

INTERNET TARMOQLARI ORQALI SODIR ETILAYOTGAN KIBERJINOYATLAR

IIV Akademiyasi kursanti Jumaqulov Faryozbek Farxodbek o'g'li

ANNOTATSIYA

Maqolada internet tarmoqlari orqali sodir etilgan kiberjinoyatlar tushunchasi va turlarini aniqlash uning jamiyatga xavf solayotgan dolzarb muammolardan biri ekanligi va yildan yilga kiberjinoyat qurbonlari soni ortib borayotganligi bilan bog'liq masalalar ko'rib chiqilishi bilan birgalikda O'zbekiston Respublikasida ushbu jinoyatlarning jinoiy-huquqiy tahlili, fan va texnikaning yangi yutuqlari, internet, kompyuter va boshqa innovatsion texnologiyalar imkoniyatlaridan foydalangan holda kiberjinoyatlar sodir etilishiga imkon beruvchi omillar ko'rsatib o'tilgan.

Kalit so'zlar: Kiberjinoyatlar, raqamli va elektron dalillar, hacker, fishing o'yinlari, xavfsizlik, kodlar, innovatsiyalar, axborot-kommunikatsiya texnologiyalari.

ПЕРЕДАВАЕМЫЕ ЧЕРЕЗ СЕТИ ИНТЕРНЕТА КИБЕРПРЕСТУПЛЕНИЯ

АННОТАЦИЯ

В статье определены понятие и виды киберпреступлений, совершаемых через сеть Интернет, которая является одной из актуальных проблем, угрожающих обществу, а количество жертв киберпреступлений с каждым годом увеличивается, а также проведен уголовно-правовой анализ данных преступлений. Республика. В Узбекистане также показаны факторы, позволяющие совершать киберпреступления с использованием Интернета, компьютеров и других инновационных технологий.

Ключевые слова: Киберпреступления, цифровые и электронные доказательства, хакер, фишинговые игры, безопасность, коды, инновации, информационно-коммуникационные технологии.

KIRISH

Kiberjinoyat virtual makondagi ijtimoiy xavfli qilmish bo'lib, uni internet tarmoqlari va boshqa axborot telekommunikatsiya vositalari yordamida modellashtirilgan kiberjinoyat deb ta'riflashimiz mumkin. Kiberjinoyatga kompyuter tizimi yoki tarmog'ida axborot-kommunikatsiya texnologiyalaridan foydalangan holda sodir etilishi mumkin bo'lgan har qanday jinoyatlar 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 tushunchasiga umumiy ta'rif berilgan bo'lib, uning tor doiradagi ma'nosida axborot texnologiyalari bilan bog'liq jinoyatlarni ham qamrab oladi, bunda kompyuter texnologiyalari subyekti, axborot xavfsizligi jinoyat obyeksi hisoblanadi.

Hozirgi kunda raqamli texnologiyalar rivojlanib borayotgan zamonda kiberjinoyatlar axborot texnologiyalari sohasidagi jamoatchilik munosabatlariga jiddiy tahdid solmoqda desak mubolag'a bo'lmaydi shuning uchun zamonaviy sharoitda ularga qarshi kurashish davlat va fuqarolar uchun jiddiy muammoga aylandi. Davlatning huquqni muhofaza qilish organlari tomonidan ularni zararsizlantirish bo'yicha qarshi choralarni ishlab chiqmoqda, kiberjinoyatlarga qarshi kurashish strategiyasi va taktikasi va usullarini ishlab chiqmoqda. Kiberjinoyatlar inson ko'ziga ko'rinmaydigan kibermakonda turli xil sharoitlarda sodir etiladi, ularning sodir etilishiga yordam beradigan omillar mavjud. Ularni aniqlash va ilmiy tahlil asosida sud ekspertiza usullarini, tegishli tergov harakatlarini o'tkazish taktikasini ishlab chiqish kerak.

