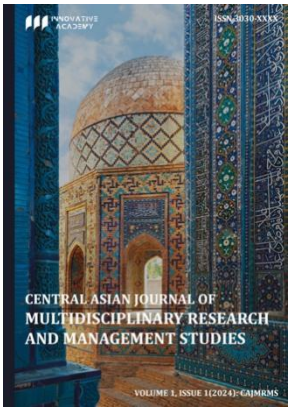

RAQAMLI DUNYODA VIRTUAL FIRIBGARLIKDAN HIMOYALANISH CHORALARI VA UNGA QARSHI HUQUQIY MEXANIZMLAR

Abdullayeva Barno To'liboyevna

Toshkent davlat yuridik universiteti talabasi

https://doi.org/10.5281/zenodo.21297989

ARTICLE INFO

Received: 1st July 2026
Accepted: 2nd July 2026
Published: 10th July 2026

KEYWORDS

virtual firibgarlik, fishing, account takeover, autentifikatsiya, antivirus, domen, firewall.

ABSTRACT

Bugungi kunda firibgarlikning eng keng tarqalgan turi bu – internet orqali odamlarni aldab, ularning pullarini o'zlashtirish ya'ni "virtual firibgarlik" hisoblanyapti. Mazkur maqolada raqamli texnologiyalarning jadal rivojlanish davrida virtual firibgarlikning tobora ortib borayotgan xavfi va uning oqibatlari ko'rib chiqilgan. Maqolada raqamli muhitda keng tarqalgan firibgarlik turlari – fishing, vishing, onlayn-savdodagi aldovlar va boshqa usullar – tahlil qilinib, ulardan himoyalanishning zamonaviy choralari, jumladan, kiberxavfsizlik vositalari, autentifikatsiya usullari, shaxsiy ma'lumotlarni himoyalash strategiyalari va foydalanuvchilarning raqamli savodxonligini oshirish ahamiyati keng yoritilgan.

Shuningdek, maqolada virtual firibgarlikka qarshi kurashishning milliy va xalqaro darajadagi huquqiy asoslari, va ularni samarali bartaraf etish yo'llari tahlil qilingan. Kiberjinoyatlarga qarshi kurashda xalqaro hamkorlikning o'rni va tajribasi, shuningdek, O'zbekiston Respublikasi qonunchiligida virtual firibgarlik uchun belgilangan javobgarlik masalalari ham o'rganilgan. Yakuniy qismda esa, virtual firibgarlikdan samarali himoyalanish va unga qarshi kurashish bo'yicha kompleks yondashuv zarurligi asoslanib, tegishli taklif va tavsiyalar ishlab chiqilgan.

I. KIRISH

Raqamli texnologiyalarning rivojlangani sayin firibgarlar ham yanada puxta rejalashtirilgan sxemalarni ishlab chiqib, ishonuvchan va sodda odamlarni aldashga harakat qilmoqdalar. Kundan kunga butun dunyo bo'ylab minglab odamlar virtual firibgarlik qurboniga aylanmoqda. Kimdir shaxsiy bank kartasi ma'lumotlarini firibgar elektron pochta yoki ijtimoiy tarmoq profillariga yuborib qo'yishi boshqasi esa yolg'on ma'lumotlar tufayli firibgarlar tuzog'iga tushib qolishi mumkin. Bunday noqonuniy xatti-harakatlar nafaqat odamlarning jiddiy moliyaviy zarar ko'rishiga, balki ularning jismoniy va ruhiy salomatligiga ham jiddiy zarar yetkazishiga olib kelishi mumkin. Axborot texnologiyalarining jadal rivojlanishi va kompyuter texnologiyalarining keng qo'llanilishi axborot sohasida jinoyatlar

sodir etilishiga hamda firibgarlikning yangi turlarining paydo bo‘lishiga zamin yaratmoqda. Bunday jinoyatlarning amalga oshirish usullari esa doimiy ravishda takomillashib bormoqda. Shu sababli har bir internet foydalanuvchisi firibgarlarning hiyla-nayranglariga uchrab qolmaslik uchun internetda keng tarqalgan firibgarlik turlarini bilishi va shaxsiy moliyaviy xavfsizlikning asosiy qoidalariga rioya qilishi zarur.

Statistik ma’lumotlarga ko‘ra, AQShda har kuni o‘rtacha 7123 kishi virtual firibgarlikning qurboniga aylanadi (Online Scam Statistics, 2025). Shuningdek, GreatHorn ma'lumotlariga ko'ra, korxona tashkilotlarning 57 foizi har hafta yoki har kuni fishing firibgarligiga duch keladi. Barcha yuborilgan elektron pochta xabarlarining deyarli 1,2 foizi zararli bo'lib, har kuni 3,4 milliard fishing xatlarini tashkil qiladi. Bu raqamlar kiberxavfsizlik muammolarining dolzarbligini ko‘rsatib, kiberjinoyatchilikka qarshi kurashni kuchaytirish zarurligini tasdiqlaydi. Shu sababli ushbu maqolada aynan onlayn firibgarlikning keng tarqalgan turlari, ularga qarshi himoya vositalari hamda virtual firibgarlikka qarshi huquqiy mexanizmlarni tahlil qilishga e’tibor qaratiladi. Shuningdek, odamlarning kibersavodxonligini oshirish bo‘yicha turli manbalarga asoslangan tavsiyalar ham beriladi.

II. ADABIYOTLAR TAHLILI VA METODLAR

Kundalik hayotimizda kiberxavfsizlik, internet xavfsizligi kabi so’zlarni ko’p marotaba eshitamiz. Xo’sh, kiberxavfsizlik o’zi nima?

Kiberxavfsizlik – bu kompyuter tizimlari, tarmoqlar va ma’lumotlarni ruxsatsiz kirishdan, foydalanishdan, oshkor qilishdan, buzilishdan, o’zgartirishdan yoki yo’q qilishdan himoya qilish amaliyoti. U nafaqat biznes va davlat tashkilotlari uchun, balki har bir inson uchun ham dolzarb masaladir (Islombek Abdixakimov, 2025).

