KIBER JINOYATLAR

Isoqova Muxlisa Faxriddin qizi
Muhammad Al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti talabasi

https://doi.org/10.5281/zenodo.7824335

Annotatsiya: *Kiberjinoyat millat, davlat, jamiyatga xavf solayotgan dolzarb muammolardan biridir. Bu raqamli elektron muhitni rivojlangani sayin ortib bormoqda. Yildan yilga kiberjinoyat qurbonlari soni ortmoqda. Kiberjinoyatga qarshi kurashish, kibermakonni yo'q qilish kabi yo'llarni ko'rib gaplashib chiqamiz.*

Kalit so'zlar: *Telefon, smartfon, kompyuter, ilovalar, kiber jinoyat, hacker, fishing o'yinlar, bank kartalari, Aqsh, Rossiya, raqamli texnologiyalar, ijtimoiy tarmoqlar, xavfsizlik, kodlar, e-mail pochta*

КИБЕР ПРЕСТУПЛЕНИЯ

Аннотация:*Киберпреступность - одна из актуальных проблем, угрожающих нации, государству и обществу. С развитием цифровой электронной среды она возрастает. Число жертв киберпреступлений год от года увеличивается. Обсудим пути борьбы с киберпреступностью и уничтожить киберпространство.*

Ключевые слова: *Телефон, смартфон, компьютер, приложения, киберпреступность, хакер, фишинговые игры, банковские карты, США, Россия, цифровые технологии, социальные сети, безопасность, коды, электронная почта*

CYBER CRIMES

Abstract: *Cybercrime is one of the urgent problems that threaten the nation, state, and society. It is increasing with the development of the digital electronic environment. The number of victims of cybercrime is increasing year by year. We will discuss ways to combat cybercrime and destroy cyberspace.*

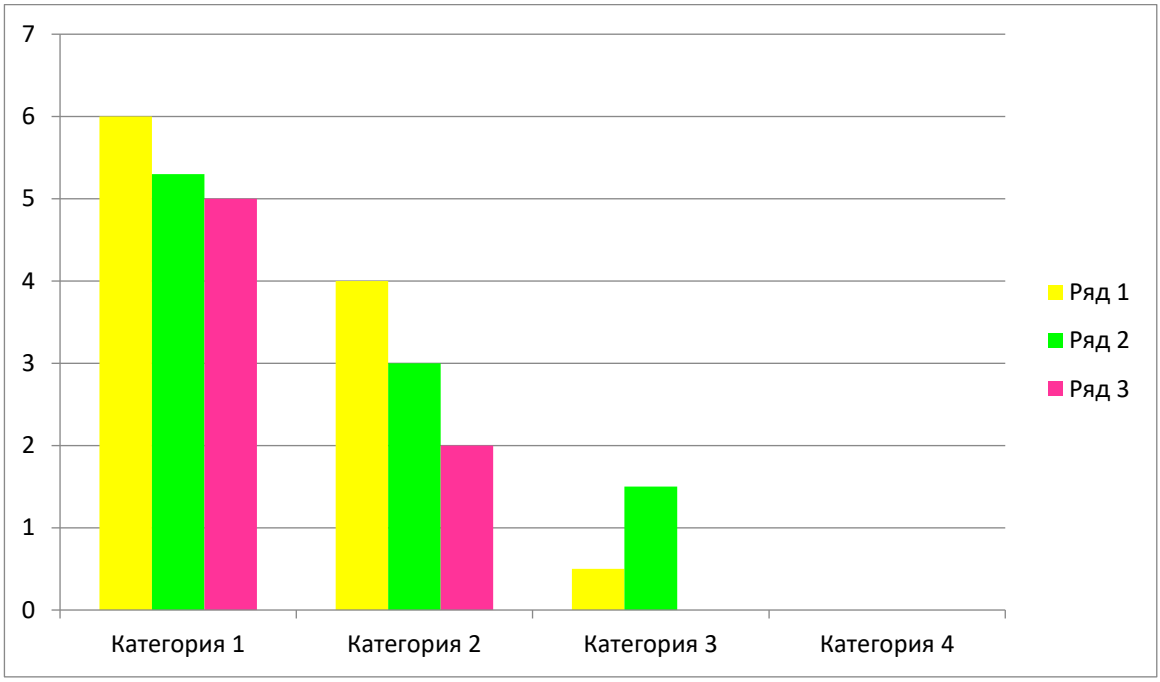
Keywords: *Phone, smartphone, computer, applications, cybercrime, hacker, phishing games, bank cards, USA, Russia, digital technologies, social networks, security, codes, e-mail*

