KIBERXAVFSIZLIKDA KIBERJINOYAT TUSHUNCHASI VA STATISTIKASI

Radjabova M.Sh., Obidov B.X., Suyunov K., Odilov O.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnalogiyalari universiteti

Annotatsiya: *Kiberxavfsizlik hamda kiberxavfsizlikda kiberjinoyatchilikni anglashda asosiy tushunchalarni bilish hamda kiberjinoatlarning qo'llanilish sohalarini doimiy tahlil qilib borish.*

Kalit so'zlar: *Kiberjinoyat, ichki va tashqi kiberjinoyatlar, kiberetika, xavfsizlik, ishonchlilik, kiberqonunlar.*

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.

«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.

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

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 sub’yektlar 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. Uorren Baffet kiberjinoyatni “insoniyatning birinchi raqamli muammosi” deb ta’riflaydi va “insoniyat uchun real xavf tug‘diradi”, deya qo‘shimcha qilib o‘tadi.

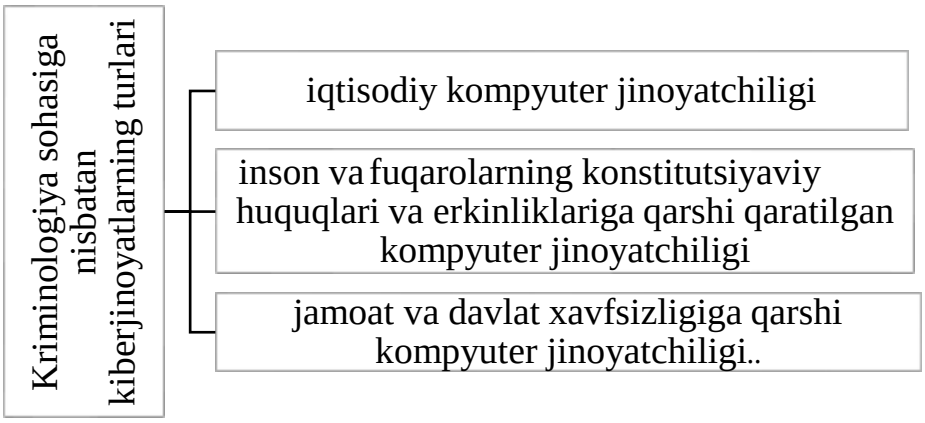
Kiberjinoyatchilik – g‘arazli yoki xuliganlik maqsadlarida himoyalashning kompyuter tizimlarini buzib ochishga, axborotni o‘g‘irlashga yoki buzishga yo‘naltirilgan alohida shaxslarning yoki guruhlarning harakatlari.

Kiberhujumga duch kelgan tashkilot uchun kiberjinoyatlar ichki yoki tashqi bo‘lishi mumkin:

Ichki kiberjinoyatlar: tarmoqqa yoki kompyuter tizimiga, ular bilan tanish va ulardan qonuniy foydalanish huquqiga ega bo‘lgan shaxs tomonidan, amalga oshiriladi. Mazkur turdagi kiberjinoyatlar odatda tashkilotning xafa bo‘lgan va norozi xodimlari tomonidan amalga oshiriladi. Ushbu xodimlarning maqsadi esa tashkilot yoki uning rahbaridan o‘ch olish yoki ochko‘zlik bo‘lishi mumkin. Xafa bo‘lgan xodim, AT infrastrukturasi, xavfsizlik arxitekturasi va tizimi bilan yaqindan tanish bo‘lgani bois, mazkur turdagi jinoyatchilik tashkilotga jiddiy ziyon yetkazishi mumkin. Bundan tashqari, kiberjinoyatchi tashkilot tarmog‘idan foydalanish imkoniyatiga ega bo‘ladi. Shuninguchun, ichki kiberjinoyatchilik natijasida maxfiy axborotning sirqib chiqish imkoniyati yuqori bo‘ladi.

