KIBERFIRIBGARLIK: ZAMONAVIY TAHDIDLAR VA ULARDAN HIMOYALANISH YO‘LLARI

Husanov Nodirbek Turdimurod o’g’li
O’zbekiston Respublikasi Ichki
ishlar vazirligi Akademiyasi
3-kurs 319-guruh kursanti
https://doi.org/10.5281/zenodo.24438695

Annotatsiya: Ushbu maqolada kiberfiribgarlikning zamonaviy ko‘rinishlari, ularning jamiyat va shaxs hayotiga ta’siri hamda undan himoyalanishning samarali usullari tahlil qilinadi. Xususan, fishing, ijtimoiy muhandislik, zararli dasturlar va soxta onlayn xizmatlar orqali amalga oshiriladigan firibgarlik turlari misollar asosida yoritilgan. Shuningdek, foydalanuvchilarning axborot xavfsizligini ta’minlashda ehtiyotkorlik, texnik vositalardan to‘g‘ri foydalanish va raqamli savodxonlikning ahamiyati ochib beriladi.
Kalit so‘zlar: kiberfiribgarlik, axborot xavfsizligi, fishing, ijtimoiy muhandislik, zararli dasturlar, onlayn firibgarlik, shaxsiy ma’lumotlar himoyasi, raqamli xavfsizlik, internet tahdidlari, kiberxavfsizlik.

Annotation: This article examines modern forms of cyber fraud, their impact on individuals and society, and effective methods of protection against them. In particular, it highlights types of fraud such as phishing, social engineering, malware, and fake online services with illustrative examples. The article also emphasizes the importance of digital literacy, cautious behavior, and the proper use of technological tools in ensuring information security.
Keywords: cyber fraud, information security, phishing, social engineering, malware, online fraud, personal data protection, digital security, internet threats, cybersecurity.

Аннотация: В данной статье рассматриваются современные формы кибермошенничества, их влияние на личность и общество, а также эффективные способы защиты от них. В частности, освещаются такие виды мошенничества, как фишинг, социальная инженерия, вредоносные программы и поддельные онлайн-сервисы на основе практических примеров. Также подчеркивается важность цифровой грамотности, осторожности пользователей и правильного использования технологий для обеспечения информационной безопасности.
Ключевые слова: кибермошенничество, информационная безопасность, фишинг, социальная инженерия, вредоносные программы, онлайн-мошенничество, защита персональных данных, цифровая безопасность, интернет-угрозы, кибербезопасность.

XXI asr — raqamli texnologiyalar asri sifatida insoniyat taraqqiyotining yangi bosqichini boshlab berdi. Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida global tarmoqlar, sun’iy intellekt, bulutli hisoblash va katta ma’lumotlar (Big Data) kabi innovatsion yechimlar keng qo‘llanilmoqda. Internet tarmog‘ining ommalashuvi esa inson faoliyatining deyarli barcha sohalarini — iqtisodiyot, ta’lim, sog‘liqni saqlash, bank-moliya tizimi va davlat

boshqaruvini tubdan o‘zgartirdi. Bugungi kunda milliardlab foydalanuvchilar kundalik hayotida raqamli xizmatlardan foydalanmoqda, bu esa global axborot makonining kengayishiga xizmat qilmoqda. Shu bilan birga, raqamlashtirish jarayoni yangi turdagi xavf-xatarlarni ham yuzaga keltirmoqda. Axborot xavfsizligi muammolari, ayniqsa, kiberjinoyatchilik va uning tarkibiy qismi bo‘lgan kiberfiribgarlik zamonaviy jamiyatning eng dolzarb muammolaridan biriga aylandi. Kiberfiribgarlik — bu jinoyatchilar tomonidan axborot texnologiyalaridan foydalangan holda moddiy yoki ma’naviy manfaat ko‘rish maqsadida amalga oshiriladigan noqonuniy faoliyat bo‘lib, u global xarakterga ega va chegaralarni tan olmaydi.

Statistik ma’lumotlarga ko‘ra, so‘nggi yillarda kiberjinoyatlar soni keskin oshib bormoqda. Ayniqsa, pandemiya davrida masofaviy ish, onlayn ta’lim va elektron tijorat hajmining ortishi natijasida firibgarlar uchun yangi imkoniyatlar paydo bo‘ldi. Ular foydalanuvchilarning ishonchiga kirish, psixologik ta’sir o‘tkazish va texnik zaifliklardan foydalanish orqali turli xil firibgarlik sxemalarini ishlab chiqmoqda. Bu esa nafaqat alohida shaxslar, balki yirik kompaniyalar va davlat tashkilotlari uchun ham jiddiy xavf tug‘dirmoqda. Zamonaviy kiberfiribgarlikning o‘ziga xos jihati — uning yuqori darajada moslashuvchanligi va tez rivojlanishidir. Masalan, fishing hujumlari yanada murakkablashib, rasmiy tashkilotlarning veb-saytlariga juda o‘xshash sahifalar yaratilmoqda. Ijtimoiy muhandislik usullari esa inson omiliga tayanib, foydalanuvchilarning beparvoligi yoki yetarli bilimga ega emasligidan foydalanadi. Bundan tashqari, zararli dasturlar yordamida qurilmalarga yashirincha kirish, ma’lumotlarni o‘g‘irlash va hatto moliyaviy operatsiyalarni boshqarish kabi holatlar ham keng tarqalmoqda.

