KIBERFIRIBGARLIK JINOYATLARI QURBONLARINING IJTIMOIY PORTRETI

Allambergenov Islambek Sadatdinovich
O‘zbekiston Respublikasi Kriminologiya tadqiqot instituti ilmiy xodim-tadqiqotchisi

Annotatsiya. *Ushbu maqolada kiberfiribgarliklar qurbonlarining demografik hamda ijtimoiy-iqtisodiy xususiyatlari tahlili asosida ularning ijtimoiy portreti taqdim etiladi.*
Kalit so‘zlar: *kiberfiribgarlik, viktimizatsiya, ijtimoiy portret, qurbonlar.*

Аннотация. *В работе представлен социальный портрет жертв кибермошенников на основе анализа их демографических и социально-экономических характеристик.*
Ключевые слова: *кибермошенничество, виктимизация, социальный портрет, жертва.*

Abstract. *The paper presents a social portrait of victims of cybercriminals based on the results of a study of their demographic and socio-economic characteristics.*
Keywords: *cyber fraud, victimization, social profile, victim.*

Kiberjinoyat – axborot texnologiyalari *(qurilma va/yoki tarmoq)* orqali sodir etiladigan hamda jamiyat uchun xavf tug‘diradigan jinoyat turi. Agar bunday harakatlar iqtisodiy maqsadga qaratilgan bo‘lsa, ular kiberfiribgarlik deb ataladi va asosan moddiy *(masalan, pul o‘g‘irlash yoki aldash orqali moliyaviy foyda olish)* yoki boshqa turda zarar yetkazishga qaratilgan bo‘ladi *(masalan, ma’lumotlarni o‘g‘irlash yoki o‘zgartirish, bevosita moliyaviy manfaat ko‘zlanmasdan).* Bunday qilmishlar uchun javobgarlik O‘zbekiston Respublikasi Jinoyat kodeksining tegishli moddalarida nazarda tutilgan. *(168-m. 3-q. “g” b. va 169-m. 3-q. “b” b.).*

Kiberfiribgarlik jinoyat sifatida qurbonga nisbatan bir necha ta’sir strategiyalariga ega, jumladan:

Vishing (ingl. voice+phishing) – telefon orqali amalga oshiriladigan firibgarlik bo‘lib, jinoyatchilar “ijtimoiy injeneriya” usullari yordamida qurbondan maxfiy ma’lumotlarni olishga urinadi.

Fishing (ingl. phishing) – Internet firibgarligi turi hisoblanib, jinoyatchilar, odatda, elektron pochta orqali yuborilgan havolalar yordamida qurbonni maxfiy ma’lumotlarni berishga majburlashadi.

Axborot texnologiyalari jamiyat uchun foydali, albatta. Ular tranzaksiyalar uzunligi bilan bog‘liq xarajatlarni qisqartirishga imkoniyat yaratdi. Biroq, shu bilan birga, bu texnologiyalardan foydalanishda yangi xarajatlar paydo bo‘ldi. Ko‘pincha tarmoqning “nozik joyi” axborot texnologiyalari emas, insonning o‘zi hisoblanadi. Hozirgi jamiyat kiberfiribgarlarni ancha yaxshi tanib, ularga qarshi kurasha oladi, lekin firibgarlik texnologiyalari tinimsiz rivojlanib bormoqda. Bu esa kibermakondagi jinoyatchilarga aholining yangi qatlamlarini qurbon qilish imkonini beradi.

Dunyo miqyosida kiberfiribgarliklar 1990-yillar oxiri va 2000-yillar boshlarida shakllandi. Ilk “fishing” xatlari 1996–1997-yillarda “America online” kompaniyasi *(internet-provayder va onlayn-servis platforma)* foydalanuvchilariga qarshi qo‘llanilgan, bu kiberfiribgarlikning klassik boshlanishi

hisoblanadi. 2000-yillarga kelib elektron pochta orqali moliyaviy aldovlar, soxta loyihalar va “Nigeriya maktublari” deb tanilgan sxema ommalashdi.

