ISSN: 2181-3906 2026

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 5 / ISSUE 5 / UIF:8.2 / MODERNSCIENCE.UZ

ZAMONAVIY SHAROITDA AXBOROT TEXNOLOGIYALARIDAN FOYDALANGAN HOLDA O‘ZGALAR MULKINI TALON-TAROJ QILISH BILAN JINOYATLARGA QARSHI KURASHISHNING DOLZARB MASALALARI

Abduraxmonova Gulsanam Ikromjon qizi
Jahon iqtisodiyoti va diplomatiya universiteti
“Xalqaro huquq” fakulteti 2-kurs talabasi.
Farruh Tashev Muzaffarovich
Ilmiy rahbar. Jahon iqtisodiyoti va diplomatiya universiteti
“Xalqaro huquq va ommaviy huquq fanlari” kafedrasi katta o‘qituvchisi.
Email: *abdurahmonovagulsanam@gmail.com*
https://doi.org/10.5281/zenodo.20280278

Annotatsiya. *Zamon qanchalik rivojlanib borsa shu bilan birga jinoyatlarning yangi turlari ham kelib chiqadi. Hozirgi kundagi eng global muammo bu kiber jinoyatlardir. 2021-2025-yillarning statistikasiga ko’ra, O‘zbekistonda kiberjinoyatlar soni 16 mingdan oshganini tasdiqlamoqda. Mazkur maqola, bunday tarkibdagi jinoyatlarning yana qanday turlari mavjudligi hamda uning amalga oshirilish tartibi haqida ma’lumotlar berishga va uni tahlil qilishga qaratilgan.*

Kalit so‘zlar: *hakerlik, oq haker, qora haker, kulrang haker, zararli dasturlar, troyan viruslari, to‘lov viruslari, fishing, ijtimoiy muhandislik, dasturiy taminotning qaroqchiligi, kiberxavsizlik.*

Аннотация. *С течением времени появляются и новые виды преступлений. Самой глобальной проблемой сегодня является киберпреступность. Согласно статистике за 2021-2025 годы, число киберпреступлений в Узбекистане превысило 16 тысяч. Цель данной статьи — предоставить информацию и проанализировать, какие еще виды подобных преступлений существуют и как они совершаются.*

Ключевые слова: *хакинг, «белый хакинг», «черный хакинг», «серый хакинг», вредоносное ПО, троянские кони, программы-вымогатели, фишинг, социальная инженерия, пиратство программного обеспечения, кибербезопасность.*

Annotation. *As time progresses, new and increasingly complex types of crimes continue to emerge. Today, cybercrime stands out as one of the most pressing global challenges. According to statistics from 2021 to 2025, the number of cybercrime cases in Uzbekistan has exceeded 16,000, demonstrating the seriousness of this issue. This article is aimed at examining the existing types of cybercrimes, their methods of execution, and providing an analysis of their socio-legal aspects.*

Keywords: *Hacking, white hat hacker, black hat hacker, gray hat hacker, malicious software (malware), Trojan viruses, ransomware, phishing, social engineering, software piracy, cybersecurity.*

KIRISH.

Hozirgi kunda zamonaviy axborot texnologiyalari judayam jadal rivojlanib kelmoqda. Shu bilan birga aholining kundalik hayot tarzini ham ancha osonlashtirdi. Bularga: davlat xizmatlari (passport, ro’yxatdan o’tish) masofadan bajarilishi, onlayn to’lovlar va ta’lim sifatining oshishini

o’z ichiga oladi. Ammo bu rivojlanish bilan birga turli xil katta xavflar ham kelib chiqdi. Kiberxavfsizlik muammolari deyarli har kuni odamlarning shaxsiy ma’lumotlari tarqalib, kartalaridagi pullar g’oyib bo’lib, hattoki aldab ham ularning ma’lumotlarini olgan holda turli qabih ishlar bajarilib kelinmoqda. 2025-yil ma’lumotlariga ko‘ra, O‘zbekistonliklarning 1,9 trl so‘m mablag‘lar o‘g‘irlangan. Ma’lum bo’lishicha, bu jinoyatning 98% izi kartalardan pul yechib olishga qaratilgan. Bu nafaqat yakka shaxsga balkida biznes va davlat muassasalariga ham tahdidlar kuchaymoqda natijada esa kompaniyaning axborotlari o’g’irlanib, mijozlarning ishonchini suiste’mol qilishga olib kelmoqda.