Virtual firibgarlik – bu raqamli texnologiyalar va internet tarmoqlari orqali amalga oshiriladigan, aldov yo‘li bilan internet foydalanuvchilarning shaxsiy ma’lumotlarini pullarini yoki boshqa shunga o’xshash zarur ma’lumotlarini qo‘lga kiritishga qaratilgan noqonuniy harakatlarni o‘z ichiga oladigan kiberjinoyat shaklidir (Kaspersky, 2024). Ushbu tushuncha odatda internet, turli xil ijtimoiy tarmoqlar, yoki elektron pochta orqali amalga oshiriladigan kiberjinoyatchilik faoliyatini qamrab oladi. Jumladan, shaxsiy ma’lumotlarni o‘g‘irlash, fishing hamda moliyaviy manfaat olish maqsadida amalga oshiriladigan turli xakerlik usullari ham shular jumlasidandir.

Onlayn xizmatlar vositasida jabrlanuvchilarni nishonga oluvchi internet firibgarlari yildan-yilga o‘sib, har yili millionlab dollar miqdoridagi yo‘qotishlarga sabab bo‘lmoqda. Internetdan foydalanishning kengayishi va kiberjinoyatchilik texnikalarining yanada takomillashishi ushbu xavflarni yanada oshirib, global miqyosda jiddiy tahdidga aylantirmoqda. Shu sababli quyida onlayn firibgarlikning eng keng tarqalgan turlarini tahlil qilamiz.

1. Fishing – bu elektron pochta, matnli xabarlar, telefon qo‘ng‘iroqlari va boshqa aloqa kanallari orqali amalga oshiriladigan, shaxslarni aldashga qaratilgan eng keng tarqalgan kiberhujumlardan biridir (Proofpoint, 2025). Ushbu hujumning asosiy maqsadi – internet foydalanuvchisini moliyaviy ma’lumotlar, tizimga kirish identifikatorlari yoki boshqa maxfiy ma’lumotlarni oshkor qilishga majburlashdir. Fishing hujumlari ko‘pincha foydalanuvchini ishonchli manba sifatida ko‘rsatilgan soxta veb-saytlarga yo‘naltirish yoki zararli fayllarni yuklab olishga undash orqali amalga oshiriladi. Axborot manipulyatsiyasining eng keng tarqalgan shakllaridan biri bo‘lgan fishing, insonni chalg‘itish va aldash maqsadida psixologik ta’sir o‘tkazish hamda turli yolg‘on axborot tarqatish usullaridan foydalanadi. Tajovuzkorlar o‘zlarini ishonchli tashkilot vakillari, masalan, bank xodimlari, davlat organi xodimlari yoki yirik IT kompaniyalari vakili sifatida ko‘rsatib, jabrlanuvchilardan maxfiy ma’lumotlarni oshkor qilishni talab qiladi. Ko‘pincha bunday hujumlar quyidagilarni o‘z ichiga oladi:

Soxta veb – saytlarga yo‘naltiruvchi havolalarni bosishga undash;

Zararli (apk) fayllarni yuklab olish va o‘rnatishga majburlash;

Bank hisob raqamlari, shaxsiy kredit karta ma’lumotlari yoki tizimga kirish identifikatorlarini oshkor qilish (Proofpoint, 2025).

Firibgarlarning aniq maqsadlari turlicha bo‘lishi mumkin, biroq ularning umumiy niyati – shaxsiy ma’lumotlar yoki tizimga kirish ma’lumotlarini o‘g‘irlashdan iborat. Fishing hujumlari odatda shoshilinchlik hissini uyg‘otish orqali maqsadga erishadi. Masalan, foydalanuvchiga hisobining bloklanishi, moliyaviy yo‘qotish xavfi yoki ish joyidan ayrilish ehtimoli haqida xabar yuboriladi. Bunday vaziyatda jabrlanuvchilar firibgarning talablarini bajarishga shoshilishadi va ma’lumotlarning haqiqiyligini tekshirishga vaqt ajratmaydi.

Fishing hujumlari doimiy ravishda takomillashib, xavfsizlik tizimlarini va inson omiliga asoslangan tekshiruv mexanizmlarini chetlab o‘tish yo‘llarini izlaydi. Shu sababli, tashkilotlar o‘z xodimlarini doimiy ravishda eng so‘nggi fishing usullarini aniqlash va ularga qarshi choralar ko‘rishga o‘rgatishlari zarur. Katta miqyosdagi ma’lumotlar buzilishiga sabab bo‘lish uchun atigi bitta xodimning fishingga tushishi kifoya hisoblanadi. Shu bois, fishing kiberxavfsizlikka tahdid soluvchi eng xavfli va murakkab hujum turlaridan biri hisoblanadi, chunki u faqat texnik himoya choralariga emas, balki inson omiliga asoslangan hushyorlikka ham tayanadi. Bugungi kunda fishingning 15 ga yaqin turi mavjud bo‘lib, ular orasida elektron pochta fishingi (email phishing), vishing (telefon orqali fishing), smishing (SMS orqali fishing), Wi-Fi fishing, angler fishing va boshqa turdagi zamonaviy usullar mavjud hisoblanadi (Proofpoint, 2025). Ushbu usullar turli xildagi platformalar va texnologiyalardan foydalangan holda amalga oshirilsa ham, ularning asosiy maqsadi o‘zgarmaydi ya’ni odamlarni aldash yo‘li bilan shaxsiy ma’lumotlarini qo‘lga kiritish, moliyaviy manfaat ko‘rish va tizimlarga ruxsatsiz kirishdir.