2004–2007-yillarda onlayn-bank va elektron to‘lov tizimlarining kengayishi firibgarliklarga yangi yo‘l ochib, “fishing”, “keylogger” *(klaviaturada tergan barcha tugmalarini yashirincha qayd etuvchi zararli dastur)* va “ilk ijtimoiy injeneriya” usullari jadal rivojlandi. 2010-yillarga kelib smartfonlar va mobil to‘lovlar ommalashganda kiberfiribgarlik global industriya darajasiga yetdi [1].

O‘zbekistonda kiberfiribgarlik bilan bog‘liq holatlar 2014-yildan keyin paydo bo‘la boshladi. Bu onlayn-banking va internet-xizmatlar ommalashuvi bilan bog‘liq. Firibgarlar bank xodimi sifatida o‘zlarini tanishtirib, mijozlar ma’lumotlariga ega bo‘lish uchun telefon qo‘ng‘iroqlaridan faol foydalana boshladi. Kibermakonni tartibga soluvchi mustahkam qonuniy baza hali shakllanmagan edi. Shu tufayli kiberfiribgarlar maxfiy ma’lumotlarni qo‘lga kiritish maqsadida “ijtimoiy injeneriya”dan keng foydalangan. Internet hali rivojlanishning boshlang‘ich bosqichida bo‘lgani uchun uning qamrovi ham keng emas edi. Kiberfiribgarliklardan eng ko‘p jabr ko‘rganlar asosan yoshi katta insonlar bo‘lgan.

AQSH Federal tergov byurosi Internet jinoyatlari bo‘yicha murojaat markazining 2020-yilgi hisobotida AQSHda kiberfiribgarlik borasida murojaatlar soni 791 mingdan oshgani, bu esa tarixiy rekord ekani ыayd etilgan [2].

Shu bilan birga, “Ransomware” bo‘yicha yillik tahliliy hisobotda 2020-yildagi kiberhujumlar 150 foizga o‘sib, asosan, tibbiyot muassasalari, laboratoriyalar va vaksina logistikasi kabi hayotiy muhim infratuzilmalar nishonga olingan [3].

“Google Threat Analysis Group” pandemiya davrida har kuni “COVID” mavzusi bilan bog‘liq 18 millionga yaqin zararli xabar va fishing urinishlarini bloklaganini ma’lum qildi [4].

Yevropa Ittifoqining Kiberxavfsizlik agentligi hisobotlarida aytilishicha, ish va ta’limning onlayn shaklga o‘tishi “DdoS” *(xizmatni ishdan chiqarish uchun ommaviy trafik bilan bosim o‘tkazish hujumi)* hujumlari jadalligini oshirdi. Yevropa Ittifoqi qo‘shma politsiya xizmatining 2021-yilgi hisobotida esa pandemiyadan foydalanib amalga oshirilgan investitsion firibgarlik, soxta grant va “yordam puli” platformalari keng tarqalgani ta’kidlanadi. Microsoft ham vaksina, test natijalari va karantin qoidalari mavzusidagi “spear-phishing” kampaniyalari millionlab foydalanuvchilarni nishonga olganini bildirgan. Hatto Butunjahon sog‘liqni saqlash tashkiloti nomi bilan tarqatilgan soxta xatlar ham sezilarli darajada ko‘paygan [5].

“Deloitte” kompaniyasi kiberxavfsizlik va tahdidlarni kuzatishga ixtisoslashgan global markazi tahlillariga ko‘ra, uydan ishlash rejimi korporativ tarmoqlar xavfsizligini susaytirib, ochiq Wi-Fi orqali hujumlar uchun yangi imkoniyatlar yaratdi [6].

Ikkinchi bosqich COVID-19 pandemiyasi davrini qamrab oladi. 2019–2020-yillardagi pandemiya davri aholiga onlayn xizmat ko‘rsatish sohasining keskin rivojlanishiga olib keldi va bu esa yangi firibgarlik usullarining paydo bo‘lishi hamda mavjud sxemalarning yanada kuchayishi uchun turtki bo‘ldi. Shu davrda “Telegram” orqali tarqatilgan “apk-fayllar” yordamida amalga oshirilgan virusli hujumlar ommalashdi, ular foydalanuvchilarning shaxsiy ma’lumotlari o‘g‘rilari edi. Shu paytdan boshlab kiberfiribgarlik jabrdiydalari ijtimoiy portreti yosharib bordi.