ASOSIY QISM:

Kelgusida kiber jinoyatchilar xavfsizlik tizimlarini mustaqil ravishda o'rgana oladigan sun'iy intellektdan foydalanishni boshlaydilar. 2024 yilga kelib, kiber jinoyatlardan moliyaviy yo'qotishlar deyarli 70% ga etadi.

Juniper Research tadqiqotchilarining fikriga ko'ra, zarar har yili o'rtacha 11 foizga oshadi va 2024 yilga kelib 5 trillion dollardan oshadi. O'tgan yili mutaxassislar kiber jinoyatlardan etkazilgan zararni 3 trillion dollarga baholashgan. Har yili kompaniyalar tobora ko'proq raqamli muhitga bog'liq bo'lib, zarar etkazilishi ma'lumotlarning tarqalishi uchun qonun bo`yicha olinadigan jarimalar tufayli ortadi. Vaqt o'tishi bilan nafaqat himoya usullari yaxshilanmoqda.

Tahlilchilar kiber jinoyatchilar kelajakda xavfsizlik tizimlarini mustaqil o'rganishga qodir bo'lgan sun'iy intellektdan foydalanishni boshlashlari haqida ogohlantirmoqda.

So'nggi yillarda AI texnologiyasi kiber tahdidlardan himoya qilish uchun faol foydalanilmoqda. Kiberxavfsizlik korporativ madaniyatning tobora muhim qismiga aylanib bormoqda, ammo bu tendentsiya kompyuter tizimlari foydalanuvchilari orasida keng tarqalmadi.

Xodimlarni kiberxavfsizlik asoslariga o'rgatish ushbu sohada xarajatlarni yanada samarali rejalashtirishga yordam beradi, tahlilchilar fikriga ko'ra, har yili atigi 8 foizga o'sadi.

Mutaxassislar, shuningdek, IT-kompaniyalar har doim inson omilini hisobga olishlari kerakligini ta'kidladilar, chunki tajovuzkorlar ijtimoiy muhandislik usullaridan faol foydalanishda davom etmoqdalar.

KIBERJINOYATLARNING TURLARI.[1]

Kiberjinoyat turlariga o’tishdan avval, ushbu atamaning ilmiy hamda huquqiy ta’rifini berish kerak. **Kiberjinoyat** — 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 saviyasiga zarar yetkazish maqsadida sodir etiladi. Maxfiy ma’lumotlar qonuniy tarzda himoyalangan holatda yuz beruvchi kiberjinoyatlar bilan bog‘liq ko‘pgina jinoyatlar mavjud. Xalqaro miqyosda hukumat ham, nodavlat subyektlar ham kiberjinoyatlar, 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 kiberjinoyatlar ba’zan kiberurush deb ataladi.

[1] https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention

ISSN: 2181-3906 2026

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 5 / ISSUE 5 / UIF:8.2 / MODERNSCIENCE.UZ

Uorren Baffet kiberjinoyatni „insoniyatning birinchi raqamli muammosi“ deb ta’riflaydi va „insoniyat uchun real xavf tug‘diradi“, deya qo‘shimcha qilib o‘tadi. Kiberjinoyatlarning 5 ta turi mavjud:

1.Hakerlik- komputer tizimlarini, dasturlashni hamda tizimga kirib undan foydalanish yoki buzish ko‘nikmasiga ega bo’lgan mutaxasis. Hakerlarning 3ta turi mavjud: oq, qora va kulrang hakerlar. Oq hakerlar asosan, tizim xavfsizligini tekshirish va yaxshilash uchun yo’llangan mutaxasislar. Qora hakerlar esa, g‘araz niyatli shaxslarning tizimni buzib kirgan holda nomaqbul ishlarni amalga oshirishi. Kulrang hakerlar- shunchaki tizimni xavfsizligini tekshirish maqsadida uni buzib kirish natijasida, kamchiliklarini topib beradigan mutaxasis.