Statistik ma’lumotlarga qaraganda Google har kuni 100 millionga yaqin fishing xabarlarini bloklaydi, bu esa muammoning qanchalik keng tarqalganini ko‘rsatadi. Fishing hujumlari ko‘plab sohalarga jiddiy ta’sir ko‘rsatmoqda. 2022 - yilda butun dunyo bo‘ylab yuborilgan elektron xabarlarning 48,63 foizi spam bo‘lgani qayd etilgan. Xususan, bu turdagi hujumlar ko‘pincha mashhur brendlar nomidan amalga oshiriladi. Masalan, 2022- yilning birinchi choragida eng ko‘p taqlid qilingan brend LinkedIn bo‘lib, fishing hujumlarining 52 foizi aynan ushbu platformaga qaratilgan. Shuningdek, DHL (14%), Google (7%), Microsoft (6%) va FedEx (6%) ham firibgarlar tomonidan ko‘p qo‘llangan (AAG IT Support, 2025) .

Fishing hujumlari global miqyosda turli davlatlarga ham katta zarar yetkazmoqda. 2021-yilda spam xabarlarning katta qismi Rossiya (24,77%), Germaniya (14,12%), AQSh (10,46%) va Xitoy (8,73%) kabi davlatlardan kelib chiqqan. Ayniqsa, moliya sektori, energetika sohasi va chakana savdo kompaniyalari fishingning asosiy nishoniga aylangan. 2021-yilda moliya sohasidagi kiberhujumlarning 46 foizi fishing bilan bog‘liq bo‘lsa, energetika sohasida bu ko‘rsatkich 60 foizni tashkil etgan. Bundan tashqari, fishing hujumlari muayyan yosh guruhlariga ham ta’sir ko‘rsatmoqda. Tadqiqotlarga ko‘ra, Millennials va Gen-Z (18-40 yosh) internet foydalanuvchilari fishing hujumlariga uchrash ehtimoli yuqori (23%), bu esa X avlod (41-55 yosh) vakillari orasidagi 19 foizlik ko‘rsatkichga nisbatan ancha yuqori.Firibgarlar zamonaviy xabar almashish platformalaridan faol foydalanmoqda: xususan, fishing hujumlarining 90 foizi WhatsApp, 5,04 foizi esa Telegram kabi ijtimoiy tarmoq ilovlalari orqali yuboriladi (AAG IT Support, 2025).

Tinch okeani mintaqalarida fishing hujumlari 2020-2021 yillarda 168 foizga oshgan. Buyuk Britaniyada esa fishing 2022-yilda biznes uchun eng xavfli kiberjinoyatlardan biriga aylangan.

AQShda esa bu turdagi hujumlar natijasida 2021-yilda 2,7 milliard dollar zarar ko‘rilgan (AAG IT Support, 2025) .

Fishing kampaniyalarining samaradorligi ham ortib bormoqda. 2021-yilda bunday xabarlarga bosish darajasi o‘rtacha 17,8 foizni tashkil etgan bo‘lsa, qo‘shimcha telefon qo‘ng‘iroqlari bilan amalga oshirilgan fishing hujumlarining samaradorligi 53,2 foizga yetgan. Bu shuni ko‘rsatadiki, fishing hujumlari yanada murakkablashib, an’anaviy himoya vositalarini chetlab o‘tish yo‘llarini topmoqda (AAG IT Support, 2025) .

Shuningdek, har oyda o‘rtacha 1,4 million yangi fishing saytlari yaratilayotgani ham muammoning dolzarbligini tasdiqlaydi. Raqamli xavfsizlik bo‘yicha yetarlicha bilimga ega bo‘lmagan internet foydalanuvchilari ushbu tahdidlar oldida zaif bo‘lib qolmoqda. Aynan shuning uchun ham kiberxavfsizlik bo‘yicha doimiy ravishda o‘quv dasturlari, xabardorlik kampaniyalari va mustahkam himoya choralarini joriy etish bugungi kunda dolzarb vazifalardan biri hisoblanadi.

2. Account Takeover (ATO) – bu virtual firibgarlik turi ham hozirgi kunda eng ommabop hisoblanadi. Account Takeover bu hisob (akkount) ni noqonuniy egallab olish firibgarligi – bu kiberjinoyatchilar tomonidan qonuniy internet foydalanuvchisining hisob qaydnomasini ruxsatsiz egallab olishi va boshqarishi bilan tavsiflanadigan hujum turi hisoblanadi. Ushbu hujum natijasida virtual firibgarlar foydalanuvchilarning bank hisoblari, elektron pochta, ijtimoiy tarmoq profillarini ularning ruxsatisiz egallab olishadi va yomon maqsadlarda foydalanishadi (Kaspersky, 2024). Hisobni noqonuniy egallab olish (ATO) firibgarligida kiberjinoyatchilar uchun turli xil maqsadlarni ko‘zlaydi. Bu hujumlarning asosiy maqsadi foydalanuvchilarning shaxsiy ma’lumotlarini, moliyaviy resurslarini va boshqa muhim ma’lumotlarni qo‘lga kiritishdan iborat. ATO hujumlari orqali jinoyatchilar faqat moliyaviy foyda olishni emas, balki maqsadli shaxs yoki tashkilotning shaxsiy hayoti, biznes faoliyatlari buzilishi shuningdek, shaxsiy obrosiga ham putur yetkazishi mumkin. ATO hujumlarida firibgarlar foydalanuvchining akkountini ruxsatsiz egallab olganidan keyin ulardan quyidagi maqsadlarda foydalanishlari mumkin.

Moliyaviy manfaatlar – hisobni egallab olishning eng keng tarqalgan maqsadlaridan biri – moliyaviy foyda olishdir. Kiberjinoyatchilar o‘g‘irlangan bank hisoblarini yoki moliyaviy xizmatlarga kirish huquqini qo‘lga kiritganidan so‘ng, foydalanuvchining mablag‘larini o‘g‘irlash yoki firibgarlik qilish uchun ishlatishadi. Bunday hujumlar ayniqsa, onlayn bank xizmatlari, to‘lov tizimlari, kredit kartalari va boshqa moliyaviy tizimlar bilan bog‘liq. Hisobni egallash orqali jinoyatchilar shuningdek, firibgarlik yo‘llari orqali investitsiya hisoblarini boshqarish yoki o‘z manfaatlariga ishlatishlari mumkin (Kaspersky, 2024).

