AXBOROT XAVFSIZLIGINING ZAMONAVIY JAMIYATDAGI AHAMIYATI VA UNI TA'MINLASH MUAMMOLARI

Mirzaqulov Boburjon Zokirjon o'g'li
Namangan davlat texnika universiteti bakalavriat talabasi
Yangi Namangan tumani, Namangan viloyati, O'zbekiston
E-mail: boburjonmirzaqulov91@gmail.com, tel.: +998 95 131 25 95

ЗНАЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННОМ ОБЩЕСТВЕ И ПРОБЛЕМЫ ЕЁ ОБЕСПЕЧЕНИЯ

Мирзакулов Бобуржон Зокиржон угли
Студент бакалавриата Наманганского государственного технического университета
Янгинаманганский район, Наманганская область, Узбекистан
E-mail: boburjonmirzaqulov91@gmail.com, тел.: +998 95 131 25 95

THE IMPORTANCE OF INFORMATION SECURITY IN MODERN SOCIETY AND THE CHALLENGES OF ENSURING IT

Mirzakulov Boburjon Zokirjon ugli
Bachelor's student, Namangan State Technical University
Yangi Namangan district, Namangan region, Uzbekistan
E-mail: boburjonmirzaqulov91@gmail.com, tel.: +998 95 131 25 95

Annotatsiya. Maqolada raqamli transformatsiya sharoitida axborot xavfsizligining shaxs, jamiyat va davlat hayotidagi ahamiyati tadqiq etilgan. Kiberhujumlar va kiberjinoyatlar sonining keskin o'sishi muammoning dolzarbligini belgilashi asoslangan. Tadqiqotda tizimli va qiyosiy tahlil, normativ-huquqiy hujjatlarning kontent-tahlili hamda rasmiy statistik ma'lumotlarning ikkilamchi tahlili usullaridan foydalanilgan. Natijada axborot xavfsizligining uch darajali ijtimoiy modeli taklif etilgan, O'zbekistondagi kibertahdidlar dinamikasi va huquqiy asoslar umumlashtirilgan. Asosiy xavf omili sifatida inson omili va aholi

raqamli savodxonligining yetarli emasligi ko‘rsatilgan hamda kiber madaniyatni shakllantirishga doir amaliy tavsiyalar ishlab chiqilgan.

Kalit so‘zlar: axborot xavfsizligi, kiberxavfsizlik, kiberjinoyatchilik, shaxsga doir ma’lumotlar, raqamli savodxonlik, kiber madaniyat.

Аннотация. В статье исследовано значение информационной безопасности для личности, общества и государства в условиях цифровой трансформации. Обоснована актуальность проблемы, обусловленная резким ростом числа кибератак и киберпреступлений. В исследовании применены методы системного и сравнительного анализа, контент-анализа нормативно-правовых документов и вторичного анализа официальных статистических данных. Предложена трёхуровневая социальная модель информационной безопасности, обобщены динамика киберугроз и правовые основы в Узбекистане. В качестве главного фактора риска выделены человеческий фактор и недостаточная цифровая грамотность населения, разработаны практические рекомендации по формированию киберкультуры.

Ключевые слова: информационная безопасность, кибербезопасность, киберпреступность, персональные данные, цифровая грамотность, киберкультура.

Abstract. The article examines the importance of information security for the individual, society and the state in the context of digital transformation. The relevance of the problem is substantiated by the sharp growth in the number of cyberattacks and cybercrimes. The study applied systemic and comparative analysis, content analysis of legal documents and secondary analysis of official statistical data. A three-level social model of information security was proposed, and the dynamics of cyber threats and the legal framework in Uzbekistan were summarized. The human factor and insufficient digital literacy of the population were identified as the main risk factors, and practical recommendations for building a cyber culture were developed.

Keywords: information security, cybersecurity, cybercrime, personal data, digital literacy, cyber culture.