Tashqi kiberjinoyatlar: odatda tashqaridan yoki tashkilot ichkarisidan yollangan hujumchi tomonidan amalga oshiriladi. Mazkur kiberjinoyatchilik tashkilotning nafaqat moliyaviy yo‘qotishlariga, balki obro‘sining yo‘qolishiga ham sababchi bo‘ladi. Hujum tashqaridan amalga oshirilgani bois, hujumchi harakatni tashkilot AT infrastrukturasini skaner qilish va unga aloqador ma’lumotlarni to‘plashdan boshlaydi. Xususan, malakali buzg‘unchi dastlab tashkilotdafoydalanilgan tarmoqlararo ekran vositasining log faylini tahlil qilishdan boshlaydi. Shu bois, tarmoq ma’muri mazkur imkoniyatni buzg‘unchiga taqdim etmasligi shart.

Kiberjinoyat amalga oshirilganidagi asosiy maqsadlar



Ular jinoyatchilarga millionlab AQSh dollari miqdoridagi noqonuniy daromadlar keltiradi. Ular orasida keng tarqalgani firibgarlik, asosan,bank hisob raqamlari va bank kartalari orqali amalga oshiriladi. Xalqaroamaliyotda plastik kartalar bilan sodir etilgan jinoyatlar yo‘qolgan yokio‘g‘irlangan kartalar, soxta to‘lov kartalarini yaratish yoki ulardanfoydalanish, karta taqdim etmasdan bank hisob varag‘i ma’lumotlariniolish va noqonuniy foydalanish, shuningdek, karta egasi tomonidan sodir etilgan jinoyatlar bilan bog‘liq.

Kiberjinoyatlarning yana bir turi inson va fuqorolarning huquqlariga va erkinliklariga qaratilgan jinoyatlar - “kompyuter qaroqchiligi”dir. Ushbu jinoyatlar dasturiy ta’minotni noqonuniy nusxalash, ishlatish va tarqatishda namoyon bo‘ladi.

Iqtisodiy kompyuter jinoyatchiligi amalda ko‘p uchraydi. Ular jinoyatchilarga millionlab AQSh dollari miqdoridagi noqonuniydaromadlar keltiradi. Ular orasida keng tarqalgani firibgarlik, asosan,bank hisob raqamlari va bank kartalari orqali amalga oshiriladi. Xalqaro amaliyotda plastik kartalar bilan sodir etilgan jinoyatlar yo‘qolgan yoki o‘g‘irlangan kartalar, soxta to‘lov kartalarini yaratish yoki ulardan foydalanish, karta taqdim etmasdan bank hisobvarag‘i ma’lumotlarini olish va noqonuniy foydalanish, shuningdek, karta egasi tomonidan sodir etilgan jinoyatlar bilan bog‘liq.

“Maykrosoft Armaniston” kompaniyasining direktori Grigor Barsegyanning ta’kidlashicha, “kompyuter qaroqchiligi”ning ishlabchiqaruvchilarga yetkazgan zarari yiliga 66 milliard dollarni tashkil etgan. Uning so‘zlariga ko‘ra Armanistonlik iste’molchilar, o‘zlarining moliyaviy resurslarini tejash maqsadida, viruslarni yuqtirish xavfi yuqori bo‘lgan dasturlardan ongli ravishda foydalanganlar.

Kompyuter jinoyatchiligining oxirgi turi - jamoat yoki davlat xavfsizligiga qarshi kompyuter jinoyatchiligi, ularga davlat yoki jamoat xavfsizligiga qaratilgan

xavfli xatti - harakatlar taalluqli. Ular ko‘pincha ma’lumot uzatish qoidalarining, mamlakat mudofaa tizimining yoki uningtarkibiy qismlarining buzilishi bilan bog‘liq.