Kiberfiribgarlikning yana bir xavfli jihati — uning iqtisodiy va ijtimoiy oqibatlaridir. Moliyaviy yo‘qotishlardan tashqari, ma’lumotlar bazasining buzilishi, shaxsiy axborotlarning oshkor bo‘lishi va tashkilotlar obro‘sining pasayishi kabi salbiy holatlar yuzaga keladi. Bu esa o‘z navbatida jamiyatda raqamli texnologiyalarga nisbatan ishonchning kamayishiga olib kelishi mumkin. Ayniqsa, rivojlanayotgan davlatlarda kiberxavfsizlik infratuzilmasining yetarlicha rivojlanmagani ushbu muammoni yanada keskinlashtiradi. Shu nuqtai nazardan, kiberfiribgarlikka qarshi kurashish kompleks yondashuvni talab etadi. Bu jarayonda nafaqat texnik himoya vositalarini takomillashtirish, balki aholining raqamli savodxonligini oshirish, huquqiy mexanizmlarni kuchaytirish va xalqaro hamkorlikni rivojlantirish muhim ahamiyat kasb etadi. Har bir foydalanuvchi o‘zining axborot xavfsizligi uchun mas’ul ekanligini anglab yetishi va oddiy ehtiyot choralariga amal qilishi zarur.

Mazkur maqolaning maqsadi — kiberfiribgarlikning zamonaviy tahdidlarini keng qamrovda tahlil qilish, uning asosiy turlarini yoritish hamda samarali himoyalanish usullarini ilmiy-amaliy jihatdan asoslab berishdan iborat. Ushbu tadqiqot natijalari foydalanuvchilarning kiberxavfsizlik bo‘yicha bilim va ko‘nikmalarini oshirishga xizmat qiladi.

Kiberfiribgarlik va kiberxavfsizlik muammolari zamonaviy ilmiy tadqiqotlarda eng dolzarb yo‘nalishlardan biri sifatida keng o‘rganilmoqda. Raqamli iqtisodiyotning jadal rivojlanishi, internet foydalanuvchilari sonining keskin ortishi va global axborot makonining kengayishi natijasida kiberjinoyatchilik, xususan, kiberfiribgarlikning ko‘lami va murakkabligi ham ortib bormoqda. Shu bois ushbu sohada olib borilgan ilmiy izlanishlar turli yo‘nalishlarda — texnologik, ijtimoiy, iqtisodiy va huquqiy jihatlar kesimida amalga oshirilmoqda. Xalqaro ilmiy adabiyotlarda kiberfiribgarlik tushunchasi ko‘pincha kengroq bo‘lgan kiberjinoyatchilik doirasida tahlil qilinadi. Tadqiqotchilar kiberfiribgarlikni axborot-kommunikatsiya

texnologiyalaridan foydalangan holda foydalanuvchilarning ishonchini suiiste'mol qilish orqali moddiy yoki ma'naviy manfaat ko'rishga qaratilgan faoliyat sifatida ta'riflaydilar. Ko'plab ilmiy ishlarda ushbu hodisaning asosiy xususiyatlari sifatida uning anonimligi, tez moslashuvchanligi va transmilliy xarakterga ega ekanligi qayd etiladi. Bu esa kiberfiribgarlikka qarshi kurashishni murakkablashtiruvchi omillar sifatida baholanadi.

