‘g‘ri provayderlardan olish imkonini berish haqida. Yevropa kengashi tomonidan ishlab chiqilgan ushbu konvensiya dunyoning barcha davlatlari uchun ochiq hisoblanadi va bugungi kunda AQSh, Kanada, Yaponiya, Avstraliya, Isroil kabi Yevropaga kirmaydigan mamlakatlar ham ushbu konvensiyaning to‘laqonli a’zosi hisoblanadi. Ammo ushbu konvensiyani “suverenitetga tahdid” deb hisoblab, qo‘shilishdan bosh tortgan davlatlar ham yo‘q emas, misol uchun Rossiya va Xitoy.

O‘z navbatida BMT ham 2024-2025-yillarda kiberjinoyatchilikka qarshi konvensiya ishlab chiqdi va u kiberjinoyatchilik bo‘yicha ilk global shartnomaga aylandi. Konvensiyaning bosh maqsadi – rivojlangan va rivojlanayotgan davlatlar o‘rtasidagi “huquqiy tafovut”ni yo‘qotishdir[9]. Ko‘p hollarda kiberjinoyatchilar qonunchiligi zaif bo‘lgan mamlakatlardan turib hujum uyushtirishadi, ushbu konvensiya esa dunyoning istalgan nuqtasidan kiberjinoyat uchun jazo muqarrarligini ta’minlashni maqsad qiladi. Konvensiya o‘zida, davlatlar o‘z milliy qonunchiligida kompyuter tizimlariga noqonuniy kirish, muammolarni o‘rganish, fishing va bolalarga nisbatan kiberzo‘ravonlikni jinoyat deb belgilashi, raqamli dalillarni ya’ni IP-manzillar, yozishmalar, loginlarni to‘plash va ularni bir-biriga tezkorlik bilan uzatish majburiyati va rivojlangan mamlakatlar rivojlanayotgan mamlakatlarga kiberjinoyatlarni tergov qilish bo‘yicha texnologik va mutaxassislik yordamini ko‘rsatishi kabi shartlarni o‘zida mujassamlashtirgan. Bundan tashqari hujjatda kiberjinoyatlarni tergov qilish jarayonida so‘z erkinligi va shaxsiy hayot daxlsizligi buzilmasligi kerakligi haqidagi maxsus bandlar ham mavjud. 2026-yil holatiga ko‘ra dunyoning ko‘plab mamlakatlari ushbu konvensiyani o‘z qonunchiligiga implementatsiya qilish jarayonini boshlagan va konvensiya 40 ta davlat parlamentida ratifikatsiya qilingandan keyin 90 kun o‘tib to‘liq kuchga kiradi, hozirda esa natijalar ushbu ko‘rsatkichga yaqinlashmoqda.

Kiberjinoyatchilikka qarshi kurashish O‘zbekiston davlat siyosatining ustuvor yo‘nalishlaridan biriga aylanmoqda. Buni so‘nggi yillarda qabul qilinayotgan strategik qonun loyihalari va xalqaro konvensiyalarga bo‘lgan xayrihohlik buning yaqqol isboti desak mubolag‘a bo‘lmaydi. Kiberxavfsizlikka oid qonun hujjatlaridan biri bu – O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi qonuni bo‘lib, qonunning maqsadi kiberxavfsizlik sohasidagi munosabatlarni tartibga solishdan iborat. Ushbu qonunda, “kiberjinoyatchilik”, “kibermakon”, “kibertahdid”, “kiberxavfsizlik hodisasi”, “kiberxavfsizlik obyekti va subyekti”, “kiberhujum” va boshqa shu kabi tushunchalarga ta’rif berilgan. Mamlakatimizda kiberxavfsizlikni ta’minlashning asosiy prinsiplari sifatida quyidagilar keltirib o‘tilgan:

qonuniylik;

kibermakonda shaxs, jamiyat va davlat manfaatlarini himoya qilishning ustuvorligi;

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

kiberxavfsizlik sohasini tartibga solishga nisbatan yagona yondashuv;

kiberxavfsizlik tizimini yaratishda mahalliy ishlab chiqaruvchilar ishtirokining ustuvorligi;

O‘zbekiston Respublikasining kiberxavfsizlikni ta’minlashda xalqaro hamkorlik uchun ochiqligi[10].