Kiberqonunlar. Qonun (huquq) — inson, jamiyat va davlat manfaatlari nuqtai nazaridan eng muhim hisoblanadigan ijtimoiy munosabatlarni mustahkamlash, rivojlantirish va tartibga solish vositasi. Qonunning nima maqsadga qaratilganini u yo‘naltirilgan munosabatga qarab aniqlash mumkin. Shu bois qonunlar turli sohaga oid maqsadlarga ega bo‘lishi mumkin. Umumiy nomda kiberjinoatchilikni tartibga solishni maqsad qilgan qonunlar kiberqonunlar deb ataladi.

Qonunni ishlab chiquvchilar va uni himoya qiluvchilar butun dunyo bo‘ylab kiberjinoyatchilikni aniq belgilaydigan va kiber dalillarni qabul qilishni to‘liq madadlovchi kiberqonunlar zarurligi haqida ogohlantirib keladilar. Mamlakatning biror xalqaro shartnomadagi ishtiroki bu shartnomani qonuniylashtiradigan ichki qonunlar ishlab chiqilgan va tasdiqlangan taqdirdagina kuchga kiradi. Masalan, Yevropada 2004-yildaYevropaKengashi butun dunyo mamlakatlariga taklif qilingan Kiberjinoyatchilik to‘g‘risidagi Shartnoma (Budapesht konvensiyasi debham ataladi) loyihasini qabul qildi. Mazkur Shartnomani ko‘pchilik davlatlar imzolagan bo‘lsada, ularning bir nechtasigina shartnomaga moskeladigan milliy qonunlarga ega.

2020 yil fevral oyiga kelib, Birlashgan millatlar tashkilotiga a’zo bo‘lgan 106 ta (yoki 55%) davlatlar Budapesht konvensiyasiga muvofiq milliy kiberjinoyatchilik to‘g‘risidagi qonunlarga ega bo‘ldilar. Bundan tashqari, hozirda rivojlanayotgan davlatlar kiberjinoyatchilarni tergovqilish va bu jarayon uchun kerakli ma’lumotlarni yig‘ish bo‘yicha ma’lum vakolatlarni qabul qildilar.

Xususan, Respublikamizda ham “Ilm, ma’rifat va raqamli iqtisodiyotni rivojlantirish yili”da amalga oshirishga oid davlat dasturi (mualliflik huquqiga) jiddiy zarar yetkazadi. Bundan tashqari, dasturiy ta’minot kompaniyalariga katta moliyaviy yo‘qotishlarni olib keladi.

Kiberetika – kompyuterlar bilan bog‘liq falsafiy soha bo‘lib, foydalanuvchilarning xatti-harakatlari, kompyuterlar nimaga dasturlashtirilganligi, umuman insonlarga va jamiyatga qanday ta’sir ko‘rsatishini o‘rganadi.

Mulk. Axborotdan foydalanishdagi etikaga oid munozaralar uzoq vaqtdan beri mulkchilik tushunchasini tashvishga solmoqda va kiberetika sohasidagi ko‘plab to‘qnashuvlarga sabab bo‘lmoqda. Egalikka oid nizolar egalik huquqi buzilgan yoki noaniq bo‘lgan hollarda yuzaga keladi.

Intellektual mulk huquqlari. Internet tarmog‘ining doimiy ravishda o‘sib borishi va turli ma’lumotlarni zichlash texnologiyalarining (masalan, mp3 fayl formati) paydo bo‘lishi “peer-ro-peer” fayl almashinuviga katta yo‘l ochdi. Bu imkoniyat dastlab Napster kabi dasturlar yordamida amalga oshirilgan bo‘lsa,

endilikda BitTorrent kabi ma'lumotlarni uzatish protokollarida foydalanilmoqda. Uzatilganmusiqalarning aksariyati mualliflik huquqi bilan himoyalangan bo'lsada, mazkur fayl almashinuvi noqonuniy hisoblanadi.