Kiberjinoyat kuchli hackerlar tomonidan amalga oshiriladi. Davlatga, jamiyatga xavf tug'diradigan harakatlarni paydo qiladi. Bundan ko'zlangan asosiy maqsad pul undurish va moddiy manfaatga ega bo'lish. Kiberjinoyat kompyuterlardan foydalangan holda amalga oshiriladi. Bunda kompyuter qurol vazifasini bajaradi. Banklardan pul undurish, korxonalaridan har xil yo'l bilan pul undurishadi. Albatta buni mulohaza qiladigan bo'lsak bu jinoyat malakaga ega, o'zining ishining ustasi faranglari va kompyuter texnologiyalarining mutaxassislari jalb qilinadi. Buning evaziga oddiy korxonalariga qaraganda bu ishda katta miqdorda pulni tezda qo'lga kiritish va tez boyib ketish manfaati turadi. Shuning uchun ham hozirgi zamonda kiberjinoyat ortmoqda. Hozirda e'lonlar va xabarlariga qarasangiz shunday so'zlar aks etgan xabarlariga 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.

O'zbekiston Respublikasi Qonuni 15.04.2022-yildagi O'RQ-764-son bilan tasdiqlangan "Kiberxavfsizlik" to'g'risida qabul qilingan Qonunda 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 qiyinchilik tug'diradi chunki o'z ishining ustalari ya'ni mutaxassislari 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 qobiliyatini ishga solib yaqin vaqtda mo'maygina mablag'ni qo'lga kiritishadi.

MUHOKAMA

Kiberjinoyatni sodir etishga yordam beruvchi omillar obyektiv va subyektivdir. Birinchisi, axborot (kompyuter) texnologiyalari sohasida zarur jihozlarning mavjudligi, zamonaviy, yuqori texnologiyali dasturiy ta'minot va potentsial huquqbuzarning axborot tarmog'iga kirishini o'z ichiga oladi. Bunda huquqbuzarning o'zi axborot texnologiyalari sohasidagi mutaxassis sifatida, kompyuter sohasida zarur ko'nikma va texnik ko'nikmalarga ega bo'lgan shaxs kiradi. Shuni yodda tutish kerakki, Axborot texnologiyalarning ning jadal rivojlanishi turli jinoyatchilarga kiberjinoyatlar sodir etish imkonini beradi va bunda ularga kompyuter texnologiyalarining texnik imkoniyatlari, dasturiy taminotining xususiyatlarini bilish yordam beradi. Hozirgi kunda jinoiy faoliyatning bu turi keng tarqalib, kiberjinoyatlar qurboniga aylanib borayotgan fuqarolar, korxonalar va tashkilotlar soni ortib borayotganligini ko'rishimiz mumkin. Kiberjinoyatlarning yana bir turi “**kardinglash**” deb ataladigan jinoyat bo'lib, uning mohiyati to'lov kartalari bilan yani ular bilan karta egasining xabardorligisiz yoki uning rekvizitlaridan foydalanib operatsiyalarni amalga oshirishda alohida turdagi firibgarlikni sodir etishdan iborat. Shu bilan birga, jinoyatchilar shaxsiy kompyuterlar, bankomatlar, onlayn do'konlar va boshqa axborot-kommunikatsiya saytlaridan ma'lumotlarni o'g'irlashadi. Internet tarmog'i orqali sodir etiladigan Karding kiberjinoyatlarning bir turi sifatida, o'z navbatida, kichik turlarga bo'linishi mumkin: «fishing» va «skimming». Bunda birinchisi foydalanuvchi identifikatsiya ma'lumotlarini (parollar, kredit karta raqamlari, bank hisoblari va boshqalar) noqonuniy olish bilan bog'liq jinoiy harakatni sodir etish orqali amalga oshiriladi. **Skimmer** (skimmer, skimmer qurilmasi, kartalar skimmeri) - skimmerlar deb ataladigan kartalardan ma'lumotlarni o'qish uchun maxsus qurilmalardan foydalanishga qaratilgan portativ qurilma. Hujumchilar kartaning magnit chizig'idan egasining ismini, karta raqamini va boshqa ma'lumotlarni ko'chiradi. Jinoyatchilar PIN-kodni yashirincha aniqlash maqsadida bankomat klaviaturasiga mini-kameralar yoki ustki qavat o'rnatadilar. Ular karta ma'lumotlarini olgandan so'ng jinoiy xarakterdagi boshqa ko'plab noqonuniy harakatlarni amalga oshiradilar. Zamonaviy dunyoda kiberjinoyatlarning yana bir keng tarqalgan turi bu **Internet-bankingdir**. Ushbu kiberjinoyatning mohiyati pul mablag'larini o'zboshimchalik bilan olib qo'yish,