2020–2021-yillarda COVID-19 pandemiyasi tufayli dunyo miqyosida raqamli xizmatlarga ommaviy o‘tish kiberxavfsizlikka tahlikalarning keskin oshishiga sabab bo‘ldi. “Check Point Research” ma’lumotlariga ko‘ra, pandemiya boshlanishi bilan fishing hujumlari 220 foizga ortib, kiberjinoyatchilar uchun misli ko‘rilmagan imkoniyatlar ochildi. INTERPOL esa “COVID”, “vaccine”, “corona” kabi mavzulardagi soxta domenlar tez sur’atda ko‘payib, global kiberfiribgarlik kampaniyalarining asosiy quroliga aylanganini qayd etdi [7].

Bu global tendensiyalar O‘zbekistonda ham o‘z aksini topdi: pandemiya davrida mamlakatda kiberhujum va kiberfiribgarlik holatlari keskin ko‘paydi. 2024-yilda 12 milliondan ortiq kiberhujum urinishlari aniqlangan, firibgarlik holatlari esa o‘tgan yilga nisbatan 34 foizga oshgan.

Pandemiya nafaqat sog‘liqni saqlash tizimini, balki butun dunyo kiberxavfsizlik arxitekturasini jiddiy sinovdan o‘tkazdi.

O‘zbekistonda 2024-yilda sodir etilgan kiberfiribgarlik jinoyatlarining foiz ko‘rsatkichlari va turlari:

– firibgarliklarning 34 foizi moliyaviy yordam taklif qiluvchi soxta havolalar yuborish orqali;

– 22 foizi majburiyatlarni bajarish niyatisiz avans to‘lovlarini olish holatlariga to‘g‘ri kelgan;

– 17 foiz holatda firibgarlar o‘zlarini bank xodimi sifatida tanishtirib, telefon orqali amalga oshirgan;

– 14 foizi onlayn-savdo maydonchalari orqali ma’lumot o‘g‘irlash bilan bog‘liq;

– 9 foiz holatlar moliyaviy onlayn-birjalardagi firibgarliklarga to‘g‘ri keladi [8].

Kiberfiribgarlikning hozirgi bosqichida texnik vositalarni buzishdan ko‘ra “ijtimoiy injeneriya”dan foydalanish ancha kengaydi. Bunday tendensiya fishing saytlarini huquqni muhofaza qiluvchi organlar va raqamli texnologiyalar vazirligi tomonidan samarali monitoring qilish bilan izohlanadi. Ammo istalgan tizimdagi eng “nozik element” – bu insonning o‘zi.

2024-yilda barcha firibgarlik borasidagi arizalarning taxminan 35 foizi to‘lov kartalari bilan bog‘liq hodisalarga to‘g‘ri keladi. Bu kartalardan foydalanuvchilar sonining 40 milliondan kam darajadan 55 milliondan ortiq ko‘rsatkichga o‘sishi bilan bog‘liq.

Bundan tashqari, pandemiya boshlanganidan buyon firibgarlik usullari telefon qo‘ng‘iroqlaridan ancha zamonaviy sxemalarga ko‘chdi. Natijada so‘nggi besh yil ichida kiberjinoyatlar soni 68 barobarga oshdi, ularning umumiy jinoyatchilikdagi ulushi esa 2023-yildagi 6,2 foizdan 2024-yilda 44,4 foizgacha ko‘tarildi. 2021–2024-yillarda kiberjinoyatlardan kelgan zarar 1,9 trln so‘mdan oshdi. 2024-yilda mamlakatda rasman 35 mingdan ortiq firibgarlik holati qayd etilgan (2023-yilda 26 ming) [9].

Shunday qilib, COVID-19 pandemiyasi O‘zbekistonda kiberfiribgarlik o‘sishining katalizatoriga aylandi, bu esa ham holatlar sonining, ham ulardan yetkazilgan moliyaviy zararning sezilarli darajada ko‘payishiga olib keldi.