Hozirgi kunda aksariyat elektron ko'rinishdagi media fayllar(musiqa, audio va kinofilmlar) intelektual mulk huquqlariga rioya qilinmasdan ommaga tarqalmoqda. Masalan, aksariyat katta mablag' sarflangan kinofilmlarning "qaroqchilarcha (piratskiy)" versiyasiningchiqishi bois o'z sarf xarajatlarini qoplay olmaslik holatlari kuzatilmoqda. Bu holatni dasturiy ta'minotlarda ham ko'rish mumkin. Masalan, aksariyat dasturlar litsenziyaga ega hisoblansada, turli usullar yordamidaularning "darz ketgan (crack)" versiyalari amalda keng qo'llaniladi.

Masalan, litsenziyaga ega bo'lmagan Windows 10 OT, antivirus dasturiy vositalari, ofis dasturiy vositalari va h.

Mualliflik huquqini himoyalashning texnik vositalari. Mualliflik huquqini ta'minlashda turli himoya usullaridan foydalaniladi. Ular CD/DVD disklardagi ma'lumotlarni ruxsatsiz ko'chirishdan himoyalashdan tortib oddiy PDF fayllarni tahrirlash imkoniyatini cheklash kabi jarayonlarni o'z ichiga olishi mumkin. Shu bilan birga, aksariyat insonlar litsenziyali CD diskni sotib olib, undan ko'chirish imkoniyatiga ham ega bo'lishim mumkin deb o'ylaydilar.

Xavfsizlik. Internet tarmog'idagi axborotdan xavfsiz foydalanish axloqiy munozaralar mavzusi bo'lib kelmoqda. Bu birinchi navbatda jamoat faravonligini himoya qilish yoki shaxs huquqini himoya qilish masalasini o'rtaga qo'yadi. Internet tarmog'idan foydalanuvchilar sonining ortishi, shaxsiy ma'lumotlarning ko'payishi natijasidakiberjinoyatlar soni ortmoqda.

Ishonchlilik. Internetning mavjudligi va ba'zi bir shaxs yoki jamoalar tabiati tufayli ma'lumotlarning ishonchliligi bilan shug'ullanishmuammoga aylanmoqda. Boshqacha aytganda, Internetdagi ma'lumotlarning ishonchliligiga kim javob beradi? Bundan tashqari, Internetdagi ma'lumotlarni kim to'ldirishi, undagi xatolar va kamchiliklaruchun kim javobgar bo'lishi kerakligi to'g'risida ko'plab tortishuvlar mavjud. *Intellektual mulk huquqlari.* Internet tarmog'ining doimiy ravishda o'sib borishi va turli ma'lumotlarni zichlash texnologiyalarining (masalan, mp3 fayl formati) paydo bo'lishi "peer-ro-peer" fayl almashinuviga katta yo'l ochdi. Bu imkoniyat dastlab Napster kabi dasturlar yordamida amalga oshirilgan bo'lsa, endilikda BitTorrent kabi ma'lumotlarni uzatish protokollarida foydalanilmoqda. Uzatilganmusiqalarning aksariyati mualliflik huquqi bilan himoyalangan bo'lsada, mazkur fayl almashinuvi noqonuniy hisoblanadi.

Foydalanuvchanlik, senzura va filtrlash. Foydalanuvchanlik, senzura va axborotni filtrlash mavzulari kiberetika bilan bog'liq ko'plab axloqiy masalalarni

qamrab oladi. Ushbu masalalarning mavjudligi bizning maxfiylik va shaxsiylikni tushunishimizga va jamiyatdagi ishtirokimizga shubha tug‘diradi. Biror qonun qoidaga ko‘ra ma’lumotlardan foydalanishni cheklash yoki filtrlash asosida ushbu ma’lumotni tarqalishini oldini olish foydalanuvchanlikka ta’sir qilishi mumkin. Senzura ham past darajada (masalan, kompaniya o‘z xodimlari uchun) yoki yuqori darajada (hukumat tomonidan xavfsizlikni ta’minlash uchun amalga oshirilgan) bo‘lishi mumkin. Mamlakatga kiruvchi ma’lumotlarni boshqarishning eng yaxshi misollaridan biri - “BuyukXitoy Fayrvoli” loyihasi.