2.Zararli dasturlar- zararli dasturlarga asosan: viruslar, troyanlar, reklamalar va to‘lov viruslari kiradi. **Virus** bu oddiy tarkibli virus bo‘lib, odatda bu telegram akkauntlariga ulanib, shu ulangan akkauntning egasi tarzda virusli fayllarni yaqinlariga jo‘natish orqali virus tarqatadi.

Troyan viruslari- bu o’zini foydali dastur sifatida ko‘rsatib, komputerga o‘rnashib foydalanuvchining ma’lumotlarini o‘g‘irlaydi yoki yo‘q qiladi. **Reklamalar**- ijtimoiy tarmoqlardan foydalanayotgan chog‘imizda reklama sifatida namoyon bo’ladi va foydalanuvchini o‘ziga jalb qilib shaxsiy hisobiga yashirin tarzda kiradi. **To‘lov viruslari**- bu foydalanuvchining ma’lumotlarini bloklaydi va ochish uchun pul talab qiladigan virus turi.

3. Shaxsiy ma’lumotlarni o‘g‘irlash- kiberjinoyatning bunday turida shaxsning shaxsiy ma’lumotlarini o‘g‘irlab, undan noqonuniy yo‘lda foydalanadi. Lekin ko‘pincha bunday jinoyatlar har doim ham kiberhujum natijasida sodir bo‘lavermaydi, aksincha bular yuqoridagi zararli dasturlar orqali yuz beradi. Hozirda bu jinoyatning **fishing** turi omma orasida juda ham keng tarqalgan usul bo‘lib, bunda matnlar, qo‘ng‘iroqlar orqali foydalanuvchiga o‘zini uzoq muddatdan beri faoliyat yuritayotgan bank sifatida aldaydi.

4.Ijtimoiy muhandislik- foydalanuvchi bilan o‘zining soxta shaxsiyati o‘rtasida mustahkam munosabat qurgandan so‘ng, iste’molchini maqsadini amalga oshirishini va’da qilib uni manipulatsiya qiladi va qanchadur pul miqdori undirib oladi.

5. Dasturiy taminotning qaroqchiligi- Qurilmamizdagi kundalik foydalanayotgan ilovalarning hammasi ham litsenziyalangan emas. Keyinchalik bunday ilovalar qurilmangizga kirib olib, hamma kerakli ma’lumotlaringizni tarqatadi yoki yo‘q qilib yuborish ehtimoli juda katta va bu jinoyatning turi hozirda jadal rivojlanib kelmoqda.

Bundan tashqari, mobil aloqa vositasiga kelgan yangilanishlar ham xavfsiz emas. Bu kabi yangilanishlarni qabul qilsak, qurilmamizdagi ma’lumotlarimiz o‘chib ketish ehtimoli juda ham kuchli.

Bu masala hamma davlatlarni qiynab kelmoqda va kiberjinoyatchilarni topish ham oson ish emas. Bu kabi niqoblangan insonlar boshqa bir davlatda turgan holda o’z faoliyatini olib boradi.

RAQAMLI JINOYATLARGA QARSHI KURASHISH

Prezidentimiz **“AXBOROT TEXNOLOGIYALARI YORDAMIDA SODIR ETILADIGAN JINOYATLARGA QARSHI KURASHISH FAOLIYATINI YANADA KUCHAYTIRISHGA QARATILGAN CHORA-TADBIRLAR TO‘G‘RISIDA”** qonun ijro etgan va bu qonunda kiberjinoyatlarga qarshi kurashishning ustuvor vazifalari hamda bu vazifalar kimlar tomonidan amalga oshirilishi haqida ilgari surilgan.