Identifikatsiyani o‘g‘irlash va shaxsiy ma’lumotlarni soxtalashtirish – hisobni egallab olishning yana bir maqsadi – foydalanuvchining shaxsiy ma’lumotlarini o‘g‘irlashdir. Kiberjinoyatchilar foydalanuvchining ijtimoiy tarmoq akkauntlariga kirish orqali shaxsiy ma’lumotlar, masalan, tug‘ilgan sana, manzil, telefon raqami, ish joyi va boshqa maxfiy ma’lumotlarga ega bo‘lishadi. Bu ma’lumotlar keyinchalik identifikatsiya o‘g‘irlash yoki soxta shaxsiy profil yaratish uchun ishlatilishi mumkin. Bunday ma’lumotlarni qo‘lga kiritish, shuningdek, boshqa kiberhujumlar va firibgarliklar uchun asos bo‘lishi mumkin (Kaspersky, 2024).

Obro’siga putur yetkazish - kiberjinoyatchilar hisobni egallash orqali shaxsning yoki tashkilotning ijtimoiy tarmoqdagi obrosiga putur yetkazishi mumkin. Misol uchun, ular ijtimoiy tarmoqlarda soxta xabarlar tarqatish, qarshi fikrlarni chiqarish, yoki boshqalarni aldash uchun firibgarlikka aloqador xabarlar yuborishi mumkin. Tashkilotlar uchun bunday

hujumlar ularning jamoatchilikdagi obro'siga salbiy ta'sir ko'rsatishi, mijozlar va biznes sheriklarining ishonchini yo'qotishiga olib kelishi mumkin (Kaspersky, 2024).

Kompaniyalar va tashkilotlarga hujumlar – hisobni egallab olish firibgarligi tashkilotlar va kompaniyalar uchun juda katta xavf tug'diradi. Kiberjinoyatchilar korporativ elektron pochta hisoblarini, ichki tizimlarga kirish huquqini va maxfiy hujjatlar yoki ma'lumotlarni o'g'irlashni maqsad qilishadi. Bunday hujumlar tashkilotlarning katta moliyaviy zarar ko'rishiga, maxfiy ma'lumotlarning oshkor bo'lishi va tijorat sirlarining o'g'irlanishi kabi salbiy oqibatlarga olib kelishi mumkin (Kaspersky, 2024).

3. Elektron tijorat firibgarligi – bu internet orqali xarid qilish jarayonida odamlarni aldashga qaratilgan firibgarlik turlari. Bunday noqoqnuniy harakatlar odatda soxta veb-saytlar, elektron pochta xabarlari yoki ijtimoiy tarmoqlardagi e'lonlar orqali amalga oshiriladi. Firibgarlar odamlarni arzon narxlar, maxsus takliflar yoki mavjud bo'lmagan mahsulotlar bilan jalb qiladi va pulni olgandan so'ng mahsulotni yetkazib bermaydi yoki sifatsiz narsa jo'natadi (Federal Trade Commission, 2023).

Onlayn xarid qilish zamonaviy hayotning ajralmas qismiga aylangan bo'lsa-da, u bilan birga turli xavflar, jumladan, firibgarlik holatlari ham ortib bormoqda. Elektron tijorat firibgarligi – ya'ni internet orqali amalga oshiriladigan aldov sxemalari firibgarlarning soxta saytlar yaratishi, haddan tashqari arzon narxlar taklif etishi yoki shaxsiy ma'lumotlarni o'g'irlashi orqali sodir bo'ladi. Bu kabi firibgarliklar sifatsiz yoki umuman yetkazib berilmaydigan mahsulotlarni sotish, shaxsiy bank kartasi ma'lumotlarini qo'lga kiritish va boshqa noqonuniy usullar orqali amalga oshiriladi.

Bunday xavflardan himoyalanish uchun: birinchi navbatda xarid qilishdan oldin saytning ishonchliligini tekshirish; xavfsiz to'lov usullaridan foydalanish; haddan tashqari arzon yoki shubhali takliflarga ishonmaslik lozim. Bunga bir amaliy misol qiladigan bo'lsak, Kanadaning Toronto shahridan Biancah ismli xaridor TikTok'da ommalashgan go'zallik mahsulotining reklamasi orqali bir saytga kiradi. U mahsulot uchun 75 dollar to'laydi va buyurtma 6 hafta ichida yetkazib berilishi kerak bo'ladi. Ammo 18 hafta o'tsa ham, hech qanday mahsulot kelmaydi. Keyinchalik u firibgarlikka uchraganini tushunadi. Agar u xariddan avval saytning rasmiyligini tekshirganida, bunday yo'qotishlarning oldini olishi mumkin edi (BBB Scam Tracker, 2024).

Yuqorida onlayn firibgarlikning eng keng tarqalgan turlari atroflicha misollar va statistik ma'lumotlar asosida tahlil qilindi. Jumladan, fishing, hisobni egallab olish, moliyaviy firibgarlik soxta onlayn savdo platformalari orqali amalga oshiriladigan onlayn tijorat jinoyatlari hozirgi raqamli muhitda eng dolzarb xavflardan biri sifatida e'tirof etiladi. Ushbu firibgarlik sxemalarining asosiy xususiyati shundaki, ular foydalanuvchilarning ishonchidan aql bovar qilmaydigan darajada mohirona usullardan foydalanib, ularni aldash yo'li bilan shaxsiy yoki moliyaviy ma'lumotlarini qo'lga kiritishga qaratilgan. Bunday noqonuniy faoliyat nafaqat iqtisodiy zarar keltiradi, balki raqamli ekotizimga bo'lgan ishonchni pasaytirib, jamiyatda kiberxavfsizlik muammolarini chuqurlashtiradi.