Axborot erkinligi. Axborot erkinligi, ya’ni, so‘z erkinligi, shu bilan birga ma’lumotni qidirish, olish va uzatish erkinligi kiberhujumda kimgava nimaga yordam beradi degan savol tug‘iladi. Axborot erkinligi huquqi,odatda, jamiyat yoki uning madaniyatiga ta’sir ko‘rsatadigan cheklovlarga bog‘liq. Cheklovlar turli ko‘rinishda bo‘lishi mumkin. Masalan, ayrim mamlakatlarda Internet ommaviy axborot vositalaridan foydalanishning bir shakli hisoblanib, undan barcha davlat rezidentlari foydalanadilar. Bundan tashqari, Internetdan foydalanish bo‘yicha cheklovlar ayrim davlatlarning turli shtatlarida farq qilishi mumkin.

Raqamli to‘siqlar. Axborot erkinligi bilan bog‘liq axloqiy masalalardan tashqari, *raqamli to‘siq* deb ataluvchi muammo turi mavjud bo‘lib, u kiberfazodan foydalanish imkoniyati cheklanganlar o‘rtasidagi ijtimoiy tafovutni anglatadi. Dunyo mamlakatlari yoki mintaqalari o‘rtasidagi bu tafovut global raqamli to‘siq deb ataladi.

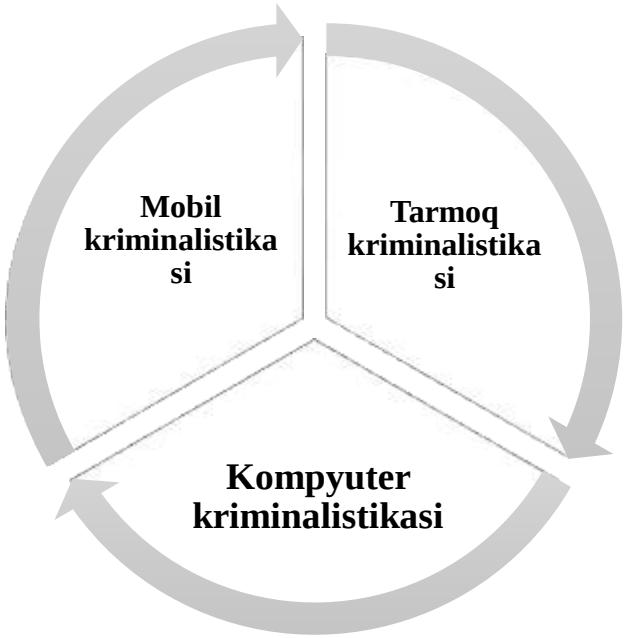
Taqiqlangan kontentlar (pornografiya). Internet tarmog‘ida mavjud bo‘lgan taqiqlangan kontentlarni voyaga yetmaganlar tomonidan foydalanish doimo axloqiy munozaralarga sabab bo‘lgan. Ayrim davlatlarda bunday kontentlardan foydalanish qat’iy taqiqlansa, ayrim davlatlarda bunga ruxsat berilgan.

Kompyuterdan foydalanish etikasi. Kompyuterdan foydalanish etikasi instituti notijoriy tashkilot bo‘lib, vazifasi texnologiyani axloqiy nuqtai nazaridan targ‘ib qilish hisoblanadi.

1.3-rasm. Buxgalteriya tizimiga qo‘yiladigan talablarni ta’kidlaydigan beshta prinsip