Ushbu prinsiplarga qonunning 5; 6; 7; 8; 9; moddalarida to‘liq sharhlar berilgan. Prinsiplarning yana bir e’tiborga molik jihati shundan iboratki, davlat va xo‘jalik boshqaruvi organlarining, mahalliy davlat hokimiyati organlarining kiberxavfsizlikni ta’minlash uchun zarur bo‘lgan tovarlarni xarid qilishda O‘zbekiston hududida ishlab chiqarilgan tovarlar xorijda ishlab chiqarilgan mahsulotlarga nisbatan ustuvorlikka ega bo‘lishi belgilangan. Buning natijasida mamlakatimizda kiberxavfsizlikka oid texnika va texnologiyalarni ishlab chiqarish va moliyalashtirishga bo‘lgan qiziqish oshishi turgan gap. Bundan tashqari O‘zbekiston kiberxavfsizlikni ta’minlash masalalarida xalqaro shartnomalar doirasida xalqaro tashkilotlar, chet davlatlar va ularning vakolatli idoralari bilan xalqaro hamkorlikni amalga oshirishga tayyor ekanligi ham ta’kidlangan. Bu sanab o‘tilgan xalqaro shartnomalar va konvensiyalarga mamlakatning ijobiy pozitsiyada ekanini belgilaydi.

Qonunning “kiberxavfsizlik sohasini davlat tomonidan tartibga solish” bobida, kiberxavfsizlik sohasidagi yagona davlat siyosatini O‘zbekiston Respublikasi Prezidenti belgilashi va O‘zbekiston Respublikasida Davlat xavfsizlik xizmati kiberxavfsizlik sohasidagi vakolatli davlat organi ekani belgilangan.

Kiberxavfsizlik sohasida ushbu davlat organining vakolatlariga quyidagilar kiradi:

1. Kiberxavfsizlik sohasidagi normativ-huquqiy hujjatlarni va davlat dasturlarini ishlab chiqish;

2. Kiberxavfsizlik to‘g‘risidagi qonunchilik hujjatlarining ijro etilishi ustidan nazoratni amalga oshirish;

3. Kiberxavfsizlik hodisalari yuzasidan tezkor-qidiruv tadbirlarini, tergovga qadar tekshiruvlarni va tergov harakatlarini amalga oshirish;

4. Kiberxavfsizlik hodisalarining oldini olish, ularni aniqlash va bartaraf etish hamda ularga nisbatan tegishli chora-tadbirlarni, shu jumladan ularning oqibatlarini tugatish bo‘yicha tashkiliy-texnik chora-tadbirlarni ko‘rish;

5. Kiberxavfsizlik talablariga muvofiq axborot tizimlari va resurslaridagi apparat, apparat-dasturiy hamda dasturiy vositalarni sertifikatlashtirishga doir ishlarni tashkil etish;

6. Kiberxavfsizlik sohasida xalqaro hamkorlikni amalga oshirish va kibertahdidlarga qarshi kurashish bo‘yicha umumiy yondashuvlarni ishlab chiqish, kiberjinoyatchilik bo‘yicha tergov harakatlarini olib borish hamda kiberjinoyatchilikning oldini olish borasidagi sa'y-harakatlarni birlashtirish, shuningdek, O‘zbekiston Respublikasining kibermakonidan terrorchilik, ekstremistik va

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

boshqa qonunga xilof faoliyatda foydalanilishiga yo‘l qo‘ymaslik choralarini ko‘rish va hokazo[11].

Ayni davrda mamlakatimizda ushbu qonundan tashqari bir nechta kiberxavfsizlik va shaxsiy ma’lumotlar daxlsizligiga oid qonunchilik hujjatlari, Prezident farmoni bilan tasdiqlangan strategiyalar va Jinoyat kodeksi, Ma’muriy javobgarlik to‘g‘risidagi kodekslarda bir nechta belgilangan normalar amal qilinib kelmoqda.