III. NATIJALAR

Texnologiyalar jadal rivojlanib borayotgan hozirgi zamonda shaxsiy ma'lumotlarni himoya qilish dolzarb masalalardan biriga aylangan. Shaxsiy ma'lumotlar deganda- shaxsning ism-sharifi, manzili, telefon raqami, elektron pochta manzili, moliyaviy ma'lumotlari, pasport ma'lumotlari va biometrik identifikatorlari kabi shaxsga doir barcha ma'lumotlar tushuniladi. Ushbu ma'lumotlar kiberjinoyatchilar uchun juda yuqori qimmatga ega bo'lib, ular firibgarlik, shaxsiy ma'lumotlarni noqonuniy ishlatish, identifikatsiyani o'g'irlash yoki boshqa jinoyatlar uchun foydalanilishi mumkin. Global statistikaga qaraydigan bo'lsak, 2023-yilda dunyo

bo‘ylab ma’lumotlar o‘g‘irlanishi bilan bog‘liq zarar 8 milliard AQSh dollaridan oshgan (Statista, 2023). 2023-yilda AQShda 1,1 milliondan ortiq shaxsiy ma’lumotlar o‘g‘irlanishi holatlari qayd etilgan, bu esa 2022-yilga nisbatan 20% ga ko‘pdir (FTC, 2023). 2023-yilda GDPR (Umumiy ma’lumotlarni himoya qilish reglamenti) qoidalarini buzganlik uchun 1,5 milliard yevrodan ortiq jarima undirilgan, bu esa kompaniyalarning ma’lumotlarni himoya qilishga jiddiy yondashishini ko‘rsatadi (GDPR Enforcement Data, 2023). Xo'sh, bu kabi firibgarlarga aldanib qolmaslik uchun internet foydalanuvchilari shaxsiy ma’lumotlarini qanday usullar orqali himoya qilishi mumkin?

Kuchli parollardan foydalanish - Shaxsiy ma’lumotlarni himoya qilishning eng muhim jihatlaridan biri kuchli va murakkab parollardan foydalanishdir. Parollar kamida 12 ta belgidan iborat bo‘lib, harflar, raqamlar va maxsus belgilarning kombinatsiyasidan tashkil topishi lozim. Bundan tashqari, iloji boricha har bir onlayn hisob uchun alohida paroldan foydalanish zarur, chunki bir xil parolni bir nechta platformalarda ishlatish foydalanuvchini bir nechta kiberhujumlar xavfiga duchor qilib qo’yishi mumkin. Har bir platforma uchun alohida va noyob parol yaratish, foydalanuvchining onlayn xavfsizligini maksimal darajada ta’minlaydi (Dr. Jeetendra Pande, 2017).

Ikki faktorli autentifikatsiyani yoqish - zamonaviy kiberxavfsizlikning eng samarali choralardan biri ikki faktorli autentifikatsiya (2FA) tizimidan foydalanishdir. Ushbu mexanizm foydalanuvchi hisoblariga ruxsatsiz kirishning oldini olish uchun qo‘shimcha xavfsizlik qatlamini ta’minlaydi. Ikki faktorli autentifikatsiya foydalanuvchini tekshirish uchun ikki xil tasdiqlash omilidan foydalanadi. Bu omillar bilgan ma’lumot (parol yoki PIN-kod), egalik qilinadigan narsa (maxsus tasdiqlash kodi yuboriladigan mobil telefon yoki autentifikatsiya dasturi) va biometrik omil (barmoq izi, yuzni tanish yoki ovoz orqali autentifikatsiya qilish) kabi elementlardan iborat. Ikki faktorli autentifikatsiya kiberhujumlar xavfini kamaytiradi, fishing hujumlariga qarshi samarali himoya vositasi bo‘lib xizmat qiladi va ko‘plab platformalarda qo‘llaniladi. Bugungi kunda bank tizimlari, elektron pochta xizmatlari, ijtimoiy tarmoqlar va bulutli saqlash xizmatlari ushbu texnologiyani qo‘llab-quvvatlaydi. Shuningdek, avtomatlashtirilgan hujumlarga qarshi samarali vosita sifatida ham 2FA muhim ahamiyat kasb etadi (Dr. Jeetendra Pande, 2017).

Shubhali havolalar va xabarlar bilan ehtiyot bo‘lish - Kiberjinoyatchilar foydalanuvchilarning shaxsiy ma’lumotlarini qo‘lga kiritish uchun turli xil aldov usullaridan foydalanadilar. Eng keng tarqalgan usullardan biri fishing bo‘lib, bu firibgarlar tomonidan yuboriladigan soxta havolalar va xabarlar orqali ma’lumot o‘g‘irlash texnikasidir. Fishing xabarlari odatda rasmiy tashkilot yoki xizmat ko‘rsatuvchi kompaniya nomidan yuboriladi va foydalanuvchini maxsus havolaga kirishga undaydi. Bunday holatlarning oldini olish uchun noma’lum manbalardan kelgan havolalarni bosmaslik, rasmiy manbalardan kelgan xabarlarning haqiqiyligini tekshirish, elektron pochta va ijtimoiy tarmoqlarda maxsus dasturlar yordamida phishing xabarlarini aniqlash zarur. Agar shubhali xabar yoki havola kelib tushsa, uni zudlik bilan tegishli xavfsizlik organlariga yoki xizmat ko‘rsatuvchi kompaniyalarga xabar qilish lozim. Ushbu ehtiyot choralari kiberjinoyatchilarning firibgarlik sxemalariga tushib qolish xavfini sezilarli darajada kamaytiradi (Dr. Jeetendra Pande, 2017).

Shaxsiy ma’lumotlarni cheklangan doirada almashish - Ijtimoiy tarmoqlarda va boshqa onlayn platformalarda ortiqcha shaxsiy ma’lumotlarni oshkor qilishdan tiyilish kerak. Kim bilan qanday ma’lumot almashayotganingizni diqqat bilan kuzatish zarur. Ishonchli antivirus dasturlari va xavfsizlik devorlari (firewall) kompyuter va mobil qurilmalarning zararli dasturlardan himoya qilishiga yordam beradi. Bunday dasturlar muntazam yangilanishi lozimdir (Dr. Jeetendra Pande, 2017).

