ISSN 2181-3187

HOZIRGI VAQTDA AXBOROT-TEXNOLOGIYALARI SOHASIDA SODIR ETILAYOTGAN JINOYATLARNING YANGI USULLARI

Sharipov Asilbek Dilmurod o'g'li
O'zbekiston respublikasi Ichki ishlar vazirligi akademiyasi kursanti

ANNOTATSIYA

Ushbu maqolada bugungi kunda yurtimizda axborot-texnologiyalari sohasida sodir etilayotgan jinoyatlarning yangi usullari,ularni kvallifikatsiya qilish sohasidagi ayrim dolzarb masalalar,sodir etilayotgan kiberjinoyatlarning umumiy statistikasi, hamda ularni oldini olishga qaratilgan profilaktik tavsiyaviy chora-tadbirlar haqida so'z yuritiladi.

Kalit so'zlar: Fishing, kibermakon, shaxsga oid ma'lumotlar, Nigeriyalik xati, Scam-419, Webmoney, kriptovalyuta.

ANNOTATION

This article illustrates new methods of crimes committed in the field of information technologies in our country today, some urgent issues in the field of their qualification, and preventive and recommended measures aimed at preventing them.

Keywords: Phishing, cyberspace, personal information, scam-419, webmoney, Nigerian letters, cryptocurrency

АННОТАТЦИЯ

В данной статье говорится о новых способах совершения преступлений в сфере информационных технологий в нашей стране сегодня, некоторых актуальных вопросах в области их квалификации, а также профилактических и рекомендуемых мерах, направленных на их предотвращение

Ключевые слова: Фишинг, Киберпространство, Персональная информация, Нигерийское письмо, Scam-419, Webmoney, Криптовалюта

Hech qaysimizga sir emaski, XXI asr axborot-texnologiyalari asri ,shunday bo'lishi bilan bir qatorda ushbu sohada sodir etilayotgan jinoyatlarning paydo bo'lish va to'xtovsiz yangi bosqichga ko'tarilib borish asri ham hisoblanadi.Ayniqsa sodir etilayotgan bu turdagi jinoyatlarni fosh etish, aniqlash ham shunga yarasha kasb, malaka qolaversa bilimlar sohasini doimiy ravishda kengaytirib borishni taqozo etadi.

Axborot texnologiyalari sohasidagi jinoyatlarning ayrim turlarini quyidagilarda ko'rish mumkin:

1. virusli dasturiy ta'minotni tarqatish;
2. foydalanuvchining maxfiy ma'lumotlarini o'g'irlash;
3. boshqa odamlarning intellektual faoliyat mahsulotlarini o'g'irlash;
4. ijtimoiy tarmoqlarda boshqalarning akkauntlarini buzish;

ISSN 2181-3187

5. yolg'on ma'lumot tarqatish, tuhmat qilish;
6. millatlararo nizo yoki dinlararo adovatni qo'zg'atish.
7. bank plastik kartalari (karta rekvizitlari) bilan noqonuniy operatsiyalar;
8. qimmatli qog'ozlar bozoridagi Internet-firibgarlik;
9. Internetdagi moliyaviy piramidalar;
10. mobil aloqa bilan bog'liq jinoyatlar;
11. elektron tijorat sohasidagi boshqa jinoyatlar.

Ushbu turdagi jinoyatlar kibermakonda axborot-texnologik vositalar yordamida sodir etiladi. **Kibermakon**[1] — axborot texnologiyalari yordamida yaratilgan virtual muhit hisoblanadi. **kiberjinoyatchilik** esa axborotni egallash, uni o‘zgartirish, yo‘q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta’minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig‘indisidir.

O'zbekiston Respublikasi Prezidenti huzuridagi Statistika agentligi bergan ma’lumotlarga ko’ra 2022-yil yurtimizda o’g’irlik jinoyati **15237** ta firibgarlik jinoyati esa **20591 ta** sodir etilgan bo’lib ularning har to’rtdan biri axborot-texnologiyalari sohasida sodir etilgan.Bundan tashqari birgina 2022-yilning o’zida mutaxassislar kiberjinoyatlardan etkazilgan zararni 3 trillion dollarga baholashgan.