1.2. Kiberjinoyat va ularning qo‘llanilish sohalari tahlili

Kiberjinoyat virtual makondagi ijtimoiy xavfli qilmish bo‘lib, uni kompyuter texnologiyalari va boshqa axborot telekommunikatsiya vositalari yordamida modellashtirilgan kiberjinoyat deb ta’riflash mumkin. Kiberjinoyatga kompyuter tizimi yoki tarmog‘ida axborot-kommunikatsiya texnologiyalaridan foydalangan holda sodir etilishi mumkin bo‘lgan har qanday jinoyat kiradi. Kibermakonda sodir etilgan ushbu jinoyatlar kompyuterlar, kompyuter dasturlari, kompyuter tarmoqlari faoliyatiga qonunga xilof ravishda aralashish, kompyuter ma’lumotlarini ruxsatsiz kirish, nusxa olish, o‘zgartirish, shuningdek axborot-kommunikatsiya texnologiyalari, kompyuter tarmoqlari yordamida yoki ular orqali sodir etilgan boshqa noqonuniy ijtimoiy xavfli harakatlardir. Jinoyat huquqida kiberjinoyat umumiy ta’rif berilgan bo‘lib, uning tor ma’nosida axborot texnologiyalari bilan bog‘liq jinoyatlarni ham qamrab oladi, bunda kompyuter texnologiyalari sub’yekti, axborot xavfsizligi jinoyat ob’yekti hisoblanadi.



1.4.-rasm. Kiberjinoyat qo‘llanilish sohalari

Kompyuter kriminalistikasi - bu ilm va san’at, u qayta tiklash uchun maxsus usullardan foydalanishni, kompyuter jinoyatlari bilan bog‘liq elektron ma’lumotlar tahlili va haqiqiyligini tekshirishni talab etadi. Unda qonun bilan kompyuter ilmlari, axborot texnologiyalari va boshqa texnik masalalar birlashtiriladi.

Tarmoq kriminalistikasi - ancha oldin paydo bo‘lgan va xavfsizlik tahlili bo‘yicha mutaxassislar ancha yillardan beri Wireshark va boshqa trafik analizatorlaridan foydalanishadi. Birinchidan, foydalanuvchilar maksimal tezroq shubhali harakatlarni aniqlash maqsadida tarmoq kriminalistikasi vositalariga faolroq tayanadigan bo‘lishdi. Ikkinchidan, xavfsizlik tizimlari ishlab chiquvchilar bunday shubhali harakatlarni aniqlash bo‘yicha ixtisoslashgan yechimlar yaratishdi.

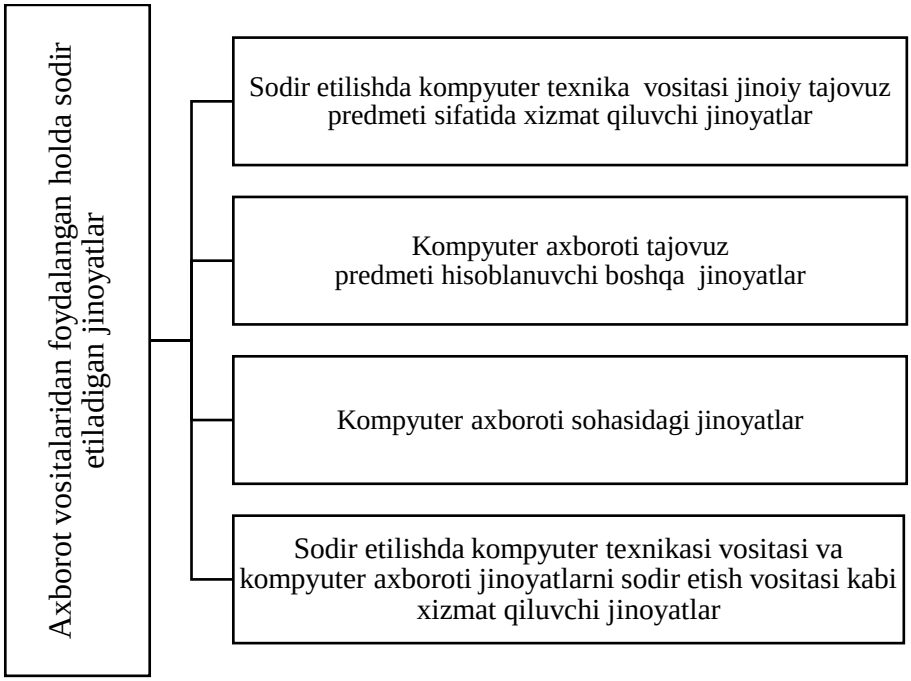
Mobil kriminalistika - uyali aloqa mavzulariga qo‘llaniluvchi – mobil qurilmalarning raqamli ma’lumotlarini olish va dekodlash imkoniyati.