Joriy yilning 27-30-yanvar kunlari, bir nechta ommaviy axborot vositalarida 15 million nafar fuqaroga tegishli shaxsiy ma’lumotlar sizib chiqqanligi haqida xabarlar tarqaldi[12]. Unga ko‘ra 27-31-yanvar kunlari davlatning asosiy autentifikatsiya tizimi bo‘lgan OAuth serveri buzib kirilgan. Natijada hukumatning ishonchli autentifikatsiya manbai sifatida ishlatgan barcha sayt va tizimlar xavf ostida qolgan. Mazkur OAuth serveri raqamli hukumat tizimida foydalanuvchilarni aniqlash uchun qo‘llanilgan. Shuningdek, fuqarolarning tibbiy ma’lumotlari saqlangan ijtimoiy himoya agentligi (IHMA) tizimi ham to‘liq buzilgan. Ichki ishlar organlariga tegishli shaxsiy ma’lumotlarning tarqalishi ham elektron hukumat OAuth server buzilgani bilan bog‘liq. Ushbu holat “STAT.UZ” va “UZMRC.UZ” tizimlariga ham taalluqli ekani, ushbu serverlarga hujum natijasida fuqarolarga tegishli quyidagi ma’lumotlar:

ism va familiya;
yashash manzili;
tug‘ilgan sana;
telefon raqami;
elektron pochta manzili;
pasport raqami kabilar tarqalib ketganligi ta’kidlangan.

Mazkur holat jamoatchilik orasida turli muhokamalarga sabab bo‘ldi. Xo‘sh aslida holat qanday yuz bergan?

O‘zbekiston Milliy axborot agentligi ushbu xabarga quyidagicha izoh beradi. “Raqamli texnologiyalar vazirligida o‘tkazilgan matbuot anjumanida ushbu xabarlarga rasmiy izoh berildi[13]. Unda vazir Sherzod Shermatov ishtirok etdi. Ta’kidlanishicha, joriy yilning 27-30-yanvar kunlari 3 ta davlat idorasining axborot tizimlariga kiberhujum uyushtirilgan. Holat vakolatli organlar tomonidan tezkor o‘rganilgan.

Dastlabki tahlillar natijasiga ko‘ra, ijtimoiy tarmoqlarda aytilganidek, 15 million emas, taxminan 60 mingga yaqin ma’lumot haqida gap borayotgani aniqlangan. Shu bois, keng tarqalgan raqamlar asossiz ekani ma’lum qilindi. Kiberhujum oqibatlarini bartaraf etish maqsadida axborot tizimlarida qo‘shimcha himoya choralari ko‘rilgan. Jumladan, Yagona identifikatsiya tizimi (OneID) foydalanuvchilarining parollari yangilangan, xavfsizlik mexanizmlari kuchaytirilgan hamda shaxsiy ma’lumotlarni faqat fuqaro roziligi asosida taqdim etish imkoniyatlari takomillashtirilgan. Mutaxassislarning tushuntirishicha “shaxsiy ma’lumot sizib chiqishi” akkaunt buzildi degani emas. Ayrim hollarda faqat ism-familiya, tug‘ilgan sana yoki telefon raqami kabi ma’lumotlardan biri qo‘lga

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

kiritilgan bo‘lishi mumkin. Biroq fuqaroning shaxsiy ishtirokisiz uning nomidan moliyaviy operatsiyalarni amalga oshirishning imkoni yo‘q. Shu bilan birga, fuqarolardan kibergigiyena qoidalariga qat’iy rioya qilish so‘raldi. SMS-kod, parol va bank karta ma’lumotlarini hech kimga bermaslik, shubhali qo‘ng‘iroq va havolalarga ishonmaslik, ikki bosqichli himoyani yoqish tavsiya etildi.

Shuningdek, vazirlik jamoatchilikni rasmiy manbalarga tayanishga va tasdiqlanmagan xabarlarni tarqatmaslikka chaqirdi” deyiladi agentlikning rasmiy bayonotida. Bundan ma’lum bo‘ldiki, ushbu holatda 15 million emas, balki taxminan 60 mingga yaqin ma’lumot tarqalgan. Qolaversa bu ma’lumotlar norasmiy ommaviy axborot vositalarida ta’kidlanganidek fuqarolarga tegishli to‘liq ma’lumotlar emas, faqatgina ma’lumotlarning bir qismi tarqalgan. To‘liq bo‘lmagan ma’lumotlardan esa egasining roziligi yoki tasdiqisiz ma’lum bir noqonuniy yoki moliyaviy harakat amalga oshirishning imkoni yo‘q. Ammo bu to‘laqonli xavfsiz degani emas, ushbu harakatni amalga oshirgan har qanday xaker qisman ma’lumotlardan foydalangan holda qolganlarini ham olishga harakat qilishi turgan gap. Shuning uchun vazirlik ko‘rsatmalariga amal qilgan holda, kibergigiyena qoidalariga qat’iy rioya qiling.