KIRISH

Hozirgi rivojlangan XXI-asrda hayotimizni zamonaviy axborot texnologiyalarisiz tasavvur qilishimiz qiyin shu jumladan yashash tarzimizni osonlashtirgan, foydali taraflari ko'p bo'lgan bilan albatta foydasiz taraflari ham bor. Tangani ikki tarafi bo'lgani kabi yaxshi va yomon jihatlari bor. Har birimiz ishlayotgan kompyuter, telefon, smartfon va hokozolarni ishlatish bilan birga ehtiyot bo'lishimiz kerak. Bulardan eng asosiysi xavfsizlik turidir. Ya'ni biz foydalanayotgan mobil telefon, kompyuterlarimizda shaxsiy ma'lumotlarimizni saqlaymiz. Deyarli ko'p odamlar hozirda online viza kartalar ochishgan, clikc payme va h. k onlayn pul o'tkazmalaridan foydalanib kelishadi. Albatta bu ilovalardan foydalanishdan oldin registratsiyadan o'tasiz, shaxsiy ma'lumotlaringiz bilan. Endi hozirda juda ko'p uchrayotgan jinoyatchilik turlaridan biri bu kiberjinoyatchilikdir. Kiberjinoyatni ommaviy axborot vositalarida, ijtimoiy tarmoqlarda, har bir odamning telefon raqamlariga hatto sms yuborilib bizni ogohlantirishmoqda. Afsuski shuncha ogohlantirishlar bilan o'zimiz bilmagan holda kiberjinoyatning qurboni bo'lib qolyapmiz. Kiberjinoyat o'zi nima ? U qanday sodir etiladi? Nima uchun bunday jinoyat turlari ko'paymoqda? degan savollarga javob beramiz. Kiberjinoyatchilik haqida 2001-yilda axborot texnologiyalari xavfsizligi bo'yicha ogohlantirishdi ya'ni bu jinoyat ortayotgani haqida. Ko'rinib turibdiki bu necha yillar oldin paydo bo'lgan jinoyat turi. Axborot texnologiyalari rivojlanishi bilan kiberjinoyatchilik ortmoqda.

TADQIQOT MATERIALLARI VA METODOLOGIYASI

Kiber jinoyat – kuchli hackerlar tomonidan amalga oshiriladi. Davlatga, jamiyatga xavf tug‘diradigan harakatlarni paydo qiladi. Bunda asosiy maqsad pul undurish va yuqorida aytganimizdek xavfli harakatlarni vujudga keltirishdir. Kiberjinoyat kompyuterlardan foydalangan holda amalga oshiriladi. Bunda kompyuter qurol vazifasini bajaradi. Banklardan pul undurish, har xil tashkilot, korxonalardan har xil yo‘l bilan pul undurishadi. Albatta bu jinoyatga malakaga ega, o‘zining ishining ustasi faranglari jalb qilinadi. Buning evaziga oddiy korxonalarga qaraganda bu ishda katta miqdorda pulni tezda qo‘lga kiritadi. Shuning uchun ham kiberjinoyat ortmoqda . Hozirda e’lonlarga, xabarlarga qarasangiz shunday so‘zlar aks etgan xabarlarga ko‘zingiz tushadi. Masalan kiberjinoyatga qarshi kurashish bo‘limi nomidan fuqoralarga turli xil taqiqlangan materiallarni tarqatuvchi (pornografiya, zo‘ravonlik, odam o‘ldirish kabi va h. k) lar bilan kurashish uchun ularning bank kartasiga pul yuborish so‘ralgan. Davlat hodimlari nomi ostida chiqarilgan bu xabar o‘sha jinoyatchilar tomonidan chiqarilgan. Kiberjinoyatchilikning ayrim yolg‘on, shunga o‘xshash gaplaridan bilib olsangiz bo‘ladi.