O’zbekiston hududida 2023-yilda quyidagi usullarda kiberjinoyatlar sodir etilmoqda:

1.Kiberfiribgarlar sizga o’zini bank xavfsizlik xizmati xodimi deb tanishtiradi hamda sizning kartangizga onlayn kredit rasmiylashtirilayotgani yoki sizning mavjud bank hisob raqamingizga texnik vositalar orqali begona shaxs kirmoqchi bo’layotganini vaj qilishib sizdan karta ma’lumotlarizngiz hamda ushbu kartadagi pul mablag’larini boshqarishga bo’lgan huquqni qo’lga kiritishadi.Ushbu usulning ijtimoiy xavfi shundaki, agar sizning bank kartangizda mablag’ bo’lmasa ham keyinchalik firibgarlar sizning kartangizdan “DROP” sifatida foydalanishadi, yani boshqa jabrlanuvchilardan o’g’irlangan mablag’larni sizning kartangizga otkazishadi hamda jinoyat izlarini yoqotish uchun sizning kartangizdan pul mablag’larini kriptovalyuta birjasiga o’tkazishib u yerdan kriptovalyuta sotib olishadi. So’ngra kriptovalyutalarni sotishib o’g’irlangan pul mablag’larini o’zlarinikiga aylantirib olishadi.Siz esa umuman xabaringiz yoq jarayonlar uchun huquqni muhofaza qiluvchi organlarga chaqirtirilasiz. Bu esa keyinchalik siz uchun ko’plab ovoragarchiliklar keltirib chiqaradi.

2. Olx.uz, Online savdo, E-auksion kabi shunga o’xshash platformalarda firibgarlar boshqa shaxslar tomonidan sotuvga qo’yilgan e’lonlar, rasmlar, ularning ma’lumotlari-ism-familiyasi, telefon raqamidan jinoyat qilish maqsadida

[1] 2022-yil 15-aprelda qabulqilingan “Kiberxavfsizlik to’g’risida”gi qonunning 3-moddasi

ISSN 2181-3187

foydalanishadi. Ya'ni ularning ma'lumotlarini ko'chirib olishib o'zlarining shaxsiy sahifalariga joylashtirishadi. Qisqacha qilib aytganda baliq tutish (fishing)uchun **qarmoq** tashlab qo'yishadi.Siz ushbu soxta sotuvga qo'yilgan mahsulotni xarid qilish maqsadida u bilan aloqaga chiqqaningizdan boshlab siz uning qarmog'iga ilina boshlagan o'ljalardan biriga aylanasiz.Shunda firibgar sizga ushbu sotib olmoqchi bo'lgan mahsulotingiz uchun siz uni band qilib qo'yishingiz lozimligi aks holda esa uni boshqa xaridorga sotib yuborishini bildirib sizni ishonchingizga kirishadi. Ko'pincha firibgarlar soxta mahsulotlarni odamlarni o'ziga jalb etish uchun odatdagidan ancha pastroq narxlarda joylashtirishadi.So'ng esa to'lovni amalga oshirish uchun sizdan kelgan kodni so'rashadi yoki sizga soxta havola yuborishadi va kartangizda operatsiyalar amalga oshirishga bo'lgan huquqni qo'lga kiritshadi.Bu usulning xavflilik jihati shundaki, nafaqat mol mulk talon-taroj qilinadi, balki shaxsga oid malumotlar to'g'risidagi qonunchilik ham buziladi.**Shaxsga doir ma'lumotlar**[1] deganda muayyan jismoniy shaxsga taalluqli bo'lgan yoki uni identifikatsiya qilish imkonini beradigan, elektron tarzda, qog'ozda va (yoki) boshqa moddiy jismda qayd etilgan axborot tushuniladi.

Yuqoridagi holatda esa tezkor xodimlar umuman jinoyatga aloqasi bo'lmagan,haqiqatdan mavjud mol-mulkini sotish maqsadida ijtimoiy tarmoqqa joylashtirgan shaxslarni chaqirishga majbur bo'lishadi.Chunki firibgarlar ushbu shaxslar tomonidan joylashtirilgan ma'lumotlardan foydalanishadi.