Adabiyotlarda alohida e'tibor qaratilgan yo'nalishlardan biri — ijtimoiy muhandislik fenomenidir. Tadqiqotlar shuni ko'rsatadiki, aksariyat kiberfiribgarlik hujumlari texnik zaifliklardan ko'ra inson omiliga asoslanadi. Firibgarlar foydalanuvchilarning psixologik holatiga ta'sir ko'rsatish, ularni chalg'itish yoki shoshilinch qaror qabul qilishga undash orqali maxfiy ma'lumotlarni qo'lga kiritadilar. Ilmiy manbalarda bu jarayonlar insonning ishonuvchanligi, qo'rquv hissi, qiziqishi yoki moddiy manfaatdorligi bilan bog'liq holda tahlil qilinadi. Shu sababli ko'plab tadqiqotchilar kiberxavfsizlikni ta'minlashda inson omilini hisobga olishni ustuvor vazifa sifatida ko'rsatadilar. Fishing (phishing) hujumlari bo'yicha olib borilgan tadqiqotlar ham keng o'rin egallaydi. Ilmiy adabiyotlarda fishing eng samarali va keng tarqalgan kiberfiribgarlik vositalaridan biri sifatida baholanadi. So'nggi yillarda fishing texnikalari sezilarli darajada takomillashib, rasmiy tashkilotlar, banklar va mashhur platformalarning dizayni hamda kommunikatsiya uslubini yuqori aniqlikda taqlid qiluvchi shakllarga o'tgan. Bundan tashqari, smishing (SMS orqali fishing) va vishing (telefon qo'ng'iroqlari orqali fishing) kabi yangi ko'rinishlar ham paydo bo'lib, foydalanuvchilar uchun xavf darajasini yanada oshirmoqda. Tadqiqotlar shuni ko'rsatadiki, foydalanuvchilarning aksariyati bunday hujumlarni aniqlashda qiyinchilikka duch keladi.

Zararli dasturlar (malware) bilan bog'liq ilmiy ishlar ham kiberfiribgarlikni o'rganishda muhim o'rin tutadi. Ushbu yo'nalishda olib borilgan tadqiqotlar malware turlarining tasnifi, ularning ishlash mexanizmlari va aniqlash usullariga bag'ishlangan. Xususan, trojanlar, ransomware, spyware va keylogger dasturlarining keng tarqalganligi qayd etiladi. Ransomware hujumlari ayniqsa so'nggi yillarda jiddiy muammoga aylangan bo'lib, ular foydalanuvchi ma'lumotlarini shifrlab, ularni tiklash evaziga to'lov talab qiladi. Ilmiy adabiyotlarda bunday tahdidlarga qarshi kurashish uchun ko'p qatlamli himoya tizimlari, doimiy yangilanishlar va xavfsizlik siyosatini takomillashtirish zarurligi ta'kidlanadi. Kiberfiribgarlikning iqtisodiy oqibatlari ham ko'plab tadqiqotlarda chuqur tahlil qilingan. Xalqaro tashkilotlar va tadqiqot markazlari tomonidan e'lon qilingan ma'lumotlarga ko'ra, kiberjinoyatlar global iqtisodiyotga har yili milliardlab dollar zarar yetkazmoqda. Bu zarar bevosita moliyaviy yo'qotishlar bilan cheklanib qolmay, balki kompaniyalar obro'sining pasayishi, mijozlar ishonchining yo'qolishi va biznes jarayonlarining izdan chiqishi kabi bilvosita oqibatlarni ham o'z ichiga oladi. Shu nuqtai nazardan, ilmiy ishlarda kiberxavfsizlikka kiritilayotgan investitsiyalarni oshirish zarurligi asoslab berilgan.

Huquqiy jihatdan olib borilgan tadqiqotlar esa kiberfiribgarlikka qarshi kurashishda qonunchilik bazasining ahamiyatini ochib beradi. Ko'plab davlatlarda kiberjinoyatlarga qarshi maxsus qonunlar qabul qilingan bo'lsa-da, ularning samaradorligi ko'pincha xalqaro hamkorlik darajasiga bog'liq ekanligi ta'kidlanadi. Chunki kiberjinoyatchilik chegaralarni tan olmaydi va ko'pincha bir nechta davlat hududida amalga oshiriladi. Shu sababli xalqaro konvensiyalar, hamkorlik dasturlari va axborot almashinuvi mexanizmlarini rivojlantirish muhim ahamiyat kasb etadi. Mahalliy va mintaqaviy tadqiqotlarda esa kiberxavfsizlikning ijtimoiy jihatlari, xususan, aholining raqamli savodxonligi darajasi asosiy e'tibor markazida turadi. Tadqiqotlar

shuni ko‘rsatadiki, ko‘plab foydalanuvchilar oddiy xavfsizlik qoidalariga amal qilmasligi sababli kiberfiribgarlik qurboniga aylanmoqda. Shu bois ta’lim tizimida kiberxavfsizlik asoslarini o‘qitish, ommaviy axborot vositalari orqali targ‘ibot ishlarini kuchaytirish va profilaktik choralarni kengaytirish zarurligi qayd etiladi.

So‘nggi yillarda ilmiy adabiyotlarda sun’iy intellekt va mashinaviy o‘rganish texnologiyalaridan foydalangan holda kiberfiribgarlikni aniqlash va oldini olish masalalari ham keng o‘rganilmoqda. Tadqiqotlar ushbu texnologiyalar yordamida shubhali faoliyatni avtomatik aniqlash, anomaliyalarni tahlil qilish va real vaqt rejimida tahdidlarga javob qaytarish imkoniyati mavjudligini ko‘rsatmoqda. Biroq, ayrim tadqiqotchilar sun’iy intellektning o‘zi ham firibgarlar tomonidan suiiste’mol qilinishi mumkinligini ta’kidlab, bu borada ehtiyotkorlik zarurligini qayd etadilar.