Kompyuter vositalari va yangi axborot texnologiyalaridan foydalangan holda sodir etiladigan jinoyatlarning o‘sishi 1.5-rasmda keltirilgan faktorlar bilan tushuntiriladi. Kompyuter texnika vositalari va yangi axborot texnologiyalaridan foydalangan holda sodir etiladigan jinoyatlarning turi va soni doimiy o‘smoqda. Bunday jinoyatlarni sodir etishda tajovuz qilish predmetlarini ikki guruhga ajratish mumkin:

- kompyuter texnikasining o‘zi va axborot;
- kompyuter texnikasi va axborotdan jinoiy tajovuz qilish quroli kabi foydalanilib hujum qilinilishi mumkin bo‘lgan ob’yektlar.

Mulkka qarshi jinoyatni sodir etishda – o‘g‘irlash, yo‘q qilish, zarar yetkazishda jinoiy tajovuz predmeti sifatida kompyuter texnikasi xizmat qiladi. Tajovuz qilish predmeti sifatida texnik vositalarning o‘zi moddiy ob’yekt kabi xizmat qiladi. Kompyuter texnikasi va axborot jinoyat sodir etish vositasi sifatida ham xizmat qilishi mumkin. Bu ma’noda kompyuter qurol yoki transport vositasi sifatida jinoyat quroli kabi bir qatorda ko‘rilishi mumkin.

Axborot vositalarining qo‘llanilishi bilan sodir etiladigan barcha jinoyatlarni mos holda to‘rt guruhga ajratish mumkin :



1.6- rasm. Axborot vositasidan foydalangan holda sodir etiladigan jinoyatlar sxemasi

Kompyuter jinoyatchiligi (Kiberjinoyat) – bu axborot texnologiyalari sohasidagi maxsus bilimlarni qo‘llash orqali muayyan bir jinoyatni sodir etgan holda moddiy yoki ma’naviy zarar yetkazish mumkin bo‘lgan jinoiy qonunbuzarlikdir.

Xulosa

Kiberjinoiyat statistikasi esa kiberxavfsizlik sohasidagi jinoyatlar haqida ma’lumotlarni to‘plash va tahlil qilishning asosiy vositasi hisoblanadi. Bu statistika, jinoyatlar turi, ulardan kelib chiqishning odatiy va zamonaviy yo‘nalishlari, kompyuter viruslaridan, firibgarlikdan yoki ma’lumotlarni olish vaqtlaridan foydalangan holda tuzilgan hamjinsliklarni aks ettiradi. Bu statistikalar, kiberxavfsizlik sohasidagi jinoyatlar va ulardan to‘g‘ri kelib chiqish uchun zarur resurslarni, strategiyalarni va qo‘llanmalarini belgilashda muhim ahamiyatga ega.

FOYDALANILGAN ADABIYOTLAR

- Salayev N.S., Ro‘ziyev R.N Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar. Monografiya ., – T.: TDYU, 2018, 139-b.
- Карпова Д.Н. Киберпреступность: глобальная проблема и еѐ решение. //Власть. №8. 2014. С. 46-50
- Anorboyev A.U Kiberjinoyatchilik, unga qarshi kurashish muammolari va kiberxavfsizlikni ta‟minlash istiqbollari. Monografiya – T.: Milliy gvardiya instituti, 2020. – 324 b.
- Нестерович С.А. Проблемы расследования преступлений, которые стоят пред сотрудниками следственных органов. // Вестник науки и образования. №8. 2018. С. 46-49.
- Karpova D.N. Cybercrimes: a global issue and its solution. Vlast’= The Power no. 8, pp. 46–50. (In Russian).
- https://iiv.uz/news/kiberjinoyatchilikka-qarshi-kiberxavfsizlik