Huquqni muhofaza qiluvchi organlarning kiberxavfsizlik markazlari tahlilchilari kiberfiribgarliklar soni ham, ularning “o‘rtacha chiptasi” ham o‘sib borayotganini ta’kidlashgan. Bu kiberfiribgarlar harakatlari maqsadli va samarali tus olganini ko‘rsatadi, bu esa bizga kiberfiribgarlik qurbonining ijtimoiy portretidan foydalanish imkonini beradi.

Jahon amaliyotida kiberfiribgarlik qurbonlarining ijtimoiy portreti muayyan umumiy belgilar bilan tasvirlanadi. Eng avvalo, 18–35 yoshli yoshlar internetdagi faolligi, onlayn savdo va investitsiya platformalariga qiziqishi tufayli fishing hamda onlayn aldovlarning eng ko‘p jabrlanuvchilari sifatida qayd etiladi. Shu bilan birga, 55 yoshdan oshgan keksalar texnologiyani yaxshi bilmasligi sababli telefon orqali amalga oshiriladigan aldovlar va soxta texnik yordam sxemalariga tez ishonishadi. Onlayn-banking va tezkor to‘lov xizmatlaridan foydalanuvchilar ham zararli havolalar va soxta operatorlar orqali ko‘plab moliyaviy yo‘qotishlarga duch keladi. Masofaviy ish izlovchilar esa yolg‘on vakansiyalar va investitsiya takliflari tuzog‘iga tushish ehtimoli yuqori bo‘lgan toifaga kiradi. Emotsional ta’sirga tez beriladigan insonlar jarima, xavf, mukofot yoki shoshilinch xabar sifatida yuborilgan soxta bildirishlarga tez ishongani uchun ko‘p hollarda firibgarlar nishoniga aylanadi. Shuningdek, Internetda qimmat buyumlar, sayohatlar yoki moddiy farovonlikni ko‘p namoyon qiladigan foydalanuvchilar xakerlar tomonidan “yuksak potensial qurbon” sifatida baholanadi va ushbu toifa ham kiberfiribgarlikning asosiy jabrlanuvchilari qatoriga kiradi [10].

Ushbu jinoyatlar qurbonlari ijtimoiy portretini tuzishda bank tuzilmalari ma’lumotlari va IIVning viktimologik ma’lumotlariga tayanish maqsadga muvofiq, chunki aynan shu tuzilmalar qarz oluvchilar va shubhali tranzaksiyalar haqidagi eng to‘liq ma’lumotga ega. Bizning maqsad – umumiy qonuniyatlarni aniqlash va ushbu ijtimoiy portretning qanday o‘zgarishini prognoz qilish.

Chuqurroq tahlil uchun quyidagi har bir bandni alohida ko‘rib chiqish, xolisona va aniq tarzda ushbu ijtimoiy portretning ko‘rinishini namoyish etish maqsadga muvofiq.

1. Ilmiy tadqiqotlarda respondentlarning ijtimoiy portretini tuzish jarayonida jinsiy mansublik omillari ko‘p hollarda alohida ta’kidlanadi. Shu bilan birga, tanlangan namunada erkaklar va ayollar soni, odatda, bir-biriga mutanosib ravishda belgilanib, O‘zbekiston aholisining yosh va jins tuzilmasi tarkibini aks ettiradi.

2. Banklar va IIV ma’lumotlariga ko‘ra, kiberfiribgarlik qurbonlari yoshi keng diapazonga ega.

Lekin statistik ma’lumotlar shuni ko‘rsatadiki, qurbonlarning aksariyati iqtisodiy jihatdan eng faol aholi qatlamidir. Bu Yevropa bo‘yicha xorijiy ma’lumotlardan farq qiladi, u yerda 50 yoshdan oshgan shaxslar ko‘p hollarda kiberfiribgarlar tuzog‘iga tushadi.

3. Oilaviy holat “to‘suvchi mexanizm” sifatida muayyan ahamiyat kasb etadi. Gipoteza sifatida aytish mumkinki, nikohdagi shaxslar ko‘pincha bir-biri bilan maslahatlashadi va bu moliyaviy xavf-xatardan saqlanish imkonini oshiradi.