1-rasm. Kiberjinoyatchilarning maqsadi.

1. (kategoriya 1. 1 sariq) 33% bu – shaxsiy ma’lumotlar
2. (katergoriya 1. 2 och yashil) 21 % bu – tijorat siri
3. (kategoriya 1. 3 malina) 19% bu – hisob ma’lumotlari
4. (kategoriya 2. 1 sariq) 9% - mijozlarning ma’lumotlar bazalari
5. (kategoriya 2. 2 och yashil) 8% - tibbiy ma’lumotlar
6. (kategoriya 2. 3 malina) 5% - to‘lov kartasi haqida ma’lumot
7. (kategoriya 3. 1 sariq) 2% - xat yozish
8. (kategoriya 3. 2 och yashil) 3% - boshqa ma’lumotlar

Dunyo statistikalariga asoslangan bu diagramma o‘sha kiberjinoyatchilarning eng keng va ko‘p qo‘llaniladigan turlari ko‘rsatilgan.

Misol uchun 1994-yil 22-sentabrdagi O‘zbekiston Respublikasi jinoyat kodeksida ham shaxsga nisbatan jinoyat sodir etgani u moddiy, ma’naviy ravishda yetkazgan zarari yoki shaxsga

nisbatan xavfli harakatlarni vujudga keltirgan shaxslarga jinoyat kodeksi bo‘yicha jazo tayinlanadi.

TADQIQOT NATIJALARI

O‘zbekiston Respublikasi Qonuni 15. 04. 2022-yildagi O‘RQ-764-son “kiberxavfsizlik” to‘g‘risida qabul qilingan qaror. Qarorda kibermakonda shaxs, jamiyat va davlat manfaatlarini ta’minlash, kiberjinoyatni sodir etgan shaxslarga nisbatan qo‘llaniladigan jazolar haqida gap boradi. Hozirda kiberjinoyatchilik haqida AQSh. Vashington, Rossiya yetakchi davlatlar qatorida turibdi. Kiberjinoyat tobora yildan yilga ortmoqda bunga asosiy sabab raqamli texnologiyalardir. Hozirda hamma jarayonlar raqamli texnologiyalar asosida bo‘layapdi. Masalan olimlarning fikriga qaraganda kiberjinoyatlar yiliga 8-11% gacha o‘sar ekan. Kiberjinoyatni sodir etgan shaxslarni topish biroz qiyinroq chunki o‘z ishining ustalari, bir kishi yoki guruh bo‘lib ishlashadi. Ularni bu ishga majbur qiladigan narsa bu – pul . Davlat ishida ishlab oylab oylik maoshni kutgandan ko‘ra ular uchun, bitta hackerlik qobilyatini ishga solib yaqin vaqtda momaygina mablag‘gani qo‘lga kiritishadi.

Kiberjinoyatni turli xil ko‘rinishlari haqida gaplashamiz.

Smartfoningizdagi shaxsiy ma’lumotlaringizga bo‘lgan tahdidlar

Misol uchun telefonimizdagi suratimizni ijtimoiy tarmoqlardan topib qilinadigan tahdidlar. Bunday holatlar kuzatilmasligi uchun har br ishimizni nimaga bunday qilayotganimiz haqida o‘zimizga savol berib to‘g‘ri anglab, tushunib olishimiz kerak. Shaxsiy ma’lumotlarni og‘irlashda, hammamizni e-mail pochta, id-raqamlar va har xil ma’lumotlarimiz bor ya’ni raqamli ma’lumotlar bular ko‘plab ishimizni bajarib uzoqni yaqin , qiyin jarayonlarni osonlashtiradi. Sizning bu kabi pochtalarga qo‘yilgan parolingizni bilib olgan odam deyarli ma’lumot va dars, ish, kundalik hayotingizdagi jarayonlarni nazorat qiladi yoki boshqaradi. Ish xonadagi muhim hujjatlaringizni hamkor chet el davlatlari bilan tuzilgan shartnomalaringizgacha ko‘rib ularni o‘zgartirishi yoki boshqarishi mumkin tizimga qayta kirishingizni cheklab qo‘yishi ham mumkin.