turli shakllarda tovlamachilik yo'li bilan noqonuniy boyishda namoyon bo'ladi. Yana ko'plab jinoyatlar mavjud va shuni takidlab aytish kerakki, ilmiy-texnikaviy taraqqiyot bir joyda turmaydi va innovatsion, telekommunikatsiya texnologiyalari jadal rivojlanmoqda va shu bilan birga axborot texnologiyalardan foydalanish dinamikasi faol amalga oshirilmoqda, buning natijasida kiberjinoyatlarning yangi turlari paydo bo'lmoqda. Yuqoridagilardan kelib chiqib, qonunchilik va xalqaro me'yoriy-huquqiy hujjatlar tahlili asosida shuni aytish mumkinki, kiberjinoyatlarning o'ziga xos xususiyati axborot kommunikatsiya texnologiyalaridan noto'g'ri foydalanishdan iborat bo'lib, noqonuniy xatti harakatlar virtual kibermakonda sodir etilishidadir. Uning chegarasi va bepoyonligi shunga mos ravishda transmilliy jinoyatlar maqomiga ega. Kiberjinoyatlar odatda yashirin, doimiy yoki bir martalik bo'lib, turli innovatsion ommaviy axborot vositalari va ularning dasturiy ta'minotidan foydalangan holda amalga oshirilishi mumkin. Bunday jinoyatlarga oid dalillar asosan axborot tarmoqlarida uzatiladi va saqlanadi. Elektron texnologiyalardan foydalanish tajovuzkor shaxsni, qonunga xilof xatti-harakati va geografik joylashuvini aniqlashda muammolarni keltirib chiqaradi.

TAHLIL VA NATIJALAR

Kiberjinoyatlarning subyektlari nafaqat axborot texnologiyalari sohasida tegishli bilimga ega bo'lgan, ular orqali ushbu kiberharakatlarni amalga oshiradigan mutaxassislar, balki har xil turdagi firibgarlar, tovlamachilar, reketlar, terrorchilar, sutenyorlar, pedofillar, odam savdosi, qurol, giyohvand moddalar bilan savdo qiladigan shaxslardir. Kiberjinoyatlar asosan iqtisodiy maqsadlarga erishish uchun va ko'pincha katta miqyosda amalga oshiriladi, kiberjinoyatchilar esa buning uchun shaxsiy ma'lumotlardan foydalanadilar. Shu bilan birga kiberjinoyatning elementi guruhli, tashkiliy xususiyatga ega va ular transmilliy shaklga ega bo'lishi mumkin. Bunday jinoyatlarga samarali qarshi turish uchun turli davlatlar o'rtasida samarali hamkorlikni tashkil etish zarur. Jinoyat obyektiga ko'ra kiberjinoyatlarni shartli ravishda ma'lum guruhlariga bo'lish mumkin va ular "**Kiberjinoyatlar to'g'risidagi xalqaro konvensiya**" ga muvofiq quyidagilarga bo'linadi:

1) Kompyuter ma'lumotlari va tizimlarining maxfiyligi, yaxlitligi va mavjudligiga qarshi jinoyatlar;

2) Kompyuterlar bilan bevosita bog'liq jinoyatlar;

3) Mualliflik huquqi va turdosh huquqlarning buzilishi bilan bog'liq jinoyatlar.

Birinchi guruhga, ya'ni kompyuter ma'lumotlari va tizimlarining maxfiyligi, yaxlitligi va mavjudligiga qarshi jinoyatlar kiradi: «noqonuniy foydalanish», «noqonuniy ushlab», «kompyuter ma'lumotlari yoki tizimlariga ta'sir qilish». Kompyuter ma'lumotlarini (tizimlarini) noqonuniy ravishda qasddan buzish, o'chirish, o'zgartirish yoki blokirovka qilishni anglatadi.