Jamoat Wi-Fi tarmoqlaridan ehtiyotkorlik bilan foydalanish - Ochiq Wi-Fi tarmoqlari kiberjinoyatchilar uchun ma’lumotlarni kuzatish va o‘g‘irlashning eng qulay vositalaridan biridir. Bunday tarmoqlarda uzatiladigan ma’lumotlar odatda shifrlanmagan bo‘lib, ular maxsus dasturlar yordamida osonlikcha qo‘lga kiritilishi mumkin. Agar bunday tarmoqlardan foydalanishga to‘g‘ri kelsa, VPN (virtual xususiy tarmoq) texnologiyasidan foydalanish tavsiya etiladi. VPN internet ulanishni shifrlaydi va foydalanuvchining haqiqiy manzilini yashirishga yordam beradi, bu esa kiberjinoyatchilarning ma’lumotlarni o‘g‘irlash ehtimolini sezilarli darajada kamaytiradi. Bundan tashqari, shaxsiy yoki moliyaviy ma’lumotlarni kiritish zarur bo‘lsa, faqat ishonchli va xavfsiz tarmoqlardan foydalanish tavsiya etiladi (Dr. Jeetendra Pande, 2020).

Yuqorida virtual firibgarlarga qarshi shaxsiy ma’lumotlarni himoya qilishning eng muhim va samarali usullari tahlil qilindi, shaxsiy ma’lumotlarni himoya qilish nafaqat texnik choralarni ko‘rishni, balki ongli va ehtiyotkorlik bilan harakat qilishni ham talab etadi. Internetda xavfsiz harakat qilish, shaxsiy ma’lumotlarni himoya qilish usullarini bilish va ularga rioya qilish har bir insonning o‘z xavfsizligi uchun hisoblanadi. Bugungi kunda texnologiyalar jadal rivojlanar ekan, raqamli makonda xavfsizlikka bo‘lgan talab ham ortib bormoqda. Shu sababli har bir inson o‘z shaxsiy ma’lumotlarini muhofaza qilish yo‘llarini chuqur o‘rganishi va amalda qo‘llashi lozim.

IV. MUHOKAMA

Hozirgi kunda internet texnologiyalarining jadal rivojlanishi bilan bir qatorda, ushbu sohadagi munosabatlarni huquqiy jihatdan tartibga solish choralari ham izchil ravishda amalga oshirilmoqda. Virtual munosabatlarni huquqiy tarafdan tahlil qilish va tartibga solish hozirgi kunda murakkab va dolzarb masalalardan biri hisoblanadi. Chunki, internet tarmog‘ida «ism» tushunchasi mavjud emas. Tarmoqda subyektni identifikatsiya qilish uning sayti, serveri, domeni orqali amalga oshiriladi. Domen deganda Internet xalqaro kompyuter tarmog‘ining domenlar zonasida jismoniy yoki yuridik shaxslarga tegishli bo‘lgan axborot resurslarini individuallashtirish uchun xizmat qiladigan shartli belgi tushuniladi. Domen subyekt, uning huquqiy xususiyatlari – muomala layoqati va huquq layoqati haqida biron-bir tasavvur hosil qilish imkonini bermaydi. Subyekt bitim tarafining domeni va loginidan iborat saytni nomlar (kompyuter displeyida ifodalar) ekan, uning huquq subyekti sifatidagi maqomi va domen ro‘yxatga olingan mamlakat haqida ham, domen va login egasi kimligi – jismoniy yoki yuridik shaxs ekanligi haqida ham bilishi mumkin emas, chunki, biz qayd etib o‘tganimizdek, login muayyan abbreviatura sifatida ifodalanishi mumkin (G.Gulyamov, I.Rustambekov, 2020). Virtual firibgarlikka qarshi kurashishning huquqiy mexanizmlari, shu jumladan milliy va xalqaro darajadagi asoslar, hozirgi kunda kiberjinoyatchilikka qarshi samarali ta'sir ko'rsatishda ham muhim rol o'ynamoqda. Bu mexanizmlar, firibgarlik va boshqa kiberjinoyatlarga qarshi kurashish uchun huquqiy asoslar yaratib, davlatlar va xalqaro tashkilotlar o'rtasidagi hamkorlikni rivojlantirishga yordam beradi. Avvalo, “kiberjinoyatchilik” tushunchasiga ta’rif beradigan bo’lsak, kiberjinoyatchilik – bu 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‘indisi (R.R.Shakurov, M.M.Vohidov, 2022). Virtual firibgarlikka qarshi kurashishning milliy va xalqaro darajadagi huquqiy asoslari haqida batafsil to'xtalib o’tadigan bo’lsak,

Milliy darajadagi huquqiy asoslar

O'zbekiston Respublikasida virtual firibgarlikka qarshi kurashish uchun bir qator huquqiy va normativ hujjatlar mavjud. Ushbu huquqiy asoslar kiberjinoyatchilikka qarshi kurashish,

firibgarliklarni oldini olish va kiberjinoyatchilikka qarshi samarali choralarni ko'rishni ta'minlaydi.

Birinchisi bu Jinoyat Kodeksi - jinoyat kodeksida kiberjinoyatlar, jumladan, firibgarlik, axborot texnologiyalari (kompyuterlar) dan qonunga xilof ravishda foydalanish, ma'lumotlarni noqonuniy o'zgartirish yoki o'g'irlash kabi jinoyatlar uchun jazolar belgilangan. Jinoyat kodeksining tegishli moddalarida bu turdagi jinoyatlarga qarshi tegishli javobgarlik belgilab qo'yilgan. Jumladan Jinoyat kodeksining 168-moddasida "Firibgarlik" jinoyatiga tegishli javobgarlik belgilangan. Shuningdek, "Axborot texnologiyalari sohasidagi qoidalarni buzish" degan alohida bob mavjud bo'lib ushbu bobda axborot texnologiyalaridan foydalanish bilan bog'liq jinoyatlar va ularga nisbatan qo'llaniladigan javobgarlik choralari belgilangan.