3.Yurtimizda eng keng tarqalgan kiberjinoyatlarning sodir etilish usullaridan yana biri bu sizga ko'p miqdorda meros qoldi deb sizga smslar yoki ijtimoiy tarmoqdan har xil xabarlar keladi va sizga haqiqatdan sizning ma'lumotlaringiz aks etgan soxta meros hujjatlarining rasmini yuborishadi. Ushbu holatga birinchi marta duch kelgan odam unga meros qolishi mumkin bo'lgan pul summasini ko'rib hayratga tushadi. Firibgarlar sizdan mablag'larni O'zbekistonga yuborish uchun soliq so'rashayotganini vaj qilishib sizdan pul undirmoqchi bo'lishadi hamda sizga hisob raqamini tashlashadi. Bu turdagi kiberjinoyat turi Scam-419 yoki "Nigeriyalik xati"deb nomlanadi.Afsuski amaliyotda hattoki katta miqdorda pul mablag'larini firibgarlarga o'z xoshishi bilan o'tkazib berayotganlar kam emas.Bu usulning ijtimoiy xavfli jihati shundaki, jinoyatni ochish o'ta murakkab chunki firibgar O'zbekiston hudida emas,qolaversa uning ma'lumotlarini yig'ish ham qiyin.

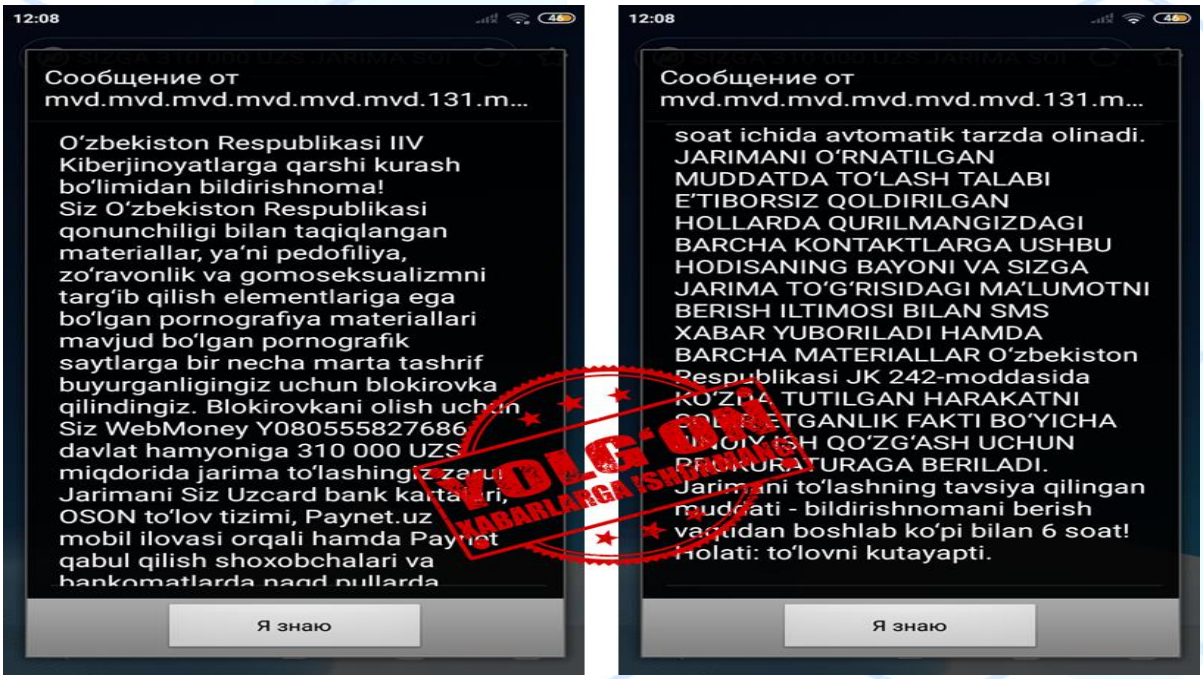
4. Firibgarlar to'lov operatorlari nomidan qo'ng'iroq qilib, tizimda qandaydir xatolik yuz berganini yoki tizim yangilangani sabab unga raqamni qayta ulab qo'yishni ro'kach qilishadi.Agar raqamni ulash uchun kodni berishmasa foydalanuvchilar

[1] 2019-yil qabul qilingan O'zbekiston Respublikasining 547-sonli "Shaxsga doir ma'lumotlar to'g'risida"gi qonuning 4-moddasi