Kiberxavfsizlik sohasi yurtboshimiz tomonidan qo‘llab-quvvatlanib kelmoqda. Buni biz yuqorida keltirilgan qonunning 32-moddasida: “***Kiberxavfsizlik subyektlarini davlat tomonidan qo‘llab-quvvatlash quyidagilardan iborat:***[2]

kiberxavfsizlik sohasidagi normativ-huquqiy bazani takomillashtirish;

kiberxavfsizlik subyektlariga soliq, bojxona imtiyozlari va preferensiyalar berish;

xo‘jalik yurituvchi subyektlarning mablag‘larini kiberxavfsizlik sohasini moliyalashtirish uchun jalb etishga shart-sharoitlar yaratish;

kiberxavfsizlik sohasida ilmiy-texnika yutuqlariga asoslangan mahsulotlarning va ilg‘or texnologiyalarning kafolatlangan tarzda joriy etilishini ta’minlash maqsadiga qaratilgan davlat xaridlarini tashkil etish;

kiberxavfsizlikni ta’minlash bilan bog‘liq davlat xaridlarini amalga oshirishda mamlakatimizda ishlab chiqarilgan mahsulotga ustuvorlik berish." dan bilishimiz mumkinki, bu jinoyatlarning hech biri bee’tibor qoldirilayotgani yo’q aksincha bunday jinoyatlarga qarshi kurash olib borilmoqda.

Lekin shunga qaramasdan, O‘zbekistonda kiberjinoytalar so‘nggi 5 yil ichida 4 865 tadan 62 440 taga yetgan. Bu sohadagi jinoyatlarga qarshi kurashish uchun hozirda xorijiy hamkorliklar va shu bilan birga xalqaro mutaxasislar jalb qilingan.

Kiberjinoyatga qarshi kurashish borasidagi chora-tadbirlar: hududlarda maxsus bo‘linmalar tuzilib, sohaviy xodimlar shtati oshirilmoqda.

Xorijiy hamkorlar bilan tajriba va axborot almashish yo‘lga qo‘yilgan. Ichki ishlar akademiyasida bu turdagi jinoyatlar uchun alohida o‘quv dasturlar ochildi va 100 nafari qo‘shimcha o‘qishga qabul qilindi.

Shu bilan bir qatorda sun’iy intelektni ham qo‘llab-quvvatlashmoqda. Bundan tashqari, kiberjinoyatlar 1 yilda 16 mingdan oshganligi sababli, moliyaviy ilovalarga ko‘p so‘rovlar kelib tushsa, cheklov qo‘yilishi, vaqtinchalik bloklash yoki boshqa choralar qo‘llanilishi ham aytib o‘tilgan.