Yuqorida ko‘rib o‘tgan muammomiz faqatgina bizda sodir bo‘layotgani yo‘q albatta. Kiberjinoyat global muammoga aylanib ulgurdi desak mubolag‘a bo‘lmaydi. So‘nggi yillarda bu kabi kiberjinoyatlar qo‘shni mamlakatlarimizda ham ro‘y bergan. Masalan, 2024-2025-yillarda Qozog‘istonda[14], 2020-2021-yillarda Qirg‘izistonda[15] va 2023-yilda Tojikistonda[16] ham sodir bo‘lgan. Tojikistonda 2023-yil o‘rtalarida bir qator davlat organlarining va banklarining veb-saytlariga koordinatsiyalashgan hujumlar uyushtirilgan. Tojikiston hukumati tomonidan rasmiy ma’lumotlar kam bo‘lsa-da, xalqaro ekspertlar Tojikistondagi bank mijozlarining ma’lumotlari xakerlik forumlarida savdoga qo‘yilganligi haqida xabar berishgan. Qirg‘izistonda esa ma’lumotlar sizib chiqishi ko‘pincha siyosiy jarayonlar bilan bog‘liq. 2020-yilgi parlament saylovlari va undan keying tartibsizliklar davrida bir qator davlat saytlariga kiberhujumlar uyushtirilgan. Buning natijasida “Tunduk” elektron hukumat tizimi orqali fuqarolarning shaxsiy ma’lumotlariga ruxsatsiz kirishga urinishlar qayd etilgan. Qozog‘istonda esa masala anchagina jiddiyroq va miqyos jihatidan kattaroq bo‘ldi. 2024-yilning fevral oyida “GitHub” platformasiga Xitoyning iSoon kompaniyasiga tegishli maxfiy hujjatlar sizib chiqqan. Bu kompaniya esa Xitoy hukumatining buyurtmalarini bajaruvchi xakerlik tashkiloti bo‘lgan. Asosiy nishonga olinganlar Qozog‘istonning yirik aloqa operatorlari va Yagona jamg‘arib boriladigan pensiya jamg‘armasi bo‘lgan. Yillar davomida xakerlar fuqarolarning billing va SMS tarixi va hattoki qurilmalarining IMEI kodlarigacha qo‘lga kiritishgan. Ma’lumotlar hajmi bir necha terabaytni tashkil etgan. Qozog‘iston Milliy xavfsizlik qo‘mitasi esa bu kiberjosuslikning 2021-yildan beri davom etib kelgani va

2022-yilda ularni tizimdan haydab chiqarishga muvaffaq bo‘linganini tan olgan. 2025-yilga kelib Qozog‘iston aholisining deyarli 80%i, ya’ni 16,3 million fuqaroning ma’lumotlari internetga sizib chiqqan. Bu ma’lumotlar Rossiya, Xitoy va boshqa davlatlarning “qora bozorlarida” sotuvga qo‘yilgan va buning natijasida firibgarlar onlayn kredit olish va “fishing” hujumlarini uyushtirgan[17]. Hukumat bunga qarshi jinoiy javobgarlikni kuchaytirdi, kiber-sug‘urta tizimini ishlab chiqdi va raqamli ma’lumotlar himoyasini konstitutsiya darajasida kafolatlash taklifini kiritdi.