Ikkinchi guruhga bevosita kompyuter vositalaridan foydalanish bilan bog'liq jinoyatlar kiradi. Bularga «soxtakorlik» va «kompyuter firibgarligi» kiradi. Aytish mumkinki hozirgi kunda bunday keng tarqalgan jinoyatlar yangi axborot muhitida tez rivojlanib kelmoqda. Kompyuter texnologiyalaridan foydalangan holda qalbakilashtirish, soxta kompyuter ma'lumotlarini kiritish, o'zgartirish, o'chirish yoki blokirovka qilish bilan bog'liq bo'lgan zararli va noqonuniy harakatlarni o'z ichiga oladi, bu ma'lumotlarning haqiqiylikini buzishga olib keladi.

Uchinchi guruhga ishlab chiqarish kompyuter tizimi orqali tarqatish maqsadida foydalanish, tarqatish va sotib olish uchun taklif va (yoki) ta'minlash, shuningdek, kompyuter orqali mualliflik huquqini buzilishi kiradi.

XULOSA

Mamlakatimiz Jinoyat kodeksining XXI-bobi “Axborot texnologiyalari sohasidagi jinoyatlar” (278¹ -278⁷-moddalari) axborot texnologiyalari sohasiga oid yetti moddasida va boshqa qonun hujjatlarida axborot tizimlari, internet tarmog'idagi axborotdan foydalanuvchilar, provayderlar, ommaviy axborot vositalarining va boshqalarning javobgarligi to'g'risidagi ayrim qoidalarning yetishmasligidir. Shu sababli O'zbekiston Respublikasi Jinoyat kodeksiga o'zgartishlar va qo'shimchalarni ishlab chiqish va belgilangan tartibda kiritishning real zarurati vujudga keldi. Jinoyat kodeksiga o'zganing mulkini o'g'irlash (o'g'irlik, firibgarlik, tovlamachilik), aloqa tarmoqlari, shu jumladan Internet bilan bog'liq jinoyatlarni tartibga solish bo'yicha axborot tizimi va ma'lumotlarga ruxsatsiz kirish, plastik va kredit kartalar orqali pul mablag'larini yechib olish bilan bog'liq ma'lumotlarni qo'shib, o'zgartirish va qo'shimchalar kiritish maqsadga muvofiq deb hisoblayman. Hozirgi zamonaviy voqelikni hisobga olgan holda “kiberjinoyat” ning kompleks tushunchasini belgilash uchun ushbu jinoyatlarning asosiy elementlarini aniqlash bo'yicha ilmiy tadqiqotlar olib borish va ushbu ijtimoiy xavfli qilmishlarni tergov qilish metodologiyasini ishlab chiqish zarur.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. Salayev N.S, Ro'ziyev R.N “Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar”. Monografiya, – T: TDYU, 2018, 139-b.
2. Anorboyev A.U “Kiberjinoyatchilik, unga qarshi kurashish muammolari va kiberxavfsizlikni taminlash istiqbollari”. Monografiya – T: Milliy gvardiya instituti, 2020. – 324 b.
3. Борова Д.М. Расследование киберпреступлений // Пробелы в российском законодательстве. №2. 2018. С. 173-175-b
4. O'zbekiston Respublikasining Qonuni Kiberxavfsizlik to'g'risida. Toshkent 2022
5. <https://lex.uz/uz/docs/-5960604>
6. <https://iiv.uz/news/kiberjinoyatchilikka-qarshi-kiberxavfsizlik>
7. <https://uz.wikipedia.org/wiki/Kiberjinoyat>

8. <https://hi-in.facebook.com/hackituz/posts/kiber-jinoyatchilik-va-uning-turlari-kiber-jinoyat-turli-shakllarda-bolishi-mumki/107669145001486/>
9. <https://community.uzbekcoders.uz/post/kiber-hujumlarni-turlari-61a7b21306b0a14545b7f422>
10. <https://fayllar.org/axborot-kommunikatsiya-tizimlarida-kiberjinoyatchilik-tahlili>.