Id-karta, Viza kartalarni boshqarish

Hozirda juda mashhur bo‘lgan bank hisob raqamingizdan, virtual kartalaringizdan sizni har xil aldov yo‘li bilan onlayn muloqot tarzida pul undurishi yoki sizni chuv tushurishi mumkin. Bu jarayonlar ustidan ko‘plab arizalar tegishli joylarga kelib tushgan. Bu jarayon juda oson tarzda amalga oshiriladi va siz kiberjinoyat qurboni bo‘lasiz. O‘zingizni har qanday holatda telefon raqamingiz yoki akkauntingizga begona shaxslar, kompaniyalar tomonidan kelgan kodlarni aytmang. Hushyor bo‘ling zamon shiddat bilan rivojlangani bois internetga kirishlar ortmoqda. Axborot texnologiyalari aholiga, jamiyatga, davlatga qulaylik yaratadi. Va qulaylik yaratadigan dasturlar, platformalar, ilova bor. Lekin bular xavfsizlik tomondan ham, har tomonlama sinab keyin ommaga joriy qilgan maqul.

Zararli dasturlar

G‘arazli maqsadlarda rivojlanayotgan yoki mahsuloti yuqori darajali tashkilotlarga kiberhujumlar uyishturilib turiladi. Zararli dasturni ularga har xil yo‘l bilan yuborishadi. Natijada ma’lumotlar, dasturlash ihdan chiqib, yoqolib qoladi. Buning uchun albatta xamma narsalardan nusxa olgan holda saqlash kerak shunda yo‘q qilingan narsalarni qaytadan tiklasa bo‘ladi.

1. Ransomwere 3%
2. Bank ishi 6%
3. Botnet 13%
4. Kriptominerlar 21%
5. Mobil 30%

6. Boshqalar 27%

Dasturchilarimiz tomonidan shunday smartdastur ishlab chiqilishini taklif qilgan bo‘lar edim. Bunda xuddi kompyuterimizni viruslardan himoya qiladigan antivirus dasturiga o‘xshab kompaniya, tashkilotlarga yuboriladigan zararli dasturlarni tezda aniqlab xabar berishi yoki to‘g‘ridan to‘g‘ri bloklab qo‘yishi va zararli dasturni ochish buyrug‘i berilganda ham buyrug‘ni inkor qilishi kerak.

MUHOKAMA

Shuning bilan ijtimoiy tarmoqlarda (telegram, Instagram, fecebook, watsap) har xil havolalar kelib turadi. Ya’ni havolani ustiga bosing va pul yutvoling degan ma’noda. Bundayam xuddi shunday universal, smart telegramlar ishlab chiqilsa maqsadga muvofiq bo‘lar edi.

Kiberjinoyatni kamaytirish uchun , oldini olish uchun davlatimizda seminarlar, trening mashg‘ulotlari o‘tqazilib kelinmoqda. Bu jarayonda og‘zaki yoki prezidentatsiya usulida ko‘nikma va tushunchalar beriladi xolos. Ammo bu kamlik qiladi. Hackerlar bunaqa jinoyatni sodir etishda qanday bilimlarga ega bo‘ladi, ko‘proq qanaqa dastur, havolalardan foydalanishadi yoki dasturlarni yaratishda olgan bilimlari va h. k hisobot qilinib, jadval ko‘rinishida tahlil qilinishi va reja tuzish lozim. Birinchi navbatda yoshlarni, talabarni It sohasida, dasturlash, kompyuter, texnika asosida tehsil olayotgan shaxslarni bilimlarini oshirish zarur. Yuqoridagi sohalarga mo‘ljallangan kasb-hunar kollej, texnikum va oliy o‘quv yurtlarimizda kuchli bilimli, sohasini yetuk mutahasislarini tayyorlash lozim. Ular sohasini zo‘r bilsagina kiberjinoyatlarga qarshi kurasha oladigan shaxs bo‘lishadi. Har bir korxona, firma, tashkilot, o‘quv yurtlari o‘zlariga kiberxavfsizlik bo‘yicha muammoni yecha oladigan xodim olishlari ham maqsadga muvofiq. It sohasidagi yoshlarni yoki dasturchilarni har xil tanlov, olimpiada, bilimlarini yuksaltiradigan ko‘rik tanlovlar tashkil qilib ularni rag‘banlantirilsa bu sohaga bo‘lgan qiziqishi ortadi.