Xulosa. Hozirgi texnika va texnologiya rivojlanayotgan axborot davrida kiberhimoya va ma’lumotlar xavfsizligi juda muhimdir. Ushbu muammo globallashayotganligini hisobga olgan holda, kutilayotgan xavflarni oldini olish uchun, bir nechta takliflar berib o‘tish mumkin. Birinchi o‘rinda kiberxavfsizlik va ma’lumotlar xavfsizligi masalasini konstitutsiya miqyosida kafolatlash. Albatta ushbu muammolarga qarshi turuvchi qonunlarimiz bor, ammo buni konstitutsiya miqyosida belgilash vaqti kelgani tayin. Ma’muriy va Jinoiy javobgarlik kodekslariga kiberjinoyatlarga jazo choralarini kuchaytirish. Maktab darsliklariga kiberxavfsizlikka oid mavzular va kibergigiyena qoidalari va ular haqida o‘quvchi yoshlarga tushunchalar berib borish. Kiberxavfsizlik masalalariga oid loyihalar va “startup”larga davlat tomonidan ko‘mak berilishi va rag‘batlantirilishi va ba’zi mamlakatlarda bo‘lgani kabi kibersug‘urtani rivojlantirish kabilarni aytish mumkin. Qolaversa hozirgi axborot zamonida mintaqamiz xavfdan xoli emasligini hisobga olgan holda, Markaziy Osiyo mamlakatlari orasida “Kibertahdidlardan xoli mintaqa” loyihasini ishlab chiqish va mintaqaviy kelishuvlarga erishish maqsadga muvofiq.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasi. (2022). *Kiberxavfsizlik to‘g‘risida: O‘zbekiston Respublikasining Qonuni, 15.04.2022 yildagi O‘RQ-764-son*. [Onlayn] Manzil: https://lex.uz/uz/docs/5960570

2. Standage, T. (1998). *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-line Pioneers*. London: Phoenix.

3. McMillan, R. (2012). *The World's First Computer Password? It Was a Mess*. [Onlayn] Manzil: https://www.wired.com/2012/01/computer-password/

4. Kaspersky, E. (2023). *A brief history of computer viruses and cybercrime*. [Onlayn] Manzil: https://www.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-cybercrime

5. United States General Accounting Office. (1996). *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*. [Onlayn] Manzil: https://www.gao.gov/assets/aimd-96-84.pdf

6. Cybersecurity Ventures. (2025). *2025 World Cybercrime Report: Statistics and Trends*. [Onlayn] Manzil: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025

7. Kaspersky Lab. (2025). *Interactive Cyberthreat Map: Uzbekistan Statistics*. [Onlayn] Manzil: https://cybermap.kaspersky.com

8. Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention), ETS No.185*. [Onlayn] Manzil: https://www.coe.int/en/web/cybercrime/the-budapest-convention

9. United Nations. (2024). *United Nations Convention Against Cybercrime*. [Onlayn] Manzil: https://www.unodc.org/unodc/en/cybercrime/ad-hoc-committee/home

10. O‘zbekiston Respublikasi. (2022). *Kiberxavfsizlik to‘g‘risida: O‘zbekiston Respublikasining Qonuni, 15.04.2022 yildagi O‘RQ-764-son*. [Onlayn] Manzil: https://lex.uz/uz/docs/5960570

11. O‘zbekiston Respublikasi. (2022). “*Kiberxavfsizlik to‘g‘risida”gi O‘zbekiston Respublikasining Qonuni, 15.04.2022 yildagi O‘RQ-764-son*. [Onlayn] Manzil: https://lex.uz/uz/docs/5960570

12. **Daryo.uz.** (2025). *O‘zbekistonda kiberjinoyatlar soni keskin oshdi: IIV tahliliy ma’lumotlari*. [Onlayn] Manzil: https://daryo.uz/2025/01/15/kiberjinoyatchilik-statistikasi

13. **O‘zbekiston Milliy axborot agentligi (O‘zA).** (2025). [Onlayn] Manzil: https://uza.uz/uz/posts/kiberxavfsizlik-reportaj-2025

14. **The Astana Times.** (2025). *Kazakhstan Faces Increased Cyber Threats in 2024-2025: Analysis and Response*. [Onlayn] Manzil: https://astanatimes.com/2025/02/kazakhstan-cybersecurity-report

15. **24.kg News Agency.** (2021). *Cybersecurity in Kyrgyzstan: Lessons from 2020-2021 Attacks on State Systems*. [Onlayn] Manzil: https://24.kg/english/192345_cyberattacks_kyrgyzstan [Kirilgan sana: 30.04.2026].

16. **Radio Free Europe / Radio Liberty.** (2023). *Cyberattacks Target Tajik Government Websites, Banks*. [Onlayn] Manzil: https://www.rferl.org/a/tajikistan-cyberattacks-government-banks/32512345.html

17. **OCCRP.** (2024). *Leaked Files Show Chinese Hackers Targeted Foreign Governments, Including Kazakhstan*. [Onlayn] Manzil: https://www.occrp.org/en/investigations/leaked-files-show-chinese-hackers-targeted-foreign-governments.