Shaxsga doir ma'lumotlar to'g'risidagi qonun (O'RQ-547-son) - Shaxsga doir ma'lumotlar to'g'risidagi qonunning asosiy vazifasi shaxsiy ma'lumotlar o'zi nima ekanligi aniqlashdan boshlanadi. Qonun qanday ma'lumotlar shaxsiy hisoblanishini belgilab, ularni yig'ish, qayta ishlash, saqlash va foydalanish tartibini tartibga soladi. Shuningdek, shaxsiy ma'lumotlarni qayta ishlashning qonuniyligi, ma'lumotlarni yig'ish va qayta ishlashning adolatli va shaffof bo'lishi, ma'lumotlarning aniqligi kabi muhim tamoyillar fuqarolarning shaxsga doir ma'lumotlarini himoya qilishga qaratilgan. Qonun, shuningdek, har bir shaxsga o'zining shaxsiy ma'lumotlari bilan bog'liq bir qator muhim huquqlarni beradi. Bu huquqlar orqali shaxs o'z ma'lumotlari haqida ma'lumot olish, ularni tuzatish yoki o'chirishni talab qilish, shuningdek, ma'lumotlarini qayta ishlashga qarshi chiqish huquqiga ega bo'ladi. Bu esa shaxsning o'z ma'lumotlari ustidan xavfsiz nazoratini ta'minlashga yordam beradi.

Kiberxavfsizlik to'g'risidagi qonun (O'RQ-764-son) - ushbu qonunning maqsadi kibermakonda xavfsizlikni ta'minlash va raqamli tahdidlarga qarshi kurashish hisoblanadi. Uning asosiy vazifasi – shaxs, jamiyat va davlat manfaatlarini kiberxavfsizlikka oid xavflardan himoya qilishdir. Bu jarayonda davlat organlari, tashkilotlar va fuqarolar o'zaro hamkorlikda ishlashi kerak. Qonun kiberxavfsizlikni ta'minlash bo'yicha yagona davlat siyosatini yuritish, kiberhujumlarning oldini olish, ularni aniqlash va oqibatlarini bartaraf etish kabi muhim yo'nalishlarni belgilaydi. Shuningdek, u muhim axborot infratuzilmasi obyektlarini himoya qilish va milliy axborot resurslarining xavfsizligini ta'minlash vazifalarini ham o'z ichiga oladi. Qonunga ko'ra, kiberxavfsizlik subyektlari sertifikatlangan dasturiy ta'minotlardan foydalanishi, ma'lumotlarni muntazam zaxiralashi va kiberhodisalar haqida vakolatli organlarga xabar berishi shart. Shuningdek, xalqaro kiberjinoyatchilikka qarshi kurashda hamkorlikni rivojlantirish va mahalliy IT ishlab chiqaruvchilarni qo'llab-quvvatlash orqali milliy kiberxavfsizlik imkoniyatlarini mustahkamlashga alohida e'tibor qaratiladi.

Axborotlashtirish to'g'risidagi qonun (O'RQ-560-II-son) - Ushbu qonun axborotlashtirish jarayonlarini tartibga solish va raqamli rivojlanishni ta'minlashga qaratilgan. Uning asosiy maqsadi – shaxslar, jamiyat va davlatning axborotga bo'lgan ehtiyojlarini qondirish, axborot resurslari, texnologiyalari va tizimlaridan samarali foydalanishni tashkil etishdi. Qonun axborot resurslaridan foydalanishda shaffoflik va qonuniylikni ta'minlash, shaxsiy ma'lumotlarni himoya qilish hamda axborot xavfsizligini kafolatlash kabi muhim yo'nalishlarga e'tibor qaratadi. U axborotlashtirish subyektlari o'rtasida samarali hamkorlikni yo'lga qo'yish orqali raqamli iqtisodiyot va jamiyatni rivojlantirishga zamin yaratadi.

Xalqaro huquqiy asoslar

Budapesht konvensiyasi - 2001-yil 23-noyabrda qabul qilingan Budapesht konvensiyasi kiberjinoyatchilikka qarshi kurashish bo'yicha birinchi xalqaro shartnoma sifatida tarixga kirgan. Hozirgi kunda 68 dan ortiq davlat ushbu konvensiyaga a'zo hisoblanadi (Council of Europe 2025). Uning asosiy maqsadi a'zo davlatlarni kiberjinoyatlarni kriminalizatsiya

qilishga, ularni tergov qilish uchun protsessual qoidalarni belgilashga va xalqaro hamkorlikni kuchaytirishga jalb qilishdir. Konvensiya kompyuter tizimlariga noqonuniy kirish, ma'lumotlarni o'g'irlash, zararli dasturlarni tarqatish kabi bir qator kiberjinoyatlarni belgilab beradi va ularga qarshi kurashish uchun huquqiy asos ya'ni javobgarlik choralarini yaratadi (R.R.Shakurov, M.M.Vohidov, 2022).

BMTning Kiberjinoyatlarga qarshi konvensiyasi (loyihasi) – Ayni paytda ishlab chiqilayotgan global xalqaro huquqiy hujjat bo‘lib, xalqaro miqyosda kiberjinoyatlarga qarshi kurashni kuchaytirishga qaratilgan. Agar ushbu konvensiya qabul qilinsa, kiberxavfsizlik bo’yicha xalqaro darajadagi eng muhim huquqiy asoslardan biri bo’lib xizmat qiladi. Ushbu konvensiya 2025-yilda Vyetnamning Xanoy shahrida bo‘lib o‘tadigan rasmiy marosimda imzolash uchun ochilishi kutilmoqda. Konvensiyani imzolash – mamlakatning unga qo‘shilish niyatini bildirishi hisoblanadi. Biroq ratifikatsiya yanada muhim bosqich hisoblanadi, unda davlat o‘zining huquqiy majburiyatlarini rasman tasdiqlaydi, ichki qonunchiligini konvensiya talablariga moslashtiradi va tegishli ruxsatlarni oladi. Ushbu konvensiyaning xalqaro huquqiy kuchga ega bo‘lishi uchun kamida 40 ta BMT a’zo davlati uni ratifikatsiya qilishi talab etiladi. 40-davlat tomonidan ratifikatsiya qilingandan so‘ng, konvensiya barcha qo‘shilgan davlatlar uchun huquqiy majburiyatga ega bo‘lishidan oldin yana 90 kun o‘tishi kerak bo‘ladi (United Nations, 2025).