Umuman olganda, mavjud ilmiy adabiyotlar tahlili shuni ko‘rsatadiki, kiberfiribgarlik murakkab, ko‘p qatlamli va dinamik rivojlanayotgan hodisa hisoblanadi. Uni samarali oldini olish uchun texnologik yechimlar, inson omili, huquqiy mexanizmlar va xalqaro hamkorlikni o‘z ichiga olgan kompleks yondashuv zarur. Shu bilan birga, tadqiqotlar kiberxavfsizlik sohasida doimiy ravishda yangi yondashuvlar va innovatsion usullar ishlab chiqish muhimligini ko‘rsatmoqda.

Ushbu ilmiy maqolada kiberfiribgarlik muammosini har tomonlama o‘rganish maqsadida kompleks metodologik yondashuv qo‘llanildi. Tadqiqotning asosiy vazifasi zamonaviy kiberfiribgarlikning shakllari, ularning ishlash mexanizmlari, tarqalish sabablari hamda ularga qarshi samarali himoya choralarini aniqlashdan iborat bo‘lib, ushbu jarayonda bir nechta ilmiy tadqiqot usullaridan foydalanildi. Avvalo, **nazariy tahlil metodi** asosiy o‘rin egalladi. Ushbu metod orqali kiberfiribgarlik tushunchasining ilmiy ta’rifi, uning kiberjinoyatchilik tizimidagi o‘rni, rivojlanish bosqichlari hamda zamonaviy transformatsiyasi o‘rganildi. Turli ilmiy monografiyalar, maqolalar, xalqaro tashkilotlar (masalan, IT xavfsizlik bo‘yicha hisobotlar) va kiberxavfsizlikka oid rasmiy manbalar chuqur tahlil qilindi. Nazariy tahlil natijasida kiberfiribgarlikning nafaqat texnik, balki ijtimoiy-psixologik hodisa ekanligi ham aniqlashtirildi. Ikkinchi muhim yondashuv sifatida **qiyosiy tahlil metodi** qo‘llanildi. Ushbu metod yordamida kiberfiribgarlikning asosiy turlari — fishing, smishing, vishing, ijtimoiy muhandislik hujumlari, zararli dasturlar (malware) va soxta onlayn platformalar o‘zaro solishtirildi. Har bir firibgarlik turining ishlash prinsipi, maqsadli auditoriyasi, texnik murakkabligi va zarar darajasi tahlil qilindi. Qiyosiy tahlil natijasida fishing hujumlari eng keng tarqalgan va eng ko‘p zarar yetkazuvchi usullardan biri ekanligi, ijtimoiy muhandislik esa inson psixologiyasiga asoslangan eng xavfli yondashuvlardan biri sifatida ajralib turishi aniqlangan.

Shuningdek, **tizimli yondashuv metodi** qo‘llanilib, kiberfiribgarlik yagona hodisa sifatida emas, balki o‘zaro bog‘liq komponentlardan iborat murakkab tizim sifatida ko‘rib chiqildi. Bu yondashuv orqali texnologik vositalar, inson omili, huquqiy asoslar va ijtimoiy muhit o‘rtasidagi o‘zaro bog‘liqlik tahlil qilindi. Natijada kiberfiribgarlikning rivojlanishiga faqat texnik zaifliklar emas, balki foydalanuvchilarning raqamli savodxonligi darajasi ham bevosita ta’sir qilishi aniqlandi. Tadqiqotda **umumlashtirish va induksiya metodlari** ham muhim rol o‘ynadi. Turli manbalardan olingan ma’lumotlar asosida kiberfiribgarlikning umumiy xususiyatlari, asosiy tendensiyalari va rivojlanish yo‘nalishlari aniqlanib, yagona ilmiy xulosalar shakllantirildi. Induktiv yondashuv yordamida alohida misollar va hodisalardan umumiy qonuniyatlar chiqarildi. Bundan tashqari, maqolada **sifatli (qualitative) tadqiqot**

yondashuvi ustuvor ahamiyat kasb etdi. Bu yondashuv kiberfiribgarlikning chuqur mazmuniy jihatlarini, ya'ni uning psixologik, ijtimoiy va madaniy omillarini o'rganishga imkon berdi. Foydalanuvchilarning internetdagi xulq-atvori, ularning xavfsizlikka bo'lgan munosabati va raqamli muhitdagi ehtiyotkorlik darajasi tahlil qilindi.