4. Shahar to‘lov qobiliyati yuqori aholini, turli xizmatlarni va iqtisodiy faollikni o‘zida mujassam etgan kuchli iqtisodiy markaz sifatida kiberfirib-garlar ta’siriga eng ko‘p moyil bo‘ladi.

5. Biroq bu yerda O‘zbekiston Respublikasi IIV statistikasiga ko‘ra viktimizatsiyaga (daromad darajasi bo‘yicha) eng ko‘p duchor bo‘luvchi toifa – doimiy daromad manbaiga ega bo‘lmagan shaxs-lar ekaniga e’tibor qaratish kerak. Gipoteza sifatida aytish mumkinki, bunday shaxslar “oson pul”ga ko‘proq moyil bo‘ladi, shu sababli aholining boshqa qatlamlariga nisbatan firibgarlar tuzog‘iga tez-tez tushadi. Shuningdek, doimiy ishga ega bo‘lma-ganlar doimiy ishlilarga nisbatan kiberfiribgarlik holatlariga ko‘proq duchor bo‘ladi, deb faraz qilish mumkin [11].

Ko‘plab xorijiy olimlar fikriga ko‘ra, kiberfirib-garlik qurbonlarining ijtimoiy portreti bir xil emas, ammo, unda ko‘p hollarda 25–44 yoshdagi ish-lovchi ayollar, o‘rta daromad va ma’lumotga ega bo‘lgan shahar aholisi uchraydi. Shu bilan birga, xavf guruhiga 50 yoshdan oshgan, xavfsizlikka kat-ta e’tibor qaratadigan va ishonchga moyil bo‘lgan shaxslar ham kiradi. Firibgarlar esa “ijtimoiy injeneriya”dan foydalanib, aholining istalgan zaif toifasiga ta’sir o‘tkazishi mumkin. Shu bois uni-versal qurbon portretini belgilab bo‘lmaydi [12].

Ushbu ijtimoiy portretlar tahlili bizga qaysi aholi qatlamlari viktimizatsiyaga eng ko‘p moyil ekanini tushunish imkonini beradi. Biroq, to‘liq tahlil uchun banklar ma’lumotlarini va O‘zbekiston Respublikasi huquqni muhofaza qiluvchi organ-larining kiberxavfsizlik markazlarining statistik ma’lumotlarini yanada chuqur o‘rganish talab etiladi.

Foydalanilgan manbalar

1. https://www.getcybersafe.gc.ca/en/resources/historyphishing?utm.com
2. https://www.ic3.gov/
3. https://www.sophos.com/
4. https://blog.google/threat-analysis-group
5. https://www.europol.europa.eu/
6. https://www2.deloitte.com/
7. https://research.checkpoint.com/
8. https://podrobno.uz/cat/proisshestviya/v-uzbekistane-kibermoshenniki-pod-vidom-rukovoditeley-vynuzhdayut-grazhdan-soobshchat-svoi-lichnye-d/
9. https://kun.uz/ru/news/2025/02/03/v-uzbekistane-za-god-soversheno-svyshe-12-mln-kiberatak
10. https://victim-support.eu/help-for-victims/info-on-specific-types-of.victims
11. https://ru.euronews.com/my-europe/2025/08/21/europe-in-motion-scybersecurity
12. https://cyberleninka.ru/article/n/manipulyatsiya-emotsionalnoy-bezopasnostyu-kibermoshennikami-s-primeneniem-tehnologiy-sotsialnoy-inzhenerii-case-study/viewer
13. O‘zbekiston Respublikasining 2003-yil 11-dekabrdagi “Axborotlashtirish to‘g‘risida”gi 560-II-sonli qonuni.
14. O‘zbekiston Respublikasining 2022-yil 15-fevraldagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-qonuni.
15. O‘zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi “Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida”gi PQ-153-son qarori
16. Sh.A. Qobilov. Kiberjinoyatlarning iqtisodiy zarari: O‘zbekistonda raqamli firibgarliklarning oqibatlari va ularni kamaytirish yo‘llari
17. Vol.3 №5 (2025). May. Journal of Effective Learning and Sustainable Innovation
18. https://www.cbr.ru/statistics/information_security/cyber_portrait/2024/
19. https://siat.stat.uz/