KIRISH

Bugungi kunda axborot jamiyat taraqqiyotining asosiy resursiga aylandi. Davlat xizmatlari, bank-moliya tizimi, ta'lim va sog'liqni saqlash sohalari tobora raqamli platformalarga ko'chmoqda. O'zbekistonda bu jarayon «Raqamli O'zbekiston – 2030» strategiyasi asosida tizimli ravishda amalga oshirilmoqda [9]. Biroq raqamlashtirishning har bir yangi bosqichi bilan birga axborotga tahdidlar ham ko'payib bormoqda. Ma'lumotlarning sizib chiqishi, firibgarlik, axborot tizimlarini ishdan chiqarishga qaratilgan hujumlar endi faqat texnik muammo emas, balki fuqarolar xavfsizligi, iqtisodiy barqarorlik va davlat institutlariga ishonch masalasiga aylandi.

Muammoning ko'lamini rasmiy raqamlar ham tasdiqlaydi. Ichki ishlar vazirligi ma'lumotiga ko'ra, so'nggi besh yilda mamlakatda kiberjinoyatlar soni 68 barobar oshgan, 2024-yilda esa ularning umumiy jinoyatchilikdagi ulushi 44,4 foizga yetgan [8]. Demak, deyarli har ikkinchi jinoyat axborot texnologiyalari yordamida sodir etilmoqda. Bu holat axborot xavfsizligini tor mutaxassislar doirasidagi masaladan butun jamiyat masalasiga aylantirmoqda.

Davlat bu chaqiriqlarga huquqiy va tashkiliy choralar bilan javob bermoqda: «Kiberxavfsizlik to'g'risida»gi Qonun qabul qilingan [12], 2026–2030-yillarga mo'ljallangan Kiberxavfsizlik strategiyasi tasdiqlangan [10]. Shunga qaramay, texnik va huquqiy choralar aholining bilimi va xatti-harakati bilan qo'llab-quvvatlanmasa, ularning samarasi cheklanib qoladi.

Tadqiqotning maqsadi — axborot xavfsizligining zamonaviy jamiyatdagi o'rni va ahamiyatini ochib berish, O'zbekistonda uni ta'minlashdagi asosiy muammolarni aniqlash va ularni hal etish yo'nalishlarini asoslash. Maqsadga erishish uchun quyidagi **vazifalar** belgilandi:

– axborot xavfsizligi tushunchasi va tarkibiy qismlarini aniqlashtirish;

– uning shaxs, jamiyat va davlat darajasidagi ahamiyatini tizimlashtirish;

– O‘zbekistondagi kibertahdidlar dinamikasini rasmiy statistika asosida tahlil qilish;

– milliy huquqiy-tashkiliy asoslarni xalqaro baholash natijalari bilan solishtirish;

– axborot xavfsizligini ta’minlashga doir amaliy tavsiyalar ishlab chiqish.

Maqolada qo‘llanilgan asosiy atamalar quyidagi ma’noda ishlatiladi. *Axborot xavfsizligi* — axborotning maxfiyligi, yaxlitligi va foydalanuvchanligini saqlash holati [6]. *Kiberxavfsizlik* — shaxs, jamiyat va davlat manfaatlarining kibermakondagi tashqi va ichki tahdidlardan himoyalanganlik holati [12]. *Kiberjinoyat* — axborot texnologiyalaridan foydalangan holda sodir etiladigan jinoyat. *Ijtimoiy muhandislik* — insonni aldash yoki uning ishonchidan foydalanib maxfiy ma’lumotlarni qo‘lga kiritish usuli.

MAVZUGA OID ADABIYOTLAR TAHLILI

Axborot xavfsizligi nazariyasida eng keng tarqalgan yondashuv «maxfiylik – yaxlitlik – foydalanuvchanlik» uchligiga (ingliz tilida *CIA triad*) asoslanadi. M. Whitman va H. Mattord axborot xavfsizligini faqat texnik vositalar majmui sifatida emas, balki siyosat, o‘qitish va xabardorlik dasturlarini ham o‘z ichiga olgan boshqaruv tizimi sifatida talqin qiladi [15]. W. Stallings va L. Brown kompyuter xavfsizligining asosiy maqsadlarini shu uch xususiyat orqali ifodalab, ularga haqiqiylik va hisobdorlik talablarini qo‘shadi [14]. R. Anderson esa xavfsizlik muhandisligi nuqtai nazaridan tizimlarning zaifligi ko‘pincha texnologiyaning o‘zida emas, balki inson xatti-harakati, iqtisodiy rag‘batlar va tashkiliy qarorlarda ekanini ko‘rsatadi [3].

Xalqaro standartlashtirish darajasida ISO/IEC 27001:2022 standarti axborot xavfsizligini boshqarish tizimiga qo‘yiladigan talablarni belgilaydi. Standart xavfsizlikni bir martalik chora emas, balki xavf-xatarlarni baholash va boshqarishga asoslangan uzluksiz jarayon sifatida qaraydi [6].

Mahalliy tadqiqotchilardan S.K. G‘aniyev, M.M. Karimov va K.A. Tashev axborot xavfsizligini axborotning ruxsatsiz oshkor etilishi, buzilishi va undan foydalanish imkoniyati yo‘qolishining oldini olish sifatida ta’riflab, tahdidlar, xavfsizlik siyosati hamda huquqiy boshqaruv masalalarini tizimli yoritgan [4]. F.M. Muxtarov axborot hujumlari davrida «Kiberxavfsizlik» fanini o‘qitishning dasturiy va metodik ta’minotini takomillashtirish masalasini o‘rganib, soxta xabarlar va axborot manipulyatsiyasini zamonaviy tahdidlarning muhim turi sifatida ajratgan [7].

Davlatlarning bu sohadagi tayyorgarligini baholashda Xalqaro elektraloqa ittifoqining (ingl. *International Telecommunication Union*, ITU) Global kiberxavfsizlik indeksi keng qo‘llaniladi. Indeks mamlakatlarni beshta yo‘nalish — huquqiy, texnik, tashkiliy choralar, salohiyatni rivojlantirish va hamkorlik bo‘yicha baholaydi [5].

Tahlil shuni ko‘rsatadiki, adabiyotlarda axborot xavfsizligi asosan texnik va huquqiy jihatdan yoritilgan. Uning ijtimoiy jihati, ya’ni aholining xabardorligi, raqamli savodxonligi va kiber madaniyatining umumiy xavfsizlik darajasiga ta’siri, ayniqsa O‘zbekistonning so‘nggi yillardagi statistik ma’lumotlari asosida yetarli darajada tahlil qilinmagan. Ushbu maqola shu bo‘shliqni qisman to‘ldirishga qaratilgan.

TADQIQOT METODOLOGIYASI

Tadqiqot nazariy-tahliliy xarakterga ega bo‘lib, unda quyidagi usullardan foydalanildi:

– *tizimli yondashuv*: axborot xavfsizligi shaxs, jamiyat va davlat darajalaridan iborat yaxlit tizim sifatida ko‘rib chiqildi;

– *normativ-huquqiy hujjatlarning kontent-tahlili*: «Shaxsga doir ma’lumotlar to‘g‘risida»gi [11] va «Kiberxavfsizlik to‘g‘risida»gi [12] qonunlar, Prezidentning PF-6079-son [9] va PF-38-son [10] farmonlari o‘rganildi;

– *ikkilamchi statistik tahlil*: 2019–2026-yillarga oid Ichki ishlar vazirligi, «Kiberxavfsizlik markazi» va Raqamli texnologiyalar vazirligi e'lon qilgan ma'lumotlar umumlashtirildi [1; 2; 8; 13];

– *qiyosiy tahlil*: milliy ko'rsatkichlar ITU Global kiberxavfsizlik indeksi 2024 natijalari bilan solishtirildi [5].

Statistik ma'lumotlar turli idoralar tomonidan turli metodikalar asosida hisoblangani sababli ular o'zaro qo'shilmadi. Har bir ko'rsatkich o'z manbasi doirasida talqin qilindi.

TAHLIL VA NATIJALAR

1. Axborot xavfsizligining tarkibiy qismlari. Adabiyotlar tahlili axborot xavfsizligini uchta asosiy va ikkita qo'shimcha xususiyat orqali tavsiflash mumkinligini ko'rsatdi. Ulardan birortasining buzilishi butun tizim xavfsizligining buzilishini anglatadi. Masalan, DDoS (ingl. *Distributed Denial of Service* — xizmat ko'rsatishni taqsimlangan rad etish) hujumi ma'lumotni o'g'irlamasa ham, foydalanuvchanlikni yo'qqa chiqaradi (1-jadval).

1-jadval

Axborot xavfsizligining asosiy xususiyatlari

Xususiyat	Mazmuni	Buzilishiga misol
Maxfiylik	Axborotdan faqat vakolatli shaxslar foydalana olishi	Shaxsga doir ma'lumotlar bazasining sizib chiqishi
Yaxlitlik	Axborotning to'liqligi, to'g'riligi va ruxsatsiz o'zgartirilmasligi	Veb-sayt sahifasini ruxsatsiz almashtirish, hujjatni soxtalashtirish
Foydalanuvchanlik	Vakolatli foydalanuvchi axborot va xizmatlardan kerakli vaqtda foydalana olishi	DDoS hujumi natijasida davlat xizmatlari portalining ishlamay qolishi
Haqiqiylik[a]	Foydalanuvchi va axborot manbasining haqiqiyligini tasdiqlash	Soxta bank sahifasi orqali fishing

Xususiyat	Mazmuni	Buzilishiga misol
Hisobdorlik[a]	Tizimdagi harakatlarni aniq shaxsga bog‘lab qayd etish	Jurnal yozuvlarining yo‘qligi sababli hodisa aybdorini aniqlab bo‘lmasligi

[a] Qo‘shimcha xususiyatlar [14] asosida kiritilgan. Manba: [4; 6; 14; 15] asosida muallif tomonidan tuzilgan.

2. Axborot xavfsizligining jamiyatdagi o‘rni. Tadqiqot natijasida axborot xavfsizligining ahamiyatini uch darajada ko‘rib chiqish taklif etildi (2-jadval). Har bir darajaning o‘z himoya obyekti, tahdidlari va oqibatlari bor.

2-jadval

Axborot xavfsizligining shaxs, jamiyat va davlat darajasidagi ahamiyati

Daraja	Himoya obyekti	Asosiy tahdidlar	Ta’minlanmaganligi oqibatlari
Shaxs	Shaxsga doir ma’lumotlar, bank kartalari, shaxsiy yozishmalar, raqamli identifikator	Fishing, ijtimoiy muhandislik, hisob qaydnomasini buzish	Moddiy zarar, shaxsiy hayot daxlsizligining buzilishi, obro‘ga putur yetishi
Jamiyat	Axborot maydoni, bank-moliya, ta’lim va sog‘liqni saqlash tizimlari	Soxta xabarlar, axborot manipulyatsiyasi, ommaviy firibgarlik	Raqamli xizmatlarga ishonchning pasayishi, ijtimoiy keskinlik
Davlat	Davlat axborot tizimlari, muhim axborot infratuzilmasi obyektlari	Davlat resurslariga kiberhujumlar, ma’lumotlarni o‘g‘irlash, xizmatlarni ishdan chiqarish	Boshqaruvning uzilishi, iqtisodiy yo‘qotish, milliy xavfsizlikka tahdid

Manba: muallif ishlanmasi.

Uch daraja bir-biri bilan chambarchas bog‘liq. Davlat axborot tizimi qanchalik yaxshi himoyalangan bo‘lmasin, uning foydalanuvchisi parolini firibgarga aytib qo‘ysa, himoya zanjiri eng zaif bo‘g‘in — inson orqali uziladi. Aksincha, davlat tizimlaridan sizib chiqqan ma’lumotlar millionlab fuqarolarni firibgarlik xavfi ostida qoldiradi. Shu sababli axborot xavfsizligini faqat texnik masala emas, balki ijtimoiy institut sifatida ko‘rib chiqish lozim.

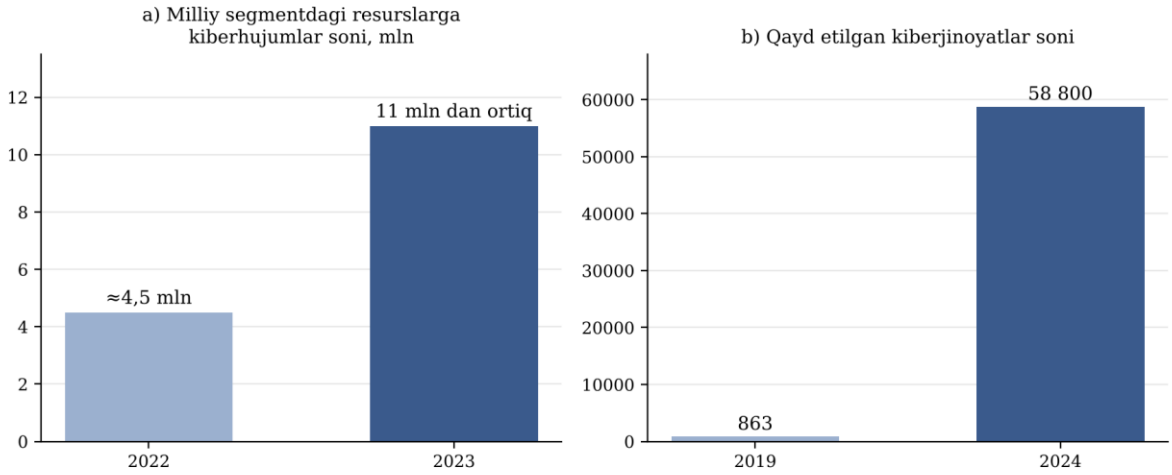
3. O‘zbekistonda kibertahdidlar dinamikasi. Rasmiy ma’lumotlar tahdidlarning ham miqdor, ham ko‘lam jihatidan o‘sib borayotganini ko‘rsatadi (3-jadval, 1-rasm).

3-jadval

O‘zbekistonda kibertahdidlar va kiberjinoyatlarning asosiy ko‘rsatkichlari

Ko‘rsatkich	Qiymati	Manba
Internetning milliy segmentidagi resurslarga tajovuzlar	2022-y. — 4,5 mln ga yaqin; 2023-y. — 11 mln dan ortiq (2,4 barobar o‘sish)	[13]
Milliy segmentda aniqlangan kiberxavfsizlik hodisalari	2022-y. — 235 ta; 2023-y. — 158 ta	[13]
Qayd etilgan kiberjinoyatlar soni	2019-y. — 863 ta (18 tur); 2024-y. — 58 800 ta (62 tur)	[8]
Kiberjinoyatlarning umumiy jinoyatchilikdagi ulushi	2023-y. — 6,2 %; 2024-y. — 44,4 %	[8]
Kiberjinoyatchilar o‘zlashtirgan mablag‘lar	So‘nggi uch yilda 1,9 trln so‘mdan ortiq, shu jumladan 2024-y. — 603 mlrd so‘m	[2]
Qayd etilgan kiberhujumlar[a]	2025-y. — 107 mln dan ortiq	[1]

[a] Raqamli texnologiyalar vaziri keltirgan umumiy ko‘rsatkich; boshqa qatorlardagi ma’lumotlardan farqli metodika bo‘yicha hisoblangan bo‘lishi mumkin.



1-rasm. O‘zbekistonda kibertahdidlar dinamikasi: a) milliy segment resurslariga tajovuzlar; b) qayd etilgan kiberjinoyatlar

Manba: [8; 13] ma’lumotlari asosida muallif tomonidan tuzilgan.

Jadval va rasmdan ikki muhim qonuniyat kelib chiqadi. Birinchidan, axborot resurslariga tajovuzga urinishlar keskin ko‘paygan bo‘lsa-da, aniqlangan kiberxavfsizlik hodisalari soni 2023-yilda kamaygan [13]. Bu davlat resurslarining texnik himoyasi kuchayib borayotganidan dalolat beradi. Ikkinchidan, fuqarolarga qarshi sodir etilayotgan kiberjinoyatlar soni besh yilda 68 barobar oshgan [8]. Ya’ni hujumchilar himoyasi kuchaygan tizimlardan ko‘ra himoyasi zaif bo‘g‘in — oddiy foydalanuvchiga ko‘proq yo‘nalmoqda.

Davlat tizimlari ham xavfdan to‘liq xoli emas. Raqamli texnologiyalar vazirining ma’lumotiga ko‘ra, 2026-yil yanvar oyida uchta davlat idorasi kiberhujumga uchrab, 60 mingga yaqin shaxsga doir ma’lumot o‘g‘irlangan. Vazir sizib chiqishlar asosan test rejimidagi yoki sertifikatsiyadan o‘tmagan tizimlarda yuz berishini ta’kidlagan [1].

4. Huquqiy-tashkiliy asoslar va xalqaro baholash. O‘zbekistonda axborot xavfsizligining huquqiy bazasi so‘nggi yillarda sezilarli darajada shakllandi. 2019-yilda «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonun qabul qilinib, fuqarolarning shaxsiy ma’lumotlariga ishlov berish va ularni himoya qilish tartibi belgilandi [11]. 2022-yil 15-aprelda qabul qilingan «Kiberxavfsizlik to‘g‘risida»gi Qonun sohadagi

munosabatlarni tartibga soluvchi asosiy hujjat bo‘lib, unda davlat organlarining axborot tizimlari va resurslarini kiberxavfsizlik talablariga muvofiqligi yuzasidan majburiy ekspertizadan o‘tkazish nazarda tutilgan [12].

2026-yil 10-martdagi PF-38-son Farmon bilan 2026–2030-yillarga mo‘ljallangan Kiberxavfsizlik strategiyasi tasdiqlandi. Unda muhim infratuzilma obyektlarida nazoratni kuchaytirish, vazirlik va idoralarda kiberxavfsizlik bo‘linmalarini tashkil etish, mutaxassislar malakasini oshirish, aholi uchun tushuntirish materiallari tayyorlash va xususiy sektorni sohaga jalb qilish kabi yo‘nalishlar belgilangan [10].

Bu sa’y-harakatlar xalqaro miqyosda ham e’tirof etilmoqda. ITU Global kiberxavfsizlik indeksi 2024 natijalariga ko‘ra, O‘zbekiston 89,2 ball to‘plab (2021-yilda 71,11 ball), faol rivojlanayotgan davlatlar guruhiga — ikkinchi darajaga (T2 Advancing) kiritildi [5]. Indeks shuningdek, milliy kiberxavfsizlik strategiyasiga ega davlatlar soni 2021-yildagi 107 tadan 2024-yilda 132 taga yetganini qayd etadi [5]. Demak, strategik hujjatlar qabul qilish jahon miqyosidagi umumiy tendensiyadir va O‘zbekiston bu jarayonda faol ishtirok etmoqda.

MUHOKAMA

Olingan natijalar o‘ziga xos ziddiyatni ko‘rsatadi. Bir tomondan, davlat darajasidagi huquqiy va texnik salohiyat o‘sib bormoqda: xalqaro indeksdagi o‘rin yaxshilangan, milliy segmentdagi hodisalar soni kamaygan. Ikkinchi tomondan, fuqarolarga qarshi kiberjinoyatlar keskin ko‘paygan va ular umumiy jinoyatchilikning deyarli yarmini tashkil etmoqda. Bu ziddiyat R. Anderson [3] hamda M. Whitman va H. Mattord [15] tomonidan ilgari surilgan fikrni tasdiqlaydi: texnik himoya qanchalik kuchli bo‘lmasin, tizim xavfsizligini oxir-oqibat inson omili belgilaydi.

Shundan kelib chiqib, kirish qismida qo‘yilgan savolga javob berish mumkin: zamonaviy jamiyatda axborot xavfsizligining asosiy muammosi texnologiya yetishmasligida emas, balki uning foydalanuvchilari — fuqarolarning xavfsizlik

madaniyati yetarli emasligida. Shu sababli axborot xavfsizligini ta’minlash quyidagi yo‘nalishlarda olib borilishi maqsadga muvofiq:

1. *Ta’lim tizimida kibergigiyenani shakllantirish.* Umumta’lim maktablari va oliy ta’lim muassasalarining barcha yo‘nalishlarida, mutaxassislikdan qat’i nazar, «Kiberxavfsizlik asoslari» moduli yoki mavzular blokini joriy etish. Bunda F.M. Muxtarov taklif etgan metodik yondashuvlardan foydalanish mumkin [7].

2. *Aholining xavf guruhlari bilan ishlash.* Keksa yoshdagi fuqarolar va internetdan endi foydalana boshlagan aholi uchun mahalla darajasida ma’rifiy tadbirlar o‘tkazish, firibgarlikning keng tarqalgan usullari haqida qisqa tushuntirish videolarini tarqatish. Bu yo‘nalish Kiberxavfsizlik strategiyasi vazifalariga ham mos keladi [10].

3. *Tashkilotlarda xavfsizlikni boshqarish tizimini joriy etish.* Davlat va xususiy tashkilotlarda ISO/IEC 27001 standarti asosida axborot xavfsizligini boshqarish tizimini qurish, xodimlarni muntazam o‘qitish va fishing hujumlariga qarshi o‘quv mashg‘ulotlari o‘tkazish [6].

4. *Majburiy ekspertiza talabiga qat’iy rioya qilish.* Davlat axborot tizimlarini kiberxavfsizlik ekspertizasidan o‘tkazmasdan ishga tushirish va ularni uzoq muddat test rejimida qoldirish amaliyotiga yo‘l qo‘ymaslik [1; 12].

5. *Statistikaning ochiqligi va yagona metodikasi.* Kiberhujumlar va kiberjinoyatlar bo‘yicha ma’lumotlarni yagona metodika asosida muntazam e’lon qilish. Hozirda turli idoralar ma’lumotlari turlicha hisoblangani sababli ularni solishtirish va dinamikasini aniq baholash qiyin.

Tadqiqot cheklovlari. Ushbu ish nazariy-tahliliy xarakterga ega bo‘lib, ikkilamchi ma’lumotlarga tayanadi. Statistik ko‘rsatkichlar turli manbalardan olingani sababli ular o‘rtasida metodik farqlar bo‘lishi mumkin. Keyingi tadqiqotlarda talabalar va aholining turli qatlamlari o‘rtasida kibergigiyena darajasini aniqlashga qaratilgan empirik so‘rovnoma o‘tkazish va taklif etilgan tavsiyalarning samaradorligini tajriba asosida tekshirish rejalashtirilmoqda.

XULOSA

Tadqiqot natijalari asosida quyidagi xulosalarga kelindi:

1. Axborot xavfsizligi maxfiylik, yaxlitlik va foydalanuvchanlik kabi asosiy xususiyatlarga tayanadi va zamonaviy jamiyatda shaxs, jamiyat hamda davlat manfaatlarini himoya qilishning zaruriy sharti hisoblanadi.

2. Taklif etilgan uch darajali model axborot xavfsizligining har bir darajada o‘z himoya obyekti va tahdidlariga ega ekanini, ammo barcha darajalar bir-biri bilan uzviy bog‘liqligini ko‘rsatdi.

3. O‘zbekistonda davlat resurslarining texnik himoyasi va huquqiy bazasi kuchayib, bu xalqaro miqyosda e’tirof etilgan bo‘lsa-da, fuqarolarga qarshi kiberjinoyatlar keskin ko‘paymoqda. Bu inson omili axborot xavfsizligining eng zaif bo‘g‘ini ekanini tasdiqlaydi.

4. Axborot xavfsizligini ta’minlash faqat texnik va huquqiy choralar bilan cheklanmasligi, balki ta’lim, ma’rifat va kiber madaniyatni shakllantirishni o‘z ichiga olgan kompleks ijtimoiy siyosat sifatida amalga oshirilishi lozim.

Maqolaning ilmiy ahamiyati axborot xavfsizligining ijtimoiy jihatini O‘zbekistonning so‘nggi statistik ma’lumotlari asosida tahlil qilganida, amaliy ahamiyati esa ishlab chiqilgan tavsiyalardan ta’lim muassasalari va davlat tashkilotlarida foydalanish mumkinligida namoyon bo‘ladi.

FOYDALANILGAN ADABIYOTLAR

1. 15 mln kishining ma’lumoti sotuvda turgani yo‘q — Sherzod Shermatov [Elektron resurs] // Kun.uz. – 2026. – 12 fevral. – URL: https://kun.uz/news/2026/02/12/15-mln-kishining-malumoti-sotuvda-turgani-yoq-sherzod-shermatov
2. 2024-yilda O‘zbekistonda kiberjinoyatlar soni 9,1 barobarga oshgan [Elektron resurs] // Spot.uz. – 2025. – 29 may. – URL: https://www.spot.uz/oz/2025/05/29/cybercrime/

3. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. – 3rd ed. – Indianapolis: Wiley, 2020.
4. G‘aniyev S.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. Axborot-kommunikatsion tizimlar xavfsizligi: o‘quv qo‘llanma. – T.: Aloqachi, 2008. – 382 b.
5. International Telecommunication Union. Global Cybersecurity Index 2024. 5th Edition. – Geneva: ITU, 2024. – URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416*1b*Global-Cybersecurity-Index-E.pdf
6. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. – Geneva: ISO, 2022.
7. Muxtarov F.M. The complex of factors in improving the software and methodological provision of “Cyber security” science teaching in the period of information attacks // Science and Innovation. – 2024. – Vol. 3, Issue 5. – P. 205. – DOI: 10.5281/zenodo.11395451.
8. O‘zbekiston Respublikasi Ichki ishlar vazirligi. IIV Tezkor-qidiruv departamenti Kiberxavfsizlik markazi faoliyatiga bag‘ishlangan press-tur [Elektron resurs]. – 2025. – 29 may. – URL: https://gov.uz/oz/iiv/news/view/57775
9. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi «“Raqamli O‘zbekiston – 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida»gi PF-6079-son Farmoni // Qonunchilik ma’lumotlari milliy bazasi. – URL: https://lex.uz/docs/5031048
10. O‘zbekiston Respublikasi Prezidentining 2026-yil 10-martdagi «O‘zbekiston Respublikasining Kiberxavfsizlik strategiyasini belgilash va kiberjinoyatchilikning oldini olish tizimini takomillashtirish to‘g‘risida»gi PF-38-son Farmoni // Qonunchilik ma’lumotlari milliy bazasi. – URL: https://lex.uz/docs/-8079286

11. O‘zbekiston Respublikasining 2019-yil 2-iyuldagi «Shaxsga doir ma’lumotlar to‘g‘risida»gi O‘RQ-547-son Qonuni // Qonunchilik ma’lumotlari milliy bazasi. – URL: https://lex.uz/docs/-4396419
12. O‘zbekiston Respublikasining 2022-yil 15-apreldagi «Kiberxavfsizlik to‘g‘risida»gi O‘RQ-764-son Qonuni // Qonunchilik ma’lumotlari milliy bazasi. – URL: https://lex.uz/docs/5960604
13. O‘zbekistondagi axborot resurslariga kiberhujumlar 2,4 barobarga oshdi [Elektron resurs] // Kun.uz. – 2024. – 29 mart. – URL: https://kun.uz/news/2024/03/29/ozbekistondagi-axborot-resurslariga-kiberhujumlar-24-barobarga-oshdi
14. Stallings W., Brown L. Computer Security: Principles and Practice. – 4th ed. – New York: Pearson, 2018.
15. Whitman M.E., Mattord H.J. Principles of Information Security. – 7th ed. – Boston: Cengage Learning, 2021.