ISSN 2181-3187

tarmoqdan uzib qo‘yilishlari, pul o‘tkazish/yechish amaliyotlarini bajara olmasliklarini hamda bloklanib qolishlarini aytib, bosim o‘tkazishadi.Yana bir ahamiyatli jihati, ular rus tilida muloqot qilishadi, bu esa ularning chindan ham to‘lov tashkilotlarining operatorlari ekanligiga ishonchni oshiradi.Agar ulardan o‘zbek tilida muloqot qilishlarini so‘rashsa, ular telefonni yopib qo‘yishadi. Kompaniya operatorining qayd etishicha, aholining ayrim qismi rus tilida yaxshi muloqot olib bora olmasliklari sabab firibgarlar aholi bilan aynan shu tilda gaplashishadi. Bu esa ularga yanada ta’sir o‘tkazishga sabab bo‘ladi

5.Ko’pincha fuqarolar,ayniqsa o’smir yoshlar har xil turdagi behayo saytlarga kirishganda quyidagi sahifa chiqib qoladi:



So‘nggi paytlarda fuqarolarimiz tomonidan pornografik foto va video mahsulotlarni targ‘ib qiluvchi internet resurslaridan foydalanish jarayonida boshqa shu kabi resurslarga avtomatik tarzda o‘tib ketish orqali «O‘zbekiston Respublikasi IIV Kiberjinoyatlarga qarshi kurash bo‘limidan bildirishnoma» sarlavhasi ostida sizib chiquvchi oynada foydalanuvchining taqiqlangan saytlarga kirgani sababli go‘yoki IIV tomonidan u 200 000 so‘m (ayrim hollarda 300 000 so‘m) miqdorida jarimaga tortilgani va «Webmoney» elektron to‘lov tizimi orqali davlat hisobiga to‘lovni amalga oshirilishi lozimligi, aks holda qurilmada saqlangan kontaktlarga foydalanuvchining pornografik foto va video mahsulotlar joylashtirilgan internet resurslaridan foydalangani haqida hodisa bayoni hamda foydalanuvchiga jarimani to‘lashi talabi bilan SMS-xabar yuborilishi haqida ma’lumot paydo bo‘lmoqda. Shu bilan birga, foydalanuvchilarning internet veb brauzeri blokirovka holatiga tushib qolmoqda.E’tibor beradigan bo’lsak ushbu sahifa havolasi hech qanaqa himoya

ISSN 2181-3187

tizimiga ega emas qolaversa pornosaytlarga tashrif buyurganlik uchun qonunchilikda hech qanaqa javobgarlik belgilanmagan.

Bundan tashqari O‘zbekiston Respublikasi Ichki ishlar vazirligi tarkibida «Kiberjinoyatlarga qarshi kurash bo‘limi» nomi bilan faoliyat yurituvchi bo‘lim yoki bo‘linma mavjud emas ammo Kiberxavfsizlik markazi mavjud, «**Webmoney**» to‘lov tizimida O‘zbekiston Respublikasi IIV tarkibiy va hududiy tuzilmalari elektron hamyonlariga ega emas.Bu tuzoqqa ko’pincha o’smirlar tushib qolmoqda.Ular ota-onalariga jarima kelishidan qo’rqishib yashirincha firibgarlar hisobiga so’ralgan pul mablag’larini o’tkazib berishmoqda.

Axborot-texnologiyalari sohasida sodir etilgan jinoyatlarni fosh etish qanchalik murakkab bo’lsa uni tergov qilish ham shunchalik bilim,malakani talab etadi,ayniqsa kvallifikatsiya qilish bilan bo’gliq bir qator muammolarga duch kelish mumkin.

Axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib firibgarlik sodir etish (JK 168-moddasi uchinchi qismi “g” bandi) deganda, moliya, bank muassasalari, fondlar va sh.k. larda bo‘lgan mulkni aldov yo‘li bilan kompyuter texnikasi vositalari, aloqa vositasi, planshet yoki boshqa shu kabi texnik qurilmalar yordamida manipulatsiya qilish orqali amalga oshiriladigan talon-toroj tushuniladi[2]. Bunday firibgarlik kompyuter tizimida ishlov beriladigan, tegishli axborot tashuvchilarda saqlanadigan yoki ma’lumotlarni uzatish tarmoqlari bo‘yicha beriladigan axborotni o‘zgartirish yo‘li bilan ham, kompyuter tizimiga yolg‘on axborot kiritish yo‘li bilan ham sodir etilishi mumkin.