Shu bilan birga, ayrim hollarda **miqdoriy (quantitative) ma'lumotlar** ham inobatga olindi. Xalqaro kiberxavfsizlik tashkilotlari tomonidan e'lon qilingan statistik ma'lumotlar, kiberhujumlar soni, zarar miqdori va foydalanuvchilarning jabrlanish darajasi kabi ko'rsatkichlar tahlil qilindi. Bu esa tadqiqotning empirik asosini mustahkamlashga xizmat qildi. Tadqiqot jarayonida **kontent tahlili metodi** ham qo'llanilib, internet resurslari, ilmiy maqolalar, yangiliklar portallari va kiberxavfsizlik bo'yicha hisobotlar o'rganildi. Ushbu metod yordamida kiberfiribgarlik haqidagi ma'lumotlarning qanday shaklda taqdim etilishi, asosiy muammolar qanday yoritilishi va jamoatchilik fikri qanday shakllanishi tahlil qilindi. Metodologik yondashuvda alohida e'tibor **inson omiliga asoslangan tahlilga** qaratildi. Chunki kiberfiribgarlikning aksariyat holatlari texnik zaifliklardan ko'ra insonlarning psixologik xatolari, ishonuvchanligi va ehtiyotsizligi bilan bog'liq. Shu sababli foydalanuvchilarning raqamli savodxonlik darajasi, xavfsizlik qoidalariga rioya qilish odatlari va ijtimoiy tarmoqlardagi faolligi ham tadqiqot doirasida o'rganildi.

Umuman olganda, qo'llanilgan metodlar kiberfiribgarlikni faqat texnik muammo sifatida emas, balki ko'p qirrali ijtimoiy-texnologik hodisa sifatida tahlil qilish imkonini berdi. Bu esa tadqiqotning ilmiy asoslanganligini oshirib, uning natijalarini amaliy jihatdan qo'llash uchun mustahkam baza yaratdi.

Tadqiqot jarayonida kiberfiribgarlikning zamonaviy holati, uning rivojlanish tendensiyalari, asosiy ko'rinishlari hamda unga ta'sir etuvchi omillar keng qamrovda o'rganildi. Olingan natijalar shuni ko'rsatadiki, kiberfiribgarlik bugungi kunda nafaqat texnik muammo sifatida, balki ijtimoiy, iqtisodiy va psixologik omillar bilan chambarchas bog'liq bo'lgan murakkab global tahdidga aylangan. Raqamli texnologiyalar rivojlanishi bilan birga firibgarlik usullari ham takomillashib, yanada yashirin va murakkab shakllarga o'tib bormoqda. Tahlillar natijasida kiberfiribgarlikning eng keng tarqalgan ko'rinishlari sifatida fishing, smishing, vishing, ijtimoiy muhandislik hujumlari, zararli dasturlar (malware), soxta onlayn do'konlar va investitsion firibgarliklar aniqlangan. Ayniqsa, fishing hujumlari eng ommaviy va xavfli usul sifatida ajralib turadi. Bunday hujumlarda firibgarlar banklar, davlat tashkilotlari yoki mashhur platformalar nomidan soxta xabarlar yuborib, foydalanuvchilarning shaxsiy ma'lumotlarini qo'lga kiritishga harakat qiladilar. So'nggi yillarda ushbu usul yanada takomillashib, rasmiy veb-saytlarning aniq nusxalarini yaratish darajasiga yetgan.

Smishing va vishing kabi mobil firibgarlik turlari ham sezilarli darajada oshgan. Mobil qurilmalar hayotimizning ajralmas qismiga aylangani sababli, firibgarlar SMS va telefon qo'ng'iroqlari orqali foydalanuvchilarni chalg'itishga urinmoqda. Zararli dasturlar esa kompyuter va mobil qurilmalarga yashirin tarzda kirib, ma'lumotlarni o'g'irlash, tizimni bloklash yoki foydalanuvchini to'lov qilishga majbur qilish kabi zararli harakatlarni amalga oshiradi. Tadqiqot natijalari shuni ham ko'rsatadiki, kiberfiribgarlikning asosiy sabablari texnologik emas, balki ko'proq inson omili bilan bog'liq. Foydalanuvchilarning raqamli savodxonligi yetarli darajada emasligi, internet xavfsizligi qoidalariga rioya qilmaslik, shubhali havolalarga ishonish va shaxsiy ma'lumotlarni ehtiyotsiz tarqatish firibgarlik holatlarining

ko‘payishiga sabab bo‘lmoqda. Shuningdek, kuchsiz parollardan foydalanish, ikki bosqichli himoya tizimlarining yo‘qligi ham xavf darajasini oshiradi.