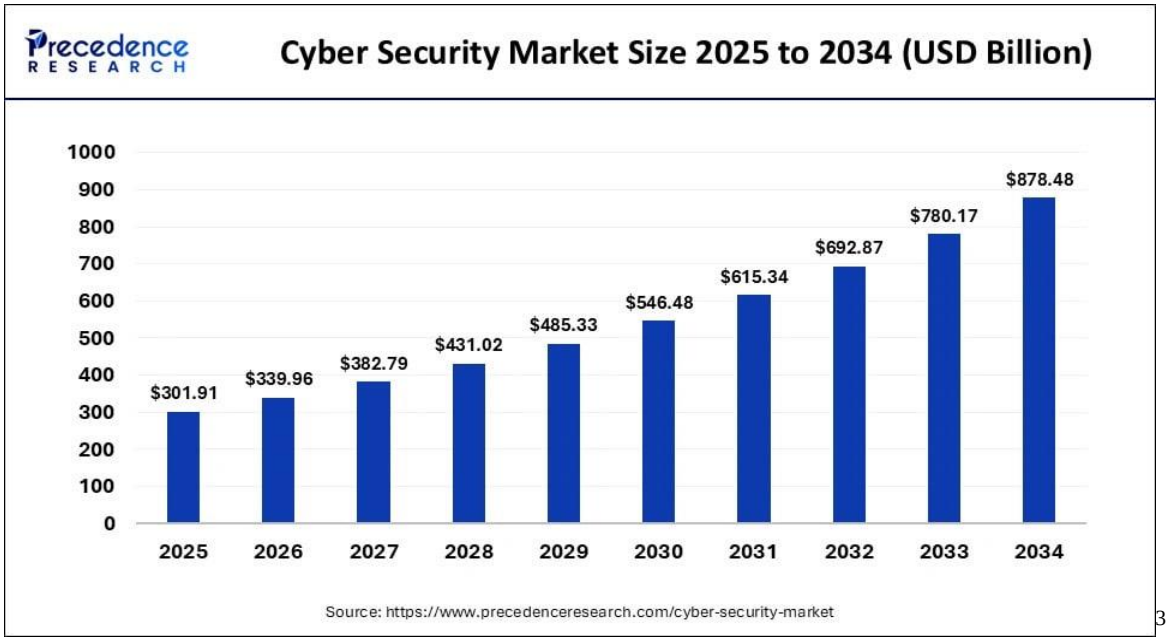
Shuningdek, 1 kunda faqat 1 ta bankdan kredit olish mumkinligi ham alohida ta’kidlab o‘tilgan. Xalqaro elektraloqa (MSE) global kiberxavsizligi ko’rsatkichi bo’yicha O’zbekiston 41 pozitsiyaga ko’tarildi. Shu bilan birga MDH davlatlari orasida kuchli uchlik liderlaridan biriga aylandi.

Tarixga nazar tashlasak, 2017-yilning Global kiberxavfsizlik bo’yicha 93-o’rinni egallagan. So’nggi kunning ma’lumotlariga ko’ra, joriy yilning 27-mart kuni Xalqaro elektraloqa indeksi bo’yicha 52-o’rinni egallagani ma’lum bo’ldi.

[2] https://lex.uz/docs/-7511145
https://csec.uz/uz/news/yangiliklar/global-kiberxavfsizlik-indekslari-va-o-zbekistonning-reytingi-kuchli-o-sish-tendensiyalari/

ISSN: 2181-3906 2026

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 5 / ISSUE 5 / UIF:8.2 / MODERNSCIENCE.UZ



[3]

Yuqoridagi grafik shuni ko’rsatadiki, 2025-2035-yilgacha global kiberxavfsizlik bozorining hajmi qanday o’zgarishi bo’yicha “Presendence Research”ning prognozini namoyon qilmoqda.

Grafikdagi asosiy ko'rsatkichlar:

2025-yilda kiberxavfsizlik bozori hajmi taxminan 301.91 milliard AQSh dollarini tashkil etishi prognoz qilinmoqda.

2030-yilda bu ko'rsatkich sezilarli darajada oshib, taxminan 546.48 milliard dollarga yetishi kutilmoqda.

2034-yilga kelib bozorning umumiy hajmi maksimal darajaga, ya'ni taxminan 878.48 milliard AQSh dollariga yetishi prognoz qilinmoqda.

Bu ma’lumotlar orqali shuni bilishimiz lozimki, 9 yil mobaynida kiberxavfsizlikni takomillashtirish borasidagi sarflaydigan pul summasining prognozlari. Qisqa qilib aytganda, bu statistika kiberhujumga qarshi kurashish uchun sarflanadigan pulni ko’rsatadi.