Axborot tizimidan, shu jumladan axborot texnologiyalaridan foydalanib sodir etilgan firibgarlik jinoyatini qonunga xilof ravishda (ruxsatsiz) axborot tizimiga kirib yoki undan foydalanib sodir etilgan o‘g‘irlik jinoyatidan farqlashda shuni nazarda tutish lozimki, firibgarlikda jabrlanuvchi aldov yoki ishonchi suiiste’mol qilinishi oqibatida mulkini yoki unga bo‘lgan huquqni axborot texnologiyalaridan foydalanib aybdor egaligiga ixtiyoriy ravishda o‘tkazadi, bunda mulk o‘z egaligidan chiqib ketayotganligini jabrlanuvchi anglagan bo‘lishi kerak. Bundan kelib chiqadiki agar jabrlanuvchining o’zi mablag’ni tashlab bersa u holda ijtimoiy xavfli qilmish jinoyat kodeksi 168-moddasi 3-qismi “g” bandi bilan agar jinoyatchining o’zi jabrlanuvchining hisob raqamini boshqarish huquqini qo’lga kiritb yechib olsa jinoyat kodeksi 169-moddasi 3-qismi “b” bandi bilan jinoiy javobgarlik vujudga keladi.Ammo shunga e’tibor berish kerakki agar talon-taroj qilingan mol-mulk qiymati bazaviy hisoblash miqdorining 500 barobaridan ortiq bo’lsa u holda qilmish yuqoridagi holatda emas balki balki 168 chi hamda 169-moddaning 4-qismi “a”bandi bilan kvallifikatsiya

[2] 2023-yil 23-iyunda qabul qilingan firibgarlikka oid Oliy Sud plenum qarorining 22-bandi.

ISSN 2181-3187

qilinadi.Asos esa jinoyat kodeksining 33-moddasi 2-qismi ya’ni agar shaxs sodir etgan qilmishda ushbu Kodeks Maxsus qismi ayni bir moddasining turli qismlarida nazarda tutilgan jinoyatlarning alomatlari mavjud bo‘lsa, u moddaning og‘irroq jazo belgilangan qismi bo‘yicha javobgarlikka tortiladi.

Yuqoridagi holatlar ro’y bermasligi uchun shaxslardan e’tiborliroq bo’lishlari qolaversa, e’lonlardagi har qanday aksiyalar, pul yutuqlari hamda boshqa takliflarni tashkilotlarning rasmiy veb-sahifasidan qayta tekshirishi,saytning rasmiyligiga ishonch hosil qilmasdan ularga o‘z shaxsiy ma’lumotlarni kiritmasligi,ijtimoiy tarmoq hamda messenjerlarda tarqatilayotgan, aksiya va yutuqli lotereya o‘yinlari to‘g‘risidagi reklamalar keltirilgan havolalarni tekshirmasdan oldin ochmasligi,rasmiy emas havolalarni boshqalarga tarqatmasligi lozim.

FOYDALANILGAN ADABIYOTLAR RO’YXATI:

1. O‘ZBEKISTON RESPUBLIKASINING JINOYAT KODEKSI. 22.09.1994
2. . O‘ZBEKISTON RESPUBLIKASINING JINOYAT-PROTSESSUAL KODEKSI .22.09.1994
3. O‘ZBEKISTON RESPUBLIKASINING QONUNI KIBERXAVFSIZLIK TO‘G‘RISIDA.O'RQ-764-сон 15.04.2022
4. O‘ZBEKISTON RESPUBLIKASINING QONUNI SHAXSGA DOIR MA’LUMOTLAR TO‘G‘RISIDA.O'RQ-547-сон 02.07.2019
5. O‘ZBEKISTON RESPUBLIKASI OLIY SUDI PLENUMINING QARORI FIRIBGARLIKKA OID ISHLAR BO‘YICHA SUD AMALIYOTI TO‘G‘RISIDA. 17-сон 23.06.2023.