Bundan tashqari, kiberfiribgarlikning rivojlanishiga texnologik taraqqiyot ham katta ta’sir ko‘rsatmoqda. Sun’iy intellekt, mashinaviy o‘rganish va avtomatlashtirilgan tizimlar firibgarlar tomonidan ham qo‘llanilmoqda. Masalan, sun’iy intellekt yordamida yaratilgan soxta ovozlar, deepfake videolar va avtomatik xabar yuborish tizimlari kiberfiribgarlikni yanada murakkab bosqichga olib chiqmoqda. Bu esa an’anaviy xavfsizlik tizimlari uchun yangi chaqiriqlarni yuzaga keltirmoqda. Tadqiqot davomida shuningdek, kiberfiribgarlikning iqtisodiy oqibatlari ham chuqur tahlil qilindi. Natijalarga ko‘ra, kiberjinoyatlar global iqtisodiyotga har yili juda katta miqdorda zarar yetkazmoqda. Bu zarar nafaqat to‘g‘ridan-to‘g‘ri moliyaviy yo‘qotishlar, balki kompaniyalar obro‘sining pasayishi, mijozlar ishonchining yo‘qolishi va biznes jarayonlarining izdan chiqishi kabi bilvosita oqibatlarni ham o‘z ichiga oladi. Ayniqsa, bank-moliya sektori, elektron tijorat va davlat axborot tizimlari eng ko‘p zarar ko‘radigan sohalar sifatida qayd etilgan.

Muhokama jarayonida xorijiy tajribalar ham chuqur tahlil qilindi. Xususan, AQSh, Yevropa Ittifoqi, Buyuk Britaniya, Janubiy Koreya va Singapur kabi davlatlarda kiberfiribgarlikka qarshi kurashish tizimli va kompleks yondashuv asosida olib borilmoqda. AQShda Federal qidiruv byurosi tarkibidagi Internet Crime Complaint Center (IC3) kiberfiribgarlik holatlarini monitoring qiladi va tahlil qiladi. Yevropa Ittifoqida esa ENISA agentligi kiberxavfsizlik bo‘yicha yagona standartlarni ishlab chiqadi va barcha a’zo davlatlar uchun umumiy siyosatni muvofiqlashtiradi. Buyuk Britaniyada National Cyber Security Centre (NCSC) aholiga real vaqt rejimida kiberxavflar haqida ogohlantirishlar berib boradi hamda ta’lim tizimida kiberxavfsizlik fanlarini keng joriy qilgan. Janubiy Koreyada esa yuqori texnologiyali real vaqt monitoring tizimlari va sun’iy intellekt asosidagi xavfsizlik platformalari faol ishlatiladi. Singapurda kiberxavfsizlik davlat siyosatining ustuvor yo‘nalishi sifatida qaralib, aholining raqamli savodxonligini oshirishga alohida e’tibor qaratiladi. Muhokama natijalariga ko‘ra, rivojlangan davlatlarda kiberfiribgarlikka qarshi kurashishda profilaktik yondashuv ustuvor ahamiyatga ega. Ya’ni, ular muammo yuzaga kelgandan keyin emas, balki uning oldini olishga qaratilgan tizimni shakllantirgan. Aksincha, ko‘plab rivojlanayotgan davlatlarda esa reaktiv yondashuv — ya’ni firibgarlik sodir bo‘lgandan keyin chora ko‘rish amaliyoti ustunlik qiladi.

Tadqiqot davomida yana bir muhim xulosa shundan iborat bo‘ldiki, kiberfiribgarlikka qarshi kurashishda faqat texnik himoya vositalari yetarli emas. Antivirus dasturlari, xavfsizlik devorlari va tizim yangilanishlari muhim bo‘lsa-da, eng asosiy himoya omili insonning o‘zi hisoblanadi. Foydalanuvchilarning raqamli madaniyati, ehtiyotkorligi va kiberxavfsizlik bo‘yicha bilim darajasi butun tizimning eng zaif yoki eng kuchli bo‘g‘ini bo‘lishi mumkin. Shuningdek, tahlillar shuni ko‘rsatadiki, ko‘plab foydalanuvchilar kiberxavfsizlik bo‘yicha nazariy bilimga ega bo‘lsa-da, amaliyotda bu qoidalarga to‘liq rioya qilmaydi. Bu esa bilim va amaliy xulq o‘rtasida sezilarli tafovut mavjudligini bildiradi. Shu sababli nafaqat o‘qitish, balki amaliy treninglar, simulyatsion mashg‘ulotlar va real hayotga yaqin holatlar orqali foydalanuvchilarni tayyorlash zarur.

Umuman olganda, tadqiqot natijalari kiberfiribgarlik murakkab, ko‘p qatlamli va doimiy rivojlanib borayotgan global muammo ekanligini tasdiqlaydi. Uni samarali bartaraf etish uchun texnologik innovatsiyalar, kuchli huquqiy baza, xalqaro hamkorlik va aholining raqamli

savodxonligini oshirishga qaratilgan kompleks yondashuv zarur. Faqatgina ushbu omillar uyg‘unlashgan taqdirda kiberfiribgarlik xavfini sezilarli darajada kamaytirish mumkin bo‘ladi.