Internet rivojlangan sayin kiberjinoyatni soni ortmoqda deyapmiz bu qanchalik o‘rinli? Internet sur’ati rivojlangan davlatlarda kiberjinoyatlar soni juda ko‘p. Valyuta, qimmatli qog‘ozlar, bank kartalaridan pul yuborishlar hamma-hammasi onlayn ravishda ham o‘tqazilmoqda. Bu esa kiberjinoyatchilar uchun ayni muddao. Axborot texnologiyalari jinoiy, qastdan, o‘z manfaatlari uchun foydalangan shaxslarga davlatimiz qo‘shimcha qonun, farmonlar qo‘shib ularga nisbatan jazoni joriy etishlari ham maqsadga muvofiq. Yoki kiberxavfsizlik yuzasidan ma’lum vaqtga mo‘ljallangan strategiyalar ishlab chiqish kerak.

Aqsh davlari rivojlangan davlatlardan biri sanaladi. Aqshda 2012-yil onlayn kridet va kartalardagi jinoyatlar 1. 5 mlrd dollarni tashkil qilgan. Rossiyada esa 2013-yilda kartalar bo‘yicha firibgarlik yevropada 4-o‘rinni 4, 6 mlrd rublni tashkil etgan. Kiberjinoyatni oldini olishning asosiy yo‘llaridn biri bu davlatlar o‘rtasidagi kiberxavfsizlik bo‘yicha tuziladigan shartnomalardir. Bunda davlatlarning qo‘llagan ko‘proq samarali usullaridan foydalanishadi, mustahkam, puxta reja tuzilib shu bo‘yicha ish olib boriladi.

Kiberjinoyatchilikning ko‘plab turlari bor. Ulardan ayrimlarini sanaymiz : Kiberpornografiya, kiberjinoyat, iqtisodiy firibgarlik jinoyati, kiberterrorchilik, zararli dasturlar orqali kiberjinoyat, atribut firibgarlik.

Kiberjinoyatga mustahkam bardosh bera oladigan dastur yoki web ilovalar, antivirus dasturlari yo‘q albatta. Faqat hozirda zamonaviy axborot texnologiyalari davrida, zamonaviy kiberhujumlarga dosh bera oladigan, har xil sharoitga moslasha oladigan turli qurilmalar, himoyalangan dasturlar yaratishni imkoni bor. Kiberxavfsizlikka kurashish, kiberjinoyatlarning oldini olish uchun yagona chora bu – himoyalangan kuchli platforma bo‘lishidir. Kiberjinoyatchilar har xil korparatsiya, bank, kompaniya, sex va h. k larga hujum uyushtirib ularni

mahsulotini sotilishi kamayishi va shunga o‘xshash har xil gaplar bilan hujumlar bilan ularni qo‘rqitib pul undurmoqchi bo‘lishadi. Bunga chuv tushgan kompaniyalar ularni xohlaganini berishadi. Natijada bu ishni eplagan kiberjinoyatchilar bundan ruh olib bundanam katta jinoyatlarni qila boshlashadi. Albatta har bir tashkilotning kiberxavfsizligi yuqori darajada bo‘lsagina bunday vaziyatda g‘olib bo‘la olishadi. Har bir kompaniyalar hujjatlarni shifrlangan holda saqlashi kerak deb bilaman!Bunda shifrlanganda ham oddiy , tarqalgan, buzush oson bo‘lgan shifrlardan foydalanmasdan shifrlashni murakkab usullaridan qo‘llagan maqul. Kiberjinoyatchilar avvalo ma’lumot o‘g‘irlashmi, hujjatlar, bankdn pul undurish, id-karta, viza kartadan pul o‘g‘irlash va h. k hamma kiberjinoyatlarda kodlarni buzib kirish uchun eng avvalo keng tarqalgan usullardan foydalanishadi. Hozirda eng oddiy, soda va ko‘p qo‘llaniladigan parollar juda ommalashgan.