JINOYAT KODEKSIDAGI SANKSIYALAR

Shuningdek, JK **278[1]-moddasi Axborotlashtirish qoidalarini buzish** Axborotlashtirish qoidalarini buzish, ya’ni belgilangan himoya choralarini ko‘rmagan holda axborot tizimlari, ma’lumotlar bazalari va banklarini, axborotga ishlov berish hamda uni uzatish tizimlarini yaratish, joriy etish va ulardan foydalanish hamda axborot tizimlaridan ruxsat bilan foydalanish fuqarolarning huquqlariga yoki qonun bilan qo‘riqlanadigan manfaatlariga yoxud davlat yoki jamoat manfaatlariga ko‘p miqdorda zarar yoxud jiddiy ziyon yetkazilishiga sabab bo‘lsa, — bazaviy hisoblash miqdorining ellik baravarigacha miqdorda jarima yoki bir yilgacha axloq tuzatish ishlari bilan jazolanadi. O‘sha harakatlar juda ko‘p miqdorda zarar yetkazgan holda sodir etilgan bo‘lsa, — bazaviy hisoblash miqdorining ellik baravaridan yuz baravarigacha miqdorda jarima yoki bir yildan ikki yilgacha axloq tuzatish ishlari bilan jazolanadi.

[3] https://www.precedenceresearch.com/cyber-security-market

Shu bilan birga, **JKning 278[2]-moddasi "Komputer axborotidan qonunga xilof ravishda foydalanish"** 2-bandida bazaviy hisoblash miqdorining 100 baravarigacha jarima yoki 3 yilgacha muayyan huquqdan mahrum qilish yoxud 1 yilgacha axloq tuzatish ishlari bilan jazolanadi.

Agarda bu harakatlar retsidivist tomonidan qilinsa, JKning shu moddasida yuqoridagi sanksiyalardan boshqacha tartibda qo‘llaniladi. Bu tarkibdagi jinoyatlar 2 ta obyektga bir vaqtning o‘zida zarar beradi. 1. Bevosita obyekti- komputer xavfsizligi, ularning tizimlari normal ishlashini taminlashga doir munosabatlar bo‘lsa, 2. Qo‘shimcha obyekti bu- fuqarolarning shaxsiy yoki mulkiy manfaatlari. [4]

FOSH ETILGAN KIBERHUJUMLAR[5]

2025-yil holatiga ko’ra, kriptoaktivlar aylanmasi bilan bog’liq bo’lgan 2 mingdan ortiq bo’lgan jinoyatlar ochib berilgan natijada esa 76 mlrd so’m O’zbekiston hududidan noqonuniy chiqib ketishni oldini olgan. Shu qatorda, firibgarlikka va jamoat xavfsizligiga tahdid soluvchi mingdan ortiq internet-resurslari bloklangan. [6] Toshkent viloyati Ichki ishlar bosh boshqarmasi tomonidan Chilonzor tumanida kiberfiribgarlar guruhi fosh etilganligi xabar berildi. Boshqarma veb-sahifasi ma’lumotlariga ko’ra, bir guruh firibgarlar “kiberbunker” yaratib, o’z faoliyatini olib borishgan. Ma’lum bo’lishicha, bu uyushgan guruh Chilonzor tumanidagi call-markaz sifatida aholini Uzum Market ilovasi orqali sovg’a yutib olishgani haqida yolg’on ma’lumotlar tarqatgan.

Aldangan aholi esa bu yutuqlarni olish uchun kredit yoki mikroqarz limiti hisobidan ushbu jinoyatchilarning o’zlari aytgan hisobga pul o’tkazishi natijasida millionlab mablag’larini qo’ldan boy bergan. Yaqinda Bishkekda bo‘lib o‘tgan Markaziy Osiyo davlatlarida kiber xavfsizlik masalalari bo‘yicha konferentsiyada mutaxassislar xakerlik singari kiber jinoyatlar milliy xavfsizlikni ta’minlash va hukumatlar rasmiy organlarining faoliyatiga xavf soluvchi omillardan biri ekanligini urg‘ulashgandi.