Tadqiqot natijalari asosida kiberfiribgarlikning oldini olish, uning zararini kamaytirish va jamiyatda raqamli xavfsizlik madaniyatini oshirish bo‘yicha bir qator ilmiy-amaliy takliflar ishlab chiqildi. Ushbu takliflar texnologik, huquqiy, ijtimoiy va ta’limiy yo‘nalishlarni qamrab olgan holda kompleks yondashuvga asoslanadi. Avvalo, eng muhim yo‘nalishlardan biri sifatida aholining **raqamli savodxonligini oshirish** masalasi alohida ta’kidlanadi. Bugungi kunda ko‘plab kiberfiribgarlik holatlari foydalanuvchilarning yetarli bilimga ega emasligi va internet xavfsizligi qoidalarini to‘liq tushunmasligi natijasida sodir bo‘lmoqda. Shu sababli maktabgacha ta’limdan boshlab oliy ta’lim muassasalarigacha bo‘lgan barcha bosqichlarda kiberxavfsizlik asoslarini o‘qitish zarur. O‘quv dasturlariga “Raqamli xavfsizlik asoslari”, “Internetda xavfsiz xulq-atvor”, “Shaxsiy ma’lumotlarni himoya qilish” kabi mavzular kiritilishi maqsadga muvofiq bo‘ladi. Bundan tashqari, aholiga mo‘ljallangan ommaviy axborot kampaniyalarini kuchaytirish ham muhim ahamiyatga ega. Televizor, radio, internet platformalari va ijtimoiy tarmoqlar orqali kiberfiribgarlikning yangi usullari haqida muntazam ogohlantirishlar berib borilishi lozim. Bu aholining xabardorlik darajasini oshirib, firibgarlik holatlarining oldini olishga xizmat qiladi. Ikkinchi muhim yo‘nalish sifatida **davlat darajasida kiberxavfsizlik infratuzilmasini rivojlantirish** taklif etiladi. Zamonaviy kiberhujumlar tezkor va murakkab bo‘lganligi sababli ularga qarshi samarali kurashish uchun real vaqt rejimida ishlaydigan monitoring tizimlari zarur. Maxsus kiberxavfsizlik markazlarini tashkil etish, ularni zamonaviy texnologiyalar bilan jihozlash va 24/7 rejimda ishlashini ta’minlash muhimdir. Shuningdek, milliy darajada kiberhujumlarni aniqlash va ularga tezkor javob berish tizimi (CERT – Computer Emergency Response Team) faoliyatini kuchaytirish lozim. Uchinchi yo‘nalish — **huquqiy bazani takomillashtirish**. Kiberfiribgarlik transchegaraviy xarakterga ega bo‘lganligi sababli, milliy qonunchilik xalqaro standartlarga moslashtirilishi zarur. Kiberjinoyatlarga qarshi kurashish bo‘yicha maxsus qonunlarni kuchaytirish, jazolarni aniq belgilash va huquqiy bo‘shliqlarni bartaraf etish muhim ahamiyatga ega. Shu bilan birga, xalqaro hamkorlikni kengaytirish, INTERPOL va boshqa tashkilotlar bilan axborot almashinuvi tizimini rivojlantirish tavsiya etiladi. To‘rtinchi yo‘nalish sifatida **tashkilotlar va biznes subyektlarining kiberxavfsizlik siyosatini kuchaytirish** zarur. Har bir kompaniya o‘z ichki xavfsizlik siyosatiga ega bo‘lishi, xodimlarni muntazam ravishda kiberxavfsizlik bo‘yicha o‘qitishi va real tahdidlar bo‘yicha treninglar o‘tkazishi kerak. Korporativ tizimlarda ikki bosqichli autentifikatsiya, ma’lumotlarni shifrlash va doimiy xavfsizlik auditlari joriy etilishi lozim. Ayniqsa, bank-moliya va elektron tijorat sohalarida xavfsizlik standartlarini yanada kuchaytirish zarur. Beshinchi muhim taklif — **sun’iy intellekt va zamonaviy texnologiyalardan samarali foydalanish**. Hozirgi kunda kiberfiribgarlikni aniqlash va oldini olishda sun’iy intellekt asosidagi tizimlar katta rol o‘ynamoqda. Mashinaviy o‘rganish algoritmlari yordamida shubhali faoliyatni erta aniqlash, anomaliyalarni kuzatish va avtomatik ogohlantirish tizimlarini yaratish mumkin. Shu bilan birga, deepfake va sun’iy intellekt asosidagi firibgarliklarga qarshi ham maxsus himoya texnologiyalarini ishlab chiqish zarur. Oltinchi yo‘nalish sifatida **ijtimoiy va psixologik profilaktika choralarini kuchaytirish** muhimdir. Kiberfiribgarlikning asosiy qismi inson psixologiyasiga ta’sir qilish orqali amalga oshiriladi. Shu sababli foydalanuvchilarda shubhali holatlarni tezda aniqlash, ehtiyotkorlik va tanqidiy fikrlash ko‘nikmalarini rivojlantirish zarur. Psixologlar va IT mutaxassislari