Kiberjinoyatlarning aksariyati internet tarmog‘idan foyladalanishda yoki foydalanayotgan foydalanuvchilarda kuzatilinadi. Shu o‘rinda chet davlarlarning internetdan qanday foydalanishini aytib o‘tmoqchiman. Rossiya davlatida voyaga yetmaganlar uchun alohida internet tarmog‘i yaratilgan. Internetdan foydalanish soatini nazorat qilish ustidan Xitoy davlati. Hindiston davlatida hindiston hududida “tiktok” ilovasi bloklab qo‘yilgan. Va h. k. Hozirda internetdan juda zo‘r va momaygina daromatga biznes qilayotganlarni ham ta’kidlab o‘tmoqchiman. Albatta har bir shaxs 1, 2 marta onlayn buyurtma qilib ko‘rgan bo‘lsa kerak. Bu xaridor uchun ham sotuvchi uchun ham qulay jarayonlardan biridir. Keling foydali taraflari emas salbiy taraflari haqida so‘z olib boramiz. Bu jarayonda: aldov qurboni, chalg‘ib qolish holatlari va eng daxshatlisi kiberjinoyat qurboni bo‘lishingiz mumkin. Yoki sizning blokingizda tez tez kiberjinoyatlar sodir etishga urinishlar bo‘ladi. Bu holatda juda e’tiborli va bank kart ava h. klarda bir necha marotalik tekshiruvlarni : face id, barmoq izi va h. k larni qo‘ygan maqul.

XULOSA

Xulosa o‘rnida kiberxavfsizlikni, kiberjinoyatlarni kamaytirish oldini olish uchun bir qator chora tadbirlarni ko‘rib chiqib uning ustida ishlar olib borishimiz zarur. Xalqaro hamkorlikni rivojlantirish nafaqat kiberjinoyatlarga qarshi kurashishni balki axborot texnologiyalarini rivojlanishiga ham zamin yaratadi.

Foydalanilgan adabiyotlar:

1. https://hi-in.facebook.com/hackituz/posts/kiber-jinoyatchilik-va-uning-turlarikiber-jinoyat-turli-shakllarda-bolishi-mumki/107669145001486/
2. https://lex. uz/uz/docs/-5960604
3. https://iiv. uz/news/kiberjinoyatchilikka-qarshi-kiberxavfsizlik
4. https://qalampir.uz/uz/news/iiv-ogo%D2%B3lantiradi-internetda-firibgarlikning-noodatiy-turi-kengayyapti-11673
5. https://uz. wikipedia. org/wiki/Kiberjinoyat
6. https://xs. uz/uz/post/kiber-zhinoyat-uchun-qandaj-zhavobgarlik-bor
7. https://hi-in.facebook.com/hackituz/posts/kiber-jinoyatchilik-va-uning-turlarikiber-jinoyat-turli-shakllarda-bolishi-mumki/107669145001486/
8. https://www. amerikaovozi. com/a/a-36-2010-03-26-voa1-93371769/807021. html
9. https://community.uzbekcoders.uz/post/kiber-hujumlarni-turlari 61a7b21306b0a14545b7f422
10. https://fayllar.org/axborot-kommunikatsiya-tizimlarida-kiberjinoyatchilik-tahlili. html?page=4

11. https://cyberleninka.ru/article/n/kiber-zhinoyatlarni-yuzaga-kelish-omillari-va-kiber-etika-muammo-va-isti-bollar
12. https://uz. eyewated. com/kiber-jinoyatchilik-bu-nima/
13. https://lex. uz/docs/-111453?ONDATE=12. 03. 2022
14. https://www.calltouch.ru/blog/kiberbezopasnost-v-2022-godu-novye-metody-prestupnikov/
15. https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/2017/06_Kiev/Presentations/Session%204%20-%20Vladimir%20Buryachok. pdf