Noma'lum shaxs Kogon shahar Xalqlar Do'stligi ko'chasida yashovchi fuqaroni va yana 3 nafar boshqa fuqarolarni aldab, plastik kartalaridan jami 4.040.000 so'm pullarni axborot texnologiyalaridan foydalangan holda yechib olib, firibgarlik jinoyatlarini sodir qilgan. Ushbu holatlar yuzasidan Kogon shahar IIB tomonidan noma'lum shaxsga nisbatan O'zbekiston Respublikasi Jinoyat kodeksining 168-moddasi 3-qismi bilan qo'zg'atilgan jinoyat ishi bo'yicha olib borilgan tezkor texnik, surishtiruv hamda tergov harakatlari davomida ushbu jinoyatni Kogon shahar “M.Ulug'bek” mahallasida yashovchi, 1999-yilda tug'ilgan O.G. ismli ayol sodir qilganligi aniqlandi. Shuningdek, navbatdagi holatda Olot tumani IIB tomonidan berilgan ma'lumotga ko'ra, noma'lum shaxs kommpyuter tizimlariga ruxsatsiz kirib, o'zganing mol-mulkini yashirin ravishda talon-toroj qilish maqsadida tumanning “Ma'rifat” mahallasida yashovchi boshqa bir fuqaroga “Milliybank” ATB tomonidan rasmiylashtirib berilgan plastik kartadan hamda shu kabi yana 9 nafar fuqarolarning kartasidan jami 12.511.000 so'm pullarni yashirin ravishda yechib olib, fuqarolarga moddiy zarar yetkazgan.

[4] Jinoyat kodeksi XX[1] bob 268-269-betlar
[5] https://yuz.uz/uz/news/82153
[6] https://vaqt.uz/uz/news/2025-yilda-ozbekistonda-kiberjinoyatlar-ortidan-19-trln-som-ogirlandi-16461?utm_source=chatgpt.com

Mazkur holatlar yuzasidan ham tuman IIB tomonidan noma'lum shaxsga nisbatan O'zbekiston Respublikasi Jinoyat kodeksining 169-moddasi 3-qismi bilan qo'zg'atilgan jinoyat ishi bo'yicha olib borilgan tezkor texnik, surishtiruv hamda tergov harakatlari davomida, ushbu kiberjinoyatlarni Olotning “Ma'rifat” mahallasida yashovchi, 2001-yilda tug'ilgan Sh.G. ismli ayol sodir qilganligi fosh etilgan.

XULOSA

Xulosa qilib aytganda, bugungi kundagi axborot texnologiyalar rivojlanib borayotgan bir vaqtda komputer texnologiyalariga bo’g’liq bo’lgan turli xil havf-xatarlar ham vujudga keladi.

Buni oldini olish maqsadida yurtboshimiz Shavkat Miromonovich Mirziyoyev keng qamrovli, samarali hamda tizimli chora-tadbirlar amalga oshirmoqda. Sizlarni ogohlantirish maqsadida, qurilmangizdagi hisob raqamlaringizga alohida kuchli parol agarda yodingizdan chiqish ehtimoli yuqori bo’lsa, yon daftarga yozishni maslahat beraman.

Turli xil ilovalarni litsenziyasini tekshirmay turib, uni aloqa vositangizga yuklab olmang hamda noma’lum raqamlarga javob bermasligingizni ta’kidlayman. ***“Noma’lum qo‘ng‘iroqlar, "yutuq", "limit ajratildi" kabi va’dalarga ishonmang.”***[7]

FOYDALANILGAN ADABIYOTLAR:

1. Jinoyat kodeksi
2. https://www.spot.uz/oz/2026/01/27/cybercrime/
3. https://lex.uz/acts/-5960604
4. https://online.norwich.edu/online/about/resource-library/5-types-cyber-crime-how-cybersecurity-professionals-prevent-attacks
5. https://lex.uz/ru/docs/-7511145
6. https://csec.uz/uz/news/axborot-xavfsizligi-yangiliklari/2024-yilga-kelib-kiber-jinoyatchiliklardan-moliyaviy-zarar-5-trillionni-tashkil-etadi/

[7] Toshkent viloyati IIBB (BBC.COM/UZBEK)