Virtual firibgarlikka qarshi kurashda milliy va xalqaro huquqiy hujjatlar juda muhim rol o‘ynaydi. Davlatlar o‘z qonunlarini mustahkamlab, fuqarolarini himoya qilishga harakat qilsa, xalqaro konvensiyalar esa mamlakatlar o‘rtasida hamkorlikni kuchaytiradi. Biroq, firibgarlik usullari doimiy o‘zgarib borayotganligi sababli, qonunlar ham yangilanib turishi kerak. Eng samarali himoya usuli shuki, qonunlarni kuchaytirish, xalqaro hamkorlikni oshirish va odamlarni xabardor qilishdir. Faqat shu yo‘l bilan internetdagi virtual firibgarlik tahdidlarini kamaytirish mumkindir.

V. XULOSA

Yuqorida virtual firibgarlik va kiberjinoyatlarga qarshi huquqiy mexanizmlarni muhim manbalar asosida tahlil qilganimizdan so‘ng, quyidagi umumiy xulosaga kelishim mumkin: bugungi kunda zamon shiddat bilan rivojlanmoqda. Zamonaviy texnologiyalar, sun’iy intellekt va shunga o‘xshash dasturlarning rivojlanishi, albatta, ijobiydir. Biroq, shu bilan birga, globallashuv davrida har bir internet foydalanuvchisi o‘z shaxsiy ma’lumotlarini himoya qilishga alohida e’tibor berishi lozim. Internetdan xavfsiz foydalanish bo‘yicha yo‘riqnomalarga rioya qilish har bir internet foydalanuvchisining firibgarlardan xavfsiz holda bo’lishini ta’minlaydi. Umuman olganda, har bir shaxs internet savodxonligiga ega bo‘lishi, shaxsiy ma’lumotlarni himoya qilish usullarini yaxshi bilishi va ularni amalda qo‘llay olishi kerak. Internetdagi har qanday ma’lumotga ko‘r-ko‘rona ishonishdan saqlanish kerak, chunki bu yuqorida ta’kidlanganidek xavfli oqibatlarga olib kelishi mumkin. Shuningdek har bir shaxs, kiberxavfsizlik sohasidagi muhim axborot va yangilinglardan xabardor bo’lish bilan bir qatorda, kiberxavfsizlik sohasidagi qonun hujjatlari va huquqiy axborotlar bilan muntazam tanishib, ularga rioya etib borishi zarur.

ADABIYOTLAR RO’YXATI:

1. R.R.Shakurov, M.M.Vohidov. Kiber huquq - huquq sohasi sifatida: risola. Yuristlar malakasini oshirish markazi, 2022.

2. G.Gulyamov, I.Rustambekov. “Kiber-huquq - yangi kompleks huquq sohasi sifatida / O‘zbekiston qonunchiligi tahlili” inLibrary, 2020.

https://inlibrary.uz/index.php/uzbek_law_review/article/view/1876

3. Dr. Jeetendra Pande. “Introduction to Cyber Security” Uttarakhand Open University, Haldwani, 2017.

https://www.uou.ac.in/sites/default/files/slm/Introduction-cyber-security.pdf

4. Abdixakimov Islombek. “Kiberxavfsizlikning kundalik hayotimizdagi ahamiyati va huquqiy jihatlari.” Toshkent davlat yuridik universiteti Elektron kutubxonasi. Accessed April 5, 2025. https://library-tsul.uz/kiberxavfsizlikning-kundalik-hayotimizdagi-ahamiyati-va-huquqiy-jihatlari/.

5. AAG IT. “The Latest Phishing Statistics.” AAG IT Services. Accessed April 4, 2025. https://aag-it.com/the-latest-phishing-statistics/.

6. BBB Marketplace Trust. “Risk Report 2024.” BBB Marketplace Trust. Accessed April 4, 2025. https://bbbmarketplacetrust.org/riskreport2024/.

7. Privacy Journal. “Scam Statistics and Facts.” Privacy Journal. Accessed April 4, 2025. https://www.privacyjournal.net/scam-statistics-and-facts/

8 United Nations. "Basic Facts About the Global Cybercrime Treaty." United Nations. Accessed April 5, 2025. https://www.un.org/en/peace-and-security/basic-facts-about-global-cybercrime-treaty.

9. Statista. "Social Media - Statistics & Facts." Statista. Accessed April 5, 2025. https://www.statista.com/topics/1164/social-networks/.

10. Federal Trade Commission. "Scams." Federal Trade Commission. Accessed April 5, 2025. https://consumer.ftc.gov/scams.

11. CMS.Law. "GDPR Enforcement Tracker." CMS.Law. Accessed April 5, 2025. https://www.enforcementtracker.com/?insights.

12. Proofpoint. "What Is Phishing? - Meaning, Attack Types & More." Proofpoint. Accessed April 5, 2025.

What Is Phishing? - Meaning, Attack Types & More | Proofpoint US

13. Kaspersky. "Online Banking Fraud: How to Keep Your Accounts Secure." Kaspersky Resource Center. Accessed April 5, 2025. https://www.kaspersky.com/resource-center/threats/online-banking-theft.

14. Council of Europe. "Convention on Cybercrime." Council of Europe. Accessed April 5, 2025. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.