# KIBER JINOYATCHILIKKA - KIBER XAVFSIZLIK

**Abduvaliyev Ulug‘bek Shavkat o‘g‘li**
*Ishtixon tuman Ichki ishlar bo’limi Tezkor qidiruv xizmati Jinoyat qidiruv bo’linmasi tezkor vakili, leytenant*
*(tel: +99899-082-43-01)*

**Annotatsiya.** *Axborot texnologiyalari jadallik bilan rivojlanib borayotgan bir vaqtda, internet tarmoqlari butun dunyo jamiyatiga, insonlarning hayoti, mulki, daxlsizligiga ham bir qancha muammolar olib kelmoqda. Hozirgi kunda ma’lumotlarni xavfsiz saqlash, ularga nisbatan bo’lishi mumkin bo’lgan hujumlardan himoya qilish eng katta muammolardan biridir. Masalan “CIBER” iborasini eshitganimizda hammaning hayolida kundan-kunga jadallik bilan rivojlanishda bo’lgan, ko’plab insonlarni og’ir ahvolga solib qo’ygan kiber jinoyatchilik gavdalanadi. Ushbu sohada turli xil kompaniyalar hamda davlat hukumatlari tomonidan kiber jinoyatlarning oldini olish uchun ko’plab ishlar amalga oshirilmoqda. Lekin amalga oshirilayotgan ishlar natijasida kiber jinoyatchilik hali ham o’z xavfini insonlarga tarqatib kelmoqda. Ushbu maqola kelajakda sodir etilishi mumkin bo’lgan hamda hozirgi kunda sodir etilib kelayotgan kiber jinoyatlarni oldini olish va ularga barham berishda kiber xavfsizlikning o’rni yoritilib beriladi.*

**Kalit so‘zlar:** *kiber, jinoyat, kiber jinoyatchilik, kiber xavfsizlik, internet tarmoqlari, shaxsiy xavfsizlik, ma’lumotlar xavfsizligi,jinoyatlarni oldini olish, firibgarlik, veb-saytlar, xakkerlik, rekvizitlar,fishing.*

**Annotation**. *At the same time as information technology is developing rapidly, internet networks are also bringing several problems to the Society of the whole world, the life, property, inviolability of people. Nowadays, keeping data safe, protecting against possible attacks on them is one of the biggest problems. For example, when we hear the phrase” CIBER", cybercrime is embodied in everyone's imagination, which is rapidly developing from day to day, putting many people in a difficult position. Many works are being done in this area by various companies as well as state governments to prevent cybercrime. But as a result of the work being done, cybercrime is still spreading its danger to humans. This article highlights the role of cyber security in preventing and ending cyber crimes that may occur in the future as well as currently occurring.*

**Keywords:** *cyber, crime, cybercrime, cyber security, internet networks, personal security,data security, crime prevention, fraud, websites, hacking,props, phishing.*

Kirish. Asrimizning global muammolari qatoriga yangidan-yangi turlari bilan tilga olinayotgan kiberjinoyatchilik kirib kelganiga ham ancha bo'ldi. Uning bizga ma'lum bo'lgan virusli dasturlarni tarqatish, parollarni buzib kirish, kredit karta va boshqa bank rekvizitlaridagi mablag'larni o'zlashtirish talon-toroj qilish, shuningdek, internet orqali qonunga zid axborotlar, xususan, bo'hton, ma'naviy buzuq ma'lumotlarni tarqatish bilan bashariyat hayotiga katta xavf solayotganidan ko'z yuma olmaymiz. Shuningdek kompyuter vositalari, internet tarmoqlar hamda axborot texnologiyalarining tezlik bilan rivojlanishi, yangi-yangi turlarining yaratilishi foydalanuvchilarga shunchaki birgina tugmani bosish bilan matn shaklda hamda audio yoki video orqali har qanday ma’lumotlarni uzatish yoki qabul qilish imkoniyatini bermoqda. Albatta bunday qulayliklar insonlarning uzog’ini yaqin qilmoqda, ularning vaqtlarini tejashga eng qulay vosita bo’lib xizmat qilmoqda. Lekin ma’lumotni qay darajada xavfsiz almashilinmoqda yoki boshqa insonga axborot qanchalik xavfsiz yetib borayotganligi haqida hech o‘ylab ko‘rganmiciz? Bu savolning javobi kiber xavfsizlikdan topa olishimiz mumkin. «Kiberjinoyatchilik» tushunchasi axborot-kommunikatsiya texnologiyalari vositalaridan foydalangan holda, virtual tarmoqda dahshat solish, virus va boshqa zararli dasturlar, qonunga zid axborotlar tayyorlash va tarqatish, elektron xatlarni ommaviy tarqatish (spam), xakerlik hujumi, veb-saytlarga noqonuniy kirish, firibgarlik, ma'lumotlar butunligi va mualliflik huquqini buzish, kredit kartochkalari raqami hamda bank rekvizitlarini o'g'irlash (fishing va farming) va boshqa turli huquqbuzarliklar bilan izohlanadi.

(Kiber jinoyat — kompyuter va tarmoqning birgalikdagi aloqasi ostida sodir etiluvchi jinoyat turi. Kompyuter jinoyat paytida maqsadli yo‘naltirilgan qurol vazifasini bajarib beradi. Kiberjinoyat kimningdir xavfsizligi va moliyaviy holatiga zarar yetkazish maqsadida sodir etiladi.)

Bugungi kunda atrofimizda sodir etilayotgan jinoyatlarning 40% ni kompyuter orqali sodir etilgan firibgarlik jinoyati tashkil etadi. Kompyuter firibgarligi — bu boshqa shaxsni mulkiy yo‘qotishga olib keladigan biror narsa qilish yoki qilmaslikka imkon berish uchun haqiqatni har qanday noto‘g‘ri ko‘rsatish. Shu nuqtai nazardan, firibgarlik quyidagi yo‘llar bilan foyda olishga olib keladi:

Ruxsatsiz tarzda o‘zgartirish. Bu kichik texnik tajribani talab qiladi va xodimlar tomonidan ma’lumotlarni kiritish yoki noto‘g‘ri ma’lumotlarni kiritishdan oldin ma’lumotlarni o‘zgartirish yoki ruxsatsiz ko‘rsatmalar kiritish yoki ruxsat etilmagan jarayonlardan foydalanish orqali o‘g‘irlashning keng tarqalgan shaklidir;

Saqlangan ma’lumotlarni o‘zgartirish yoki o‘chirish.

Boshqa firibgarlik shakllari kompyuter tizimlari yordamida osonlashtirilishi mumkin, jumladan bank firibgarligi, karding, shaxsni o‘g‘irlash, tovlamachilik va maxfiy ma’lumotlarni o‘g‘irlash. Ushbu turdagi jinoyatlar ko‘pincha shaxsiy ma’lumotlar yoki pul ma’lumotlarining yo‘qolishiga olib keladi.

Texnologiya taraqqiyoti va ko‘proq odamlar bank yoki kredit karta ma’lumotlari kabi nozik ma’lumotlarni saqlash uchun internetga tayanishi sababli, jinoyatchilar bu ma’lumotlarni o‘g‘irlashga harakat qilmoqdalar. Kiberjinoyat butun dunyo bo‘ylab odamlar uchun ko‘proq xavf tug‘dirmoqda. Axborot qanday himoyalanganligi va jinoyatchilar ushbu ma’lumotni o‘g‘irlash uchun qo‘llaydigan taktikalar haqida xabardorlikni oshirishning ahamiyati ortib bormoqda. ichki ishlar vazirligi kiber xavfsizlik markazi ma’lumotlariga ko‘ra 2023-yilning 8 oyi mobaynida kelib tushgan ariza shikoyatlarning 70% ga yaqini bank plastik kartalaridan pullarning o’z egasining ruxsatisiz o’zlashtirilib olishi yuzasidan ekanligi ham foydalanuvchilarga ogohlikni talab etadi. Har qanday sababga ko‘ra internetdan foydalanadigan har bir kishi qurbon bo‘lishi mumkin, shuning uchun onlayn rejimida qanday qilib himoyalanganligi haqida bilish muhimdir. Hozirda internet har kunlik hayotning eng tez o‘sayotgan infratuzilmasidir. Bugungi texnika dunyosida eng so‘nggi texnologiyalar inson yashash tarzini o‘zgartirib yubormoqda, masalan internet foydalanuvchilar uyidan chiqmagan holda har xil ishlarni (online kredit olish, online savdoda xarid amalga oshirish, biletlar buyurtma qilish, online ishlarini bajarish va boshqalar) bajara olishadi . Lekin yangi chiqayotgan texnologiyalar tufayli biz axborotimizni eng samarali yo‘l bilan ham xavfsiz saqlay olmaymiz va shuning uchun kiber jinoyatlar kundan-kunga ko‘payib bormoqda. Hozirda 60% dan ortiq moliyaviy kelishuvlar, har hil shartnomalar internet orqali amalga oshiriladi, shuning uchun bu soha katta miqdordagi kelishuvlar uchun eng yaxshi sifatli xavfsizlikni talab qiladi.

Kiber xavfsizlikning ko‘lami faqatgina axborot texnologiyalari sanoatida axborotni himoyalash yemas, internet foydalanuvchilarida kiber jinoyatchilik haqidagi dastlabki tushunchalarni berib o’tish, ulardan qay tarzda himoyalanish yo’llarini berib o’tish orqali ham natijaga erishishimiz mumkin. Mobil to‘lovlar, elektron savdo-sotiq, internet bank, online kredit kabi eng so‘nggi texnologiyalar ham yuqori darajadagi xavfsizlik talab yetadi. Bu texnologiyalar foydalanuvchisiga tegishli muhim ma’lumotlarni xavfsiz saqlash juda muhimdir. Kiber xavfsizlikni rivojlantirish va muhim ma’lumot infratuzilmalarini saqlash har bir millatning xavfsizligi va iqtisodiy ahvoli uchun zarur. Internetni xavfsizlashtirish (foydalanuvchilarini himoya qilish) hukumat siyosati kabi yangi xizmatlar rivojlanishining ajralmas qismidir. Insonlar orasida Kiber jinoyatga qarshi kurash

izchil, tushunarli va xavfsiz yondashuv talab qiladi. Texnologiyalarda yaratilgan xavfsizlik bosqichlari ko’plab kiber jinoyatlarga sabab bo’lib qolganligi uchun huquqni muhofaza qiluvchi organlarga jinoyatlarni oldini olishga, fosh yetishga va ularga qarshi kurashishga bog’liq bo’lgan vazifalar biriktirilganligi hamda Ichki ishlar vazirligi tizimida Kiber xavfsizlik bo’limlarining tashkil etilganligi kiber xavfsizlikning ta’minlanishida eng asosiy omildir. Hozirda ko‘plab davlatlar muhim ma’lumotlar yo‘qolishini oldini olish uchun kiber xavfsizlikka oid qat’iy qoidalar joriy qilmoqdalar. Har bir inson o‘zini kiber xavfsizligi va ko‘payib borayotgan kiber jinoyatdan saqlanish uchun tayyor bo‘lishi zarur. Kiber jinoyat. Kiber jinoyat internet va kompyuterni o‘g‘rilik va shu kabi jinoyatda asosiy qurol qilib olgan har qanday qonun bilan tqiqlangan hamda qonun bilan himoya qilinadigan ijtimoiy munosabatlarga xavf soluvchiu, zarar beruvchi noqonuniy harakatdir.

Shu o'rinda kiberterrorizm va uning jamiyat hayotiga solayotgan xavfining ko'lami ham oshib borayotganini ta'kidlash joiz.

Kiberterrorchi — bu hukumat yoki tashkilotni kompyuterlar, tarmoqlar yoki ularda saqlangan ma’lumotlarga qarshi kompyuter hujumi uyushtirish orqali o‘zining siyosiy yoki ijtimoiy maqsadlariga erishish uchun qo‘rqitadigan yoki majburlaydigan shaxs. Kiberterrorizm, umuman olganda, kibermakon yoki kompyuter resurslaridan foydalanish orqali sodir etilgan terrorchilik harakati sifatida ta’riflanishi mumkin . Shunday qilib, bayram kunlarida bombali hujumlar sodir bo‘lishi haqida Internetda oddiy targ‘ibot materiali kiberterrorizm deb hisoblanishi mumkin. Shuningdek, ayrim shaxslarga, oilalarga qaratilgan, tarmoqlar ichida guruhlar tomonidan tashkil etilgan, odamlar o‘rtasida qo‘rquv uyg‘otish, hokimiyatni namoyish etish, odamlar hayotini barbod qilish uchun zarur bo‘lgan ma’lumotlarni to‘plash, talonchilik, shantaj va hokazolarga qaratilgan xakerlik faoliyati ham mavjud Kiberterroristik harakat (kiberhujum) - kompyuterlar va axborot kommunikatsiya vositalari yordamida amalga oshirilgan, odamlarning hayoti va sog'lig'iga bevosita xavf tug'diradigan yoki potentsial xavf tug'dirishi mumkin bo'lgan, moddiy ob'ektlarga katta zarar yetkazishi yoki shunga olib kelishi mumkin bo'lgan, ijtimoiy xavfli oqibatlarning boshlanishi yoki maqsadi bo'lgan siyosiy sababdir. Zamonaviy terrorchilar uchun kibermakondan foydalanishning jozibadorligi kiberhujumni amalga oshirish katta moliyaviy xarajatlarni talab qilmasligi bilan bog'liq. ekspertlarning xulosasiga ko'ra, bu rivojlanayotgan davlatlarning taraqqiyotiga ko'maklashish, umuminsoniy demokratik tamoyillarni qaror toptirish niqobi ostida fuqarolar ongiga ta'sir o'tkazish, ularni turli yo'llar bilan o'z maqsadlari sari bo'ysundirish orqali amalga oshirilmoqda. Afsuski, bu jarayonda kiberhujumlarni uyushtirish, bu yo'lda internet global tarmog'ining mislsiz imkoniyatlaridan «samarali» foydalanishga urinishlar tobora avj olmoqda.

Ijtimoiy tarmoqlar egalari ushbu tarmoqlar sahifalarida davlat tuzumini ag'darishga da'vat qilingani uchun javobgarlikka tortilishining xalqaro miqyosdagi huquqiy asoslari yaratilmagan. Vaholanki, har bir qilingan jinoiy xatti-harakat yoki harakatsizlik mazmun-mohiyatiga ko'ra, albatta, javobsiz va jazosiz qolmasligi kerak. Internet saytlari to'satdan paydo bo'lib, ko'pincha formatini, so'ngra manzilini o'zgartiradi. Shu bois ayrim ekspertlar internetning butkul ochiqligi kabi dastlabki kontseptsiyalardan voz kechib, uning yangi tizimiga o'tishni taklif etmoqda.

Yangi modelning asosiy mohiyati tarmoqdan foydalanuvchilarning anonimligidan voz kechishdir. Bu tarmoqning jinoiy tajovuzlardan yanada ko'proq himoyalangan bo'lishini ta'minlashga imkon berdi. Misol tariqasida, yopiq tarmoq tizimiga o'tgan Xitoy davlatini va bunday jarayonga tayyorgarlik ko'rayotgan Koreya, Yaponiya hamda Rossiya davlatini keltirishimiz mumkin. Jahon hamjamiyatiga integratsiyalashayotgan mamlakatimizda axborot kommunikatsiya texnologiyalari, axborot tizimlari va zamonaviy kompyuter texnologiyalaridan samarali foydalanish bo'yicha izchil davlat siyosati olib borilmoqda.

Bugungi kunda mamlakatimizda joriy etilayotgan zamonaviy raqamli texnologiyalar, fuqarolarimizga qator qulayliklar va imkoniyatlar eshigini ochmoqda. Mazkur jarayon bilan bir qatorda, yaratilayotgan raqamli texnologiyalar va axborot tizimlarining xavfsizligini ta'minlash muammosi ham mavjud, albatta.

Bu eng dolzarb masalalardan biri - kiberxavfsizlikni ta'minlash, sodir etilishi mumkin bo'lgan kiberjinoyatlarning oldini olish va unga qarshi kurashish masalasi hisoblanadi. Kundan-kunga takomillashib ketayotgan kiberjinoyatchilikka qarshi kiberxavfsizlikni ta'minlashda quyidagi asosiy talablarni bajarish orqali ulardan himoyalanish, ya'ni kiberxavfsizlikni ta'minlashimiz mumkin: xodimlarga axborot xavfsizligi asoslarini o'rgatish ya’ni huquqni muhofaza qilish organ xodimlari kiber jinoyatchilikka qarshi kurashishda kiber xavfsizlikni ta’minlashdan oldin o’zlari shu muammolarning kelib chiqish sabablarini va bu kabvi holatlar qay tarzda amalga oshirilganligini bilishlari kerak; foydalanayotgan dasturiy mahsulotlarning zaifliklarini doimiy sinovdan o'tkazish; ishonchli antivirus dasturidan foydalanish; litsenziyalangan rasmiy dasturlardan foydalanish; axborot tizimlarini himoyalashda ko'p faktorli autentifikatsiyadan foydalanish; parollardan foydalanishda kuchli parolni saqlash siyosatiga rioya qilish; muntazam ravishda kompyuter qattiq disklaridagi ma'lumotlarni shifrlash. Shu o'rinda, mamlakatimizda kiberjinoyatlarning oldini olish va unga qarshi kurashni olib boruvchi vakolatli davlat idoralariga ham muayyan vazifalar yuklanishini alohida ta'kidlash lozim.

Xususan, ular kiberjinoyatchilikka qarshi kurash faoliyatida O'zbekiston Respublikasi va uning xalqini axborot texnologiyalari va kommunikatsiyalari orqali amalga oshirilayotgan yoki bunga imkon berayotgan shaxs, jamiyat va davlat xavfsizligini va ularning manfaatlari tashqi hamda ichki kibertahdidlardan himoya qilinishini ta'minlash, mazkur sohada qonuniylik va qonun ustuvorligini mustahkamlash, kiberjinoyatlar va kiberhuquqbuzarliklarning oldini olish, ularni aniqlash va barham berish kabi vazifalarni amalga oshirishi darkor.

Shuningdek, kiberjinoyatlar va kiberhuquqbuzarliklarni tergov qilish va ularni aniqlash, bartaraf etish hamda oldini olish bo'yicha zarur qarorlar qabul qilish, kiberjinoyatchilikka qarshi kurashish bo'yicha normativ-huquqiy hujjatlar loyihalarini ishlab chiqishda ishtirok etish, kiberterrorizm, kiberekstremizm, uyushgan jinoyatchilikka qarshi kurashish, davlat organlari manfaatlariga hamda kiberxavfsizligiga tahdid soluvchi kiberhatarlarni aniqlash va ularga qarshi kurashish, kiberjinoyatlar bo'yicha tergovga qadar tekshiruv va dastlabki tergovni o'tkazish, tezkor-qidiruv faoliyatini amalga oshirish, fuqarolarning huquq va erkinliklariga tahdid soluvchi kiberjinoyatlarning sodir etilishiga imkon yaratuvchi sabablar hamda shart-sharoitlarni aniqlash va bartaraf etish kabi muhim vazifalarni bajarishlari lozim.

## FOYDALANILGAN ADABIYOTLAR:


1. O’zbekiston Respublikasining Konstitutsiyasi
2. O’zbekiston Respublikasining Jinoyat kodeksi – 128 moddasi
3. O’zbekiston Respublikasining Jinoyat protsessual kodeksi
4. Security and Privacy Magazine. IEEECS Safety Critical Systems – Next Generation. 2013
5. "Science and Education" Scientific Journal
6. 233 www.openscience.uz[2] G. Nikhita Reddy, G.J. Ugander Reddy. Study of Cloud Computing in
7. HealthCare Industry. 2013
8. Daniel, Schatz, Julie, Wall. Towards a More Representative Definition of Cyber Security. 2012
9. Marcel, Sébastien. Handbook of Biometric Axborot vositalarining kiber xavfsizlikdagi o‘rni. nti-Spoofing. London. England. 201
10. Lewis J.A. Cybersecurity and Critical Infrastructure Protection. Washington DC, USA. 2006
11. https://uz.wikipedia.org/wiki/Kiberjinoyat

12. Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime, " Cleveland, Mississippi: Anderson Publishing.
13. Bossler, Adam M.; Berenblum, Tamar (2019-10-20). „Introduction: new directions in cybercrime research“. Journal of Crime and Justice. 42-jild, № 5. 495–499-bet.