hamkorligida maxsus treninglar va seminarlar tashkil etish foydali bo‘ladi. Yettinchi taklif — **moliyaviy xavfsizlik tizimlarini kuchaytirish**. Banklar va to‘lov tizimlari foydalanuvchilarni himoya qilish uchun qo‘shimcha xavfsizlik qatlamlarini joriy etishi kerak. Masalan, tranzaksiyalarni real vaqt rejimida tekshirish, shubhali operatsiyalarni avtomatik bloklash va foydalanuvchilarga darhol bildirish yuborish tizimlari keng qo‘llanilishi lozim. Shuningdek, foydalanuvchilarga quyidagi oddiy, ammo muhim tavsiyalarni berish zarur: noma’lum havolalarga kirmaslik, shaxsiy ma’lumotlarni hech kimga bermaslik, kuchli va murakkab parollardan foydalanish, muntazam ravishda parollarni yangilab borish hamda ikki bosqichli himoya tizimini yoqish.

Umuman olganda, kiberfiribgarlikka qarshi kurashishda yagona yondashuv yetarli emas. Bu jarayon texnik, huquqiy, ta’limiy va ijtimoiy choralarni o‘z ichiga olgan kompleks tizimni talab qiladi. Faqatgina davlat, tashkilotlar va foydalanuvchilar o‘rtasidagi hamkorlik kuchaytirilgandagina kiberfiribgarlik xavfini sezilarli darajada kamaytirish mumkin bo‘ladi.

O‘tkazilgan tadqiqot natijalari asosida shuni ta’kidlash mumkinki, kiberfiribgarlik zamonaviy raqamli jamiyatning eng dolzarb va murakkab muammolaridan biri hisoblanadi. Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi, internet foydalanuvchilari sonining keskin ortishi hamda raqamli xizmatlarning kengayishi ushbu hodisaning yanada keng tarqalishiga sabab bo‘lmoqda. Kiberfiribgarlik bugungi kunda nafaqat alohida shaxslar, balki yirik tashkilotlar, bank-moliya tizimi va hatto davlat infratuzilmalari uchun ham jiddiy tahdid sifatida namoyon bo‘lmoqda. Tadqiqot jarayonida olingan natijalar shuni ko‘rsatdiki, kiberfiribgarlikning eng keng tarqalgan ko‘rinishlari fishing, smishing, vishing, ijtimoiy muhandislik hujumlari, zararli dasturlar (malware), soxta onlayn platformalar va investitsion firibgarliklar hisoblanadi. Ushbu usullar doimiy ravishda takomillashib, yanada murakkab va yashirin shakllarga o‘tmoqda. Ayniqsa, sun’iy intellekt va avtomatlashtirilgan texnologiyalar rivojlanishi firibgarlar uchun yangi imkoniyatlar yaratib, kiberfiribgarlik darajasini yanada oshirmoqda. Tadqiqot natijalari asosida yana bir muhim xulosa shuki, kiberfiribgarlikning asosiy sababi texnologik emas, balki inson omili bilan bog‘liqdir. Foydalanuvchilarning raqamli savodxonligi yetarli darajada emasligi, internet xavfsizligi qoidalariga rioya qilmasligi, shubhali havolalarga ishonishi va shaxsiy ma’lumotlarni ehtiyotsiz ravishda oshkor qilishi firibgarlik holatlarining ko‘payishiga asosiy sabab bo‘lib xizmat qilmoqda. Shu bois kiberxavfsizlikni ta’minlashda inson omili eng muhim bo‘g‘in sifatida e’tirof etiladi.

Shuningdek, xorijiy tajribalar tahlili shuni ko‘rsatadiki, rivojlangan davlatlarda kiberfiribgarlikka qarshi kurashish tizimli va kompleks yondashuv asosida yo‘lga qo‘yilgan. AQSh, Yevropa Ittifoqi, Buyuk Britaniya, Janubiy Koreya va Singapur kabi davlatlarda maxsus kiberxavfsizlik markazlari, real vaqt monitoring tizimlari va kuchli huquqiy mexanizmlar samarali faoliyat yuritmoqda. Ushbu mamlakatlarda profilaktik yondashuv ustuvor bo‘lib, asosiy e’tibor muammoni oldindan aniqlash va uning oldini olishga qaratilgan. O‘z navbatida, rivojlanayotgan davlatlarda esa kiberfiribgarlikka qarshi kurashish ko‘pincha reaktiv xarakterga ega bo‘lib, ya’ni muammo yuzaga kelgandan keyin chora ko‘riladi. Bu esa kiberxavfsizlik tizimining samaradorligini kamaytiradi va firibgarlik holatlarining ko‘payishiga olib keladi. Shu sