



KIBERJINOYATNING ZAMONAVIY JAMIYATGA BO'LGAN TA'SIRI

*Andijon davlat pedagogika instituti
Ijtimoiy fanlar kafedrasi o'qituvchilari
Jabborova Sayyoraxon Muxammadqobilovna
Ahmedov Abdulhay Toshto'xtayevich
Andijon davlat pedagogika instituti talabalari
Shavkatova Sevinch Shoyadbek qizi
Ravshanbekova Manzura Shokirjon qizi
Qodirjonova Dilnura Oybek qizi*

Annotatsiya: Kiberjinoyatlar Mazkur maqolada kiberjinoyatlar tushunchasi, ularning turlari va zamonaviy jamiyatga bo'lgan ta'siri yoritilgan. Kiberjinoyatlar axborot texnologiyalarining rivojlanishi bilan keng tarqalib, iqtisodiy, ijtimoiy va axborot xavfsizligiga jiddiy xavf tug'dirmoqda. Maqola davomida xakerlik, phishing, zararli dasturlar va onlayn firibgarlik kabi jinoyatlarning asosiy shakllari ko'rib chiqiladi. Shuningdek, kiberjinoyatlarining moliyaviy yo'qotishlar, shaxsiy ma'lumotlarning buzilishi va jamiyatda ishonchning pasayishiga olib keladigan oqibatlarini muhokama qilinadi. Kiberjinoyatlarga qarshi kurashda qonunchilik, texnologik himoya va foydalanuvchilarning xabardorligini oshirishning ahamiyati ta'kidlanadi. Maqola kiberxavfsizlik sohasida keng qamrovli tushunchalarni taqdim etib, zamonaviy tahdidlarni bartaraf etish yo'llariga e'tibor qaratadi.

Аннотация: В данной статье описывается понятие киберпреступлений, их виды и влияние на современное общество. Киберпреступления широко распространяются с развитием информационных технологий, создавая серьезную угрозу экономической, социальной и информационной безопасности. В статье рассматриваются основные формы преступности, такие как хакерство, фишинг, вредоносное ПО и онлайн-мошенничество. Также обсуждаются последствия киберпреступности, которая может привести к финансовым потерям, утечке персональных данных и утрате доверия к обществу. Он подчеркивает важность законодательства, технологической защиты и осведомленности пользователей в борьбе с киберпреступностью. В статье дан комплексный обзор кибербезопасности и акцентировано внимание на способах противодействия современным угрозам.



Abstract: Cybercrimes This article describes the concept of cybercrimes, their types and their impact on modern society. Cybercrimes are spreading widely with the development of information technologies, posing a serious threat to economic, social and information security. The article examines the main forms of crime such as hacking, phishing, malware and online fraud. It also discusses the consequences of cybercrime, which can lead to financial losses, personal data breaches, and loss of trust in society. It emphasizes the importance of legislation, technological protection and user awareness in the fight against cybercrime. The article provides a comprehensive overview of cyber security and focuses on ways to counter modern threats.

Ключевые слова: Киберпреступность, фишинг, фишинг, вредоносное ПО, программы-вымогатели, кибербезопасность, защита конфиденциальности, онлайн-мошенничество, информационная безопасность, интернет-угрозы, кибератака, утечка данных, киберпреступники, безопасность электронной коммерции, безопасность программного обеспечения.

Keywords: Cybercrime, phishing, phishing, malware, ransomware, cyber security, privacy protection, online fraud, information security, internet threats, cyber attack, data breach, cybercriminals, e-commerce security, software security .

Kirish. Kiber-jinoyatchilik nisbatan yangi tushuncha bo'lsada, ko'plab davlatlar iqtisodiyotiga qimmatga tushayotgan muammo. Jinoyat quroli – internet va eng so'nggi raqamli texnologiyalar. Mamlakatning harbiy, strategik tarmoqlarini ishdan chiqarish salohiyatiga ega. Buzg'unchi-xakerlarni topib jazolash esa oson ish emas, chunki ular davlatdan doimo bir qadam oldinda. Bugungi hayotni zamonaviy texnologiyasiz tasavvur qilish qiyin. Uyali aloqa va internet dunyosidagi so'nggi kashfiyotlar uzoqni yaqin, og'irni yengil, biznes imkoniyatlarni esa kengaytirgan. Biroq bu qulayliklar boshqa bir sohaga e'tibor qaratmoqda. Kiber-xavfsizlik har bir davlat uchun strategik masala. Avval asosan davlat sirlari va yuqori texnologiyalar nishonga olingan bo'lsa, hozir jinoyatchilar mo'ljalni kengroq olmoqda, deydi AQSh Federal Qidiruv Byurosi (FBI) rahbari Robert Myuller. "Google qidiruv tizimiga bo'lgan hujumlardan bilamizki, nafaqat hukumatlar, balki xususiy kompaniyalar ham bu tahdid oldida ojiz. Global iqtisodiy integratsiya bizga ko'p eshiklarni ochib berdi, jinoyatchilarga esa yangi imkoniyatlarni", - deydi Myuller. Qidiruv tizimi bilan mashhur Google



korporatsiyasi yaqinda u yuritadigan sistemalar nishonga olingani haqida xabar topdi. Jinoyat Xitoydan turib amalga oshirilgan¹.

Gap intellektual mulk, mualliflik huquqi va uni o'zlashtirishga urinish haqida ketmoqda. Google qatorida Yahoo, Dow Chemical va Northrop Grumman kabi 20 dan oshiq boshqa yirik kompaniyalar ham xurujlardan shikoyat qiladi. Internetda biznes yuritish xavfli bo'lib qolgan, deydi mutaxassislar. "Masalani qay jihatidan olib qaramang, ustunlik buzg'unchi-jinoyatchilar tomonida", - deydi ekspert Larri Klinton. "Qonunlar sust. Sohani yaxshi biladigan mutaxassislar kam. Xurujlarni uyushtirish oson va arzon. Qo'lidan kelgan odam katta mukofot oladi". Buning ustiga, o'tgan yillar ichida himoya texnologiyalari bobida uncha yangilik bo'lgani yo'q. Internet – xakerlar uchun cheksiz imkoniyatlar dunyosi. "Vaziyat juda murakkab. Hisoblarga ko'ra o'tgan yili Amerika bizneslari qariyb bir trillion dollarga teng intellektual mulkidan ayrilgan. Internet sekinligi, eski texnologiyalar ham katta muammo. Rendi Vikers AQSh Ichki xavfsizligi vazirligida shu masala bilan shug'ullanadi. Uning aytishicha, xuruj qayerda rejalani, uni kim amalga oshirmoqda, buni aniqlash mushkul vazifa." Zarur resurslar bo'lmasa, qidiruv somon ichidan nina qidirish bilan barobar. Hukumat buyurtmasi asosida ishlayotgan maxsus xizmat bo'lishi mumkin, yoki zimdan ish yuritayotgan boshqa bir idora. Birovni devorga taqash qiyin".

Jumboq kaliti, deydi Vikers, jinoyatlarni bir-biriga qiyoslashda.

"Ma'lumotni bir joyga to'plab, tahlil qilib, jinoyatchini izidan axtarib boramiz. Juda mayda ish, tinimsiz surishtiruv talab qiladi. Bu ishda maqsadni aniqlash juda muhim. Bu bir guruh faollarni yo hukumat? Yoki uyidan turib, mohirligini namoyish etayotgan bir talaba bo'lsachi?" Prezident Barak Obama nazarida kibernetik xavfsizlik XXI asrning eng dolzarb muammolaridan biri. Yadro va ommaviy qirg'in qurollaridan qolishmaydi. Amerikadek, odamlar hayotini kompyutersiz tasavvur qila olmaydigan jamiyatda, internet xavfsizligi ham birinchi o'rinda. Obama ma'muriyati o'tgan yili yangi idora ochib, bu vazifani unga yuklagan. "Mustahkam tizim butun jamiyatga foyda, chunki internet texnologiyalar kirib bormagan soha-sanoatning o'zi yo'q", - deydi internet xavfsizligi bo'yicha ekspert Larri Klinton. "Buzg'unchi virus-programmalar bir kompyuterdan ikkinchisiga ko'chib yurishi sir emas. Demak himoya tizimi barchani qamrab olishi kerak". Qo'shma Shtatlar internetdagi jinoyatlarga qarshi kurashga zo'r bermoqda, ammo bir paytning o'zida global tarmoqda erkinlikni ham targ'ib qilmoqda.

¹ <https://www-amerikaovozi-com.cdn.ampproject>.



Maxfiy ma'lumotlar qonuniy tarzda himoyalangan holatda yuz beruvchi kiberjinoiyatlar bilan bog'liq ko'pgina jinoyatlar mavjud. Xalqaro miqyosda hukumat ham, nodavlat subyektlar ham kiberjinoiyatlar, jumladan, josuslik, moliyaviy o'g'irlik va boshqa transchegaraviy jinoyatlar bilan shug'ullanadi. Xalqaro chegaralarni kesib o'tuvchi va kamida bitta milliy davlatning xatti-harakatlarini o'z ichiga olgan kiberjinoiyatlar ba'zan kiberurush deb ataladi. Uorren Baffet kiberjinoiyatni „insoniyatning birinchi raqamli muammosi“ deb ta'riflaydi va „insoniyat uchun real xavf tug'diradi“, deya qo'shimcha qilib o'tadi. 2014-yilda chop etilgan hisobotda (McAfee homiyligida) jahon iqtisodiyotiga yetkazilgan yillik zarar 445 milliard dollarni tashkil qilgan. Cybersecurity Ventures tomonidan 2016-yilgi hisobotda kiberjinoiyatlar natijasida yetkazilgan global zararlar 2021-yilga kelib yiliga 6 trillion dollargacha, 2025-yilga kelib esa 10,5 trillion dollargacha ko'tarilishi bashorat qilingan edi. 2012-yilda AQShda onlayn kredit va debet kartalaridagi firibgarlik oqibatida taxminan 1,5 milliard dollar yo'qotilgan. 2018-yilda Strategik va xalqaro tadqiqotlar markazi (CSIS) tomonidan McAfee bilan hamkorlikda o'tkazilgan tadqiqot shuni ko'rsatadiki, har yili global YaIMning qariyb bir foizi, ya'ni 600 milliard dollarga yaqini kiberjinoiyatlar tufayli yo'qoladi. Jahon Iqtisodiy Forumi 2020 Global Risk hisobotida uyushgan kiberjinoiyatlar idoralari jinoiy faoliyatni onlayn qilish uchun kuchlarni birlashtirayotganini tasdiqladi, shu bilan birga ularning aniqlash va jinoiy javobgarlikka tortilish ehtimoli AQShda 1 foizdan kamroqni tashkil qiladi. So'nggi yillarda raqamli texnologiyalar rivojlanishi bilan bir qatorda kiberjinoiyatlar ham ortib bormoqda. Kiberjinoiyatlar internet va axborot-kommunikatsiya texnologiyalari yordamida amalga oshiriladigan noqonuniy faoliyatlarni o'z ichiga oladi. Ushbu maqolada kiberjinoiyatlarning mohiyati, turlari, sabab va oqibatlari hamda ularga qarshi kurash yo'llari haqida so'z yuritiladi. Kiberjinoiyatlar turlari

Kiberjinoiyatlar turlicha shakllarda namoyon bo'ladi: Hujumlar va xakerlik: Xavfsizlik tizimlarini buzish va shaxsiy ma'lumotlarni o'g'irlash.

Moliya firibgarligi: Kredit karta ma'lumotlarini o'g'irlash yoki soxta to'lov tizimlari orqali pul o'g'irlash.

Foydalanuvchilarni manipulyatsiya qilish: Fishing (soxta elektron xatlar orqali Sabab va oqibatlar

Kiberjinoiyatlarning ortishiga bir nechta sabablarni ko'rsatish mumkin:

Texnologiya sohasida yetarli bilim va tajribaga ega bo'lmagan shaxslar.

Huquqiy bazaning yetarlicha mustahkam emasligi.

Axborot xavfsizligini ta'minlashda kamchiliklar.



Oqibatlari esa quyidagilardan iborat:

Korxonalar va jismoniy shaxslarga moliyaviy zarar yetkazish.

Shaxsiy ma'lumotlar maxfiylikning buzilishi.

Davlatning axborot xavfsizligiga tahdid solish.

Kiberjinoyatlarga qarshi kurash

Kiberjinoyatlarning oldini olish uchun quyidagi chora-tadbirlarni amalga oshirish zarur:

Raqamli savodxonlikni oshirish.

Maxfiylik va xavfsizlikni ta'minlovchi dasturlarni qo'llash.

Kiberjinoyatlarning huquqiy asosi va jazo choralari mustahkamlanishi. Milliy va xalqaro hamkorlikda kiberjinoyatlarga qarshi kurash tizimini yo'lga qo'yish. Kiber xavfsizlik mutaxassislari bizning kompyuter tizimlarimiz xakerlardan xavfsizligini ta'minlash uchun ishlaydi. Bundan tashqari, ular juda ko'p martaba yo'llari tanlash uchun, chunki ko'pchilik tashkilotlar o'z tizimlarini ishonchli va xavfsiz saqlash mahoratiga bog'liq. Siz ishlashingiz mumkin katta ma'lumotlar rivojlanayotgan texnologiyalarni takomillashtirish uchun o'z iste'dodlaringdan foydalaning yoki kiberjinoyatchilarni ushlashda huquqni muhofaza qilish idoralariga yordam berishingiz mumkin. Ba'zi kompaniyalar hatto "deb nomlanuvchi kiber xavfsizlik bo'yicha mutaxassislarni yollashadi. penetratsion sinovchilar Kelajakda ma'lumotlar buzilishining oldini olish uchun nima qilish kerakligini bilish uchun o'z tizimlarini qasddan buzish. Kiber xavfsizlik bo'yicha mutaxassislar bir qator shaxsiy xususiyatlarga ega bo'lishi mumkin va ko'nikmalari. Agar siz tafsilotlarga yo'naltirilgan bo'lsangiz, muammolarni hal qilishdan hayajonlaning va yaxshi muloqot qilsangiz, bu siz uchun maydon bo'lishi mumkin. Bryus Shneyer – kiber xavfsizlik bo'yicha mutaxassis².

Kiberxavfsizlik bo'yicha dunyodagi eng taniqli mutaxassislardan biri Bryus Shnayerdir. 12 dan ortiq kitob yozgan taniqli muallif Shnayer ba'zi radikal g'oyalar, jumladan shaxsiy ma'lumotlarimizni yanada xavfsizroq qilishimiz mumkin deb o'ylashi bilan tanilgan. Ma'lumotlarimiz Internetda turli joylarda tarqalish o'rniga, Shnayer barchamiz o'zimiznikiga ega bo'lishimiz kerak deb o'ylaydi ma'lumotlar "pod" shaxsiy kompyuterlarimiz, telefonlarimiz va boshqa qurilmalarimizdan yig'ib olindi. Shnayerning so'zlariga ko'ra, ushbu podkastlar bizning ma'lumotlarimizni xavfsizroq qilishlari mumkin edi, chunki ular bizga tegishli edi, demak biz unga

² Karimov S. "Kiberjinoyatlar va ularning huquqiy yechimlari". O'zbekiston Respublikasi IIV nashri, 2021.



kimning kirish huquqini boshqarishimiz kerak. “Bu narsa hamma narsa kompyuter bo’lgan va hamma narsa siz haqingizda ma’lumot ishlab chiqaradigan dunyoda kuchlar muvozanatini tubdan o’zgartiradi”, deb yozadi Shneyer o’z blogida “Shnayer xavfsizlik to’g’risida, “.

O‘zbekiston Respublikasining “Kiberxavfsizlik to’g’risida”gi Qonunning Maqsadi kiberxavfsizlik sohasidagi munosabatlarni tartibga solishdan iborat³ Bo’lib, unda kiberxavfsizlikka oid asosiy tushanchalar, kiberxavfsizlikni Ta’minlashning asosiy prinsiplari, mazkur sohaning davlat tomonidan tartibga Solish, davlat organlari va tashkilotlarining kiberxavfsizlikni ta’minlash Borasidagi huquq va majburiyatlari, kiberxavfsizlikni ta’minlash masalalari, Kiberxavfsizlik hodisalarini tekshirish va ular bo’yicha choralar ko’rish, muhim Axborot infratuzilmasi ob’ektlari va ularning kiberxavfsizligini ta’minlashning Asosiy yo’nalishlari, kiberxavfsizlik sohasini qo’llab-quvvatlash va rivojlantirish masalalari nazarda tutilgan. Tahlillarga ko’ra, dunyo bo’ylab har yili 500 milliondan ortiq kiber hujumlar uyushtiriladi. Har soniyada 12 nafar insondan biri kiber makonda sodir etilgan hujumlar qurboniga aylanadi. Amerika Qo’shma Shtatlari, Fransiya, Angliya, Germaniya, Belgiya, Luksemburg kabi rivojlangan davlatlarda jinoyatlarning 60-65 foizi kiber hujumlar orqali sodir etilmoqda. O‘zbekistonda ham so‘nggi uch yilda bu turdagi jinoyatlar 8,3 baravarga ko‘payib, hozirda umumiy jinoyatchilikning qariyb 5 foiziga yetgan. Xususan, noqonuniy bank-moliya operatsiyalari orqali o‘zgalarning plastik kartadagi mablag‘larini o‘zlashtirish, zararli viruslar tarqatish, qimor va tavakkalchilikka asoslangan onlayn o‘yinlar, diniy aqidaparastlikka qaratilgan axborot xurujlari, onlayn savdo maydonidagi firibgarlik jinoyatlari ko‘payib bormoqda. Achinarlisi, axborot texnologiyalari yordamida huquqbuzarlik va jinoyatga qo‘l urgan shaxslar orasida yoshlar ko‘pchilikni tashkil etmoqda. Respublikamizda virtual olamdagi qonunbuzilishlarning aksariyati 16-23 yosh oralig‘idagi o‘smir-yoshlar tomonidan sodir qilinmoqda. Bundan ko‘rinib turibdiki, kiberxavfsizlikni ta’minlash masalasi bugun har qachongidan ham dolzarb ahamiyat kasb etmoqda.

Ilmiy-amaliy anjumanda ichki ishlar vazirining axborot texnologiyalari bo’yicha o‘rinbosari Najmiddin Turaxodjayev, vazirlik Tezkor-qidiruv hamkorligi boshqarmasi Kiberxavfsizlik markazi boshlig‘I Behzod Mamadjanov, Ekspert-kriminalistika bosh markazi boshlig‘I Saidolim Nuriddinov, Tergov departamenti

³ O‘zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni 2021-yil 30-aprelda qabul qilingan.



boshqarma boshlig‘I o‘rinbosari Ulug‘bek Avilov, Respublika Markaziy banki bosh eksperti Dilshod Ismailov, “Kiberxavfsizlik markazi” davlat unitar korxonasi bosh mutaxassisi Farrux Husenov, Mudofaa vazirligi Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti boshlig‘I o‘rinbosari Baxtiyorjon Rahimov, Axborotlashtirish va telekommunikatsiya texnologiyalari sohasida nazorat bo‘yicha davlat inspeksiyasi mutaxassisi Ma‘mura Mamadjanovalar so‘zga chiqishdi. Ekspertlar tomonidan kiberjinoyatlarga qarshi kurashishning zamonaviy tendensiyalari, internet tarmog‘I orqali sodir etilayotgan qonunbuzilishlarning oldini olish, sohaning huquqiy asoslarini mustahkamlash, axborot texnologiyalaridan foydalanib amalga oshirilgan jinoyatlarni kriminalistik tadqiq etish, fosh etish va tergov qilishning o‘ziga xos xususiyatlari, kiberxavfsizlikni ta‘minlashda davlat idoralari va xususiy sektorlar hamkorligini muvofiqlashtirish borasida firkmulohazalar bildirildi. Shuningdek xorijiy davlatlarning kiber jinoyatlarga qarshi kurashish sohasi bo‘yicha malakali mutaxassislarini tajriba almashishga jalb etish, kiberxavfsizlikni ta‘minlashga qaratilgan chora-tadbirlar samaradorligini oshirish, Ichki ishlar vazirligi akademiyasining imkoniyatlaridan foydalanib kelgusida ushbu turdagi jinoyatlarni fosh etish va tergov qilish bo‘yicha alohida ixtisoslik yo‘nalishi tashkil etib, malakali mutaxassis kadrlarni tayyorlash yuzasidan takliflar o‘rtaga tashlandi. Anjuman so‘nggida mazkur sohada o‘zaro tajriba almashishni yo‘lga qo‘yish va kadrlar salohiyatini rivojlantirish maqsadida Ichki ishlar vazirligi akademiyasi Dasturiy mahsulotlar va axborot texnologiyalari texnologik parki hamda Toshkent shahridagi Inha universiteti bilan hamkorlik memorandumlarini imzoladi.

Kiberjinoyat: Zamonaviy muammolar va himoya choralari

Kiberjinoyatlar zamonaviy jamiyatning eng dolzarb muammolaridan biri bo‘lib, texnologiyalar rivoji bilan birga tez sur‘atlarda kengayib bormoqda. Bu turdagi jinoyatlar internet va raqamli texnologiyalar orqali sodir etilib, shaxsiy, davlat va korporativ ma‘lumotlarga jiddiy zarar yetkazadi. Ushbu maqolada kiberjinoyatlarning turlari, ularning oqibatlari va himoya choralari haqida so‘z yuritamiz.

Kiberjinoyatlarning turlari. Kiberjinoyatlar turli shakllarda namoyon bo‘lishi mumkin. Quyida eng keng tarqalgan turlari keltirilgan: Shaxsiy ma‘lumotlarni o‘g‘irlash: Bu turdagi jinoyatlar shaxsiy va moliyaviy ma‘lumotlarni noqonuniy yo‘llar bilan qo‘lga kiritishni o‘z ichiga oladi. Masalan, bank kartalari ma‘lumotlarini o‘g‘irlash yoki shaxsiy fayllarni buzish. Firibgarlik:



Internet orqali soxta xizmatlar yoki mahsulotlarni taklif qilib.foydalanuvchilardan pul o'g'irlash. So'nggi yillarda onlayn savdo firibgarliklari keng tarqalgan.

Xakerlik:Kompyuter tizimlariga noqonuniy kirish orqali ma'lumotlarni buzish, o'zgartirish yoki o'g'irlash. Bu holatda xakerlar davlat va tijorat tashkilotlariga katta zarar yetkazadi.Zararli dasturlar (viruslar):⁴ Viruslar va zararli dasturlarni tarqatish orqali kompyuter tizimlarini ishdan chiqarish yoki foydalanuvchilarning shaxsiy ma'lumotlarini o'g'irlash.DdoS hujumlari:Tashkilotlarning serverlari yoki veb-saytlariga hujum qilib, ularni ishdan chiqarish.Kiberjinoyatlarning oqibatlar.Moliyaviy zarar:Kiberjinoyatlar natijasida yirik tashkilotlar va oddiy fuqarolar katta moliyaviy yo'qotishlarga duch keladi.Obro'ga zarar:Kompaniyalar va tashkilotlarning ma'lumotlari o'g'irlangan taqdirda, mijozlarning ishonchi yo'qoladi.

Shaxsiy xavfsizlikning buzilishi:

Shaxsiy ma'lumotlar noqonuniy ishlatilishi natijasida jabrlanuvchilar ruhiy va ijtimoiy muammolarga duch keladi.Kiberjinoyatlardan himoyalani choralari.Kuchli parollar:Har bir xizmat uchun noyob va murakkab parollardan foydalaning.

Antivirus dasturlari:Kompyuteringizni zararli dasturlardan himoyalash uchun yangilangan antivirus dasturlarini o'rnatib foydalaning.Duo faktorlash autentifikatsiyasi Ikki bosqichli tasdiqlash orqali hisoblarni qo'shimcha himoya qilish.Shubhali manbalardan saqlanish:Soxta yoki noma'lum veb-saytlar va elektron pochta havolariga kirmang.Ma'lumotlarni shifrlash:Muhim ma'lumotlarni shifrlash orqali ularni xavfsiz saqlash.

Xulosa: Zamonaviy global tahdidlarga qarshi kurashish va ularni kamaytirish uchun faqatgina milliy darajada emas, balki xalqaro miqyosda ham samarali va birgalikdagi harakatlar talab etiladi. Kiberjinoyatlarni oldini olish, ekologik inqirozlarni bartaraf etish, iqtisodiy beqarorlikni kamaytirish va pandemiyalarni boshqarish kabi muammolarni hal qilishda davlatlar, xalqaro tashkilotlar, texnologik kompaniyalar va jamiyatning barcha qatlamlari o'z mas'uliyatini anglab, faol ishtirok etishlari zarur. Shu tarzda, zamonaviy tahdidlarga qarshi kurashish va ularni kamaytirish mumkin bo'ladi.

⁴ "Axborot xavfsizligi bo'yicha xalqaro konvensiyalar to'plami". Toshkent, 2022.



Foydalanilgan adabiyotlar

1. Matyoqubov N. “Axborot xavfsizligi asoslari”. Toshkent, 2020.
2. Karimov S. “Kiberjinoyatlar va ularning huquqiy yechimlari”. O‘zbekiston Respublikasi IIV nashri, 2021.
3. “Axborot xavfsizligi bo‘yicha xalqaro konvensiyalar to‘plami”. Toshkent, 2022.
4. Internet resurslar:
www.cybersecurity.uz
www.kiberxavfsizliklari
<https://iiv.uz/news/kiberjinoyatchilikka-qarshi-kiberxavfsizlik>
<https://www.amerikaovozi.com/a/a-36-2010-03-26-voa1-93371769/807021.html>
5. S.K.Ganiyev, A. A. Ganiyev, Z. T. Xudoyqulov Kiberxavfsizlik asoslari. O‘quv qo‘llanma. –T. : “Toshkent” 2020.
6. Jabborova, S., Erkinova, I., & Shokirova, Z. (2024). VIRTUAL O‘YINLARNING YOSHLAR ONGIGA TA’SIRI. *Ilm-fan va ta'lim*, (6 (21)).
7. Jabborova, S., Mirzadavlatova, U., & Kozimova, G. (2024). TA’LIM VA TARBIYA JARAYONIDA AXBOROTNING O’RNI VA AHAMIYATI. *Ilm-fan va ta'lim*, (6 (21)).
8. Jabborova, S., Ismatillayeva, I., Fozilova, R., & Sul-tonboyev, A. (2024). TEXNOLOGIK TARAQQIYOTNING ISTIQBOLLARI. *Ilm-fan va ta'lim*, (6 (21)).
9. Jabborova, S., Daminjonova, S., Ismoilova, G., & Mamatqodirova, M. (2024). AXBOROTNING INSON HAYOTIGA TA’SIRI. *Ilm-fan va ta'lim*, (6 (21)).
10. Jabborova, S., Olimjanova, H., & Shodmonova, S. (2024). INTERNETDAN SAMARALI FOYDALANISH-DAVR TALABI. *Ilm-fan va ta'lim*, (6 (21)).
- Bahodir o‘g‘li, V. S. (2024). YURTIMIZDA ARABLAR BOSQINI VA ISLOM DININING KIRIB KELISHI. *WORLD OF SCIENCE*, 7(10), 40-44.
11. Asadbek, M., & Davronbek, I. (2023). O‘ZBEKISTON-2030 STRATEGIYASINING YANGI O‘ZBEKISTONNI BARPO ETISHNING KAFOLATI. *Ustozlar uchun*, 24(1), 204-207.
12. Dilshodbek o‘g‘li, I. D. (2023). O‘ZBEKISTONDA SIYOSIY PARTIYALARNING JAMIYAT HAYOTIDAGI O’RNI VA AHAMIYATI. *Journal of new century innovations*, 29(4), 115-120.
13. Dilshodbek o‘g‘li, I. D. (2023). O‘ZBEKISTON RESPUBLIKASI TA’LIM TIZIMIDA XALQARO VAHOLASH DASTURLARI, METODLARI VA TEXNOLOGIYALARINI JORIY QILISHNING HUQUQIY ASOSLARI. *ОБРАЗОВАНИЕ НАУКА И ИННОВАЦИОННЫЕ ИДЕИ В МИРЕ*, 21(7), 102-110.
14. Ahmedov, A. T. (2024). KASABA UYUSHMA TASHKILOTINING HUQUQIY ASOSLARI-DEMOKRATIYA VA OSHKORALIK PRINSIPLARINI SHAKLLANISHI. *Экономика и социум*, (4-1 (119)), 54-59.
15. AHMEDOV, A. (2024). KASABA UYUSHMA TASHKILOTLARINING BOSHQA JAMOAT TASHKILOTLARI BILAN O‘ZARO HAMKORLIKLARI. *News of the NUUZ*, 1(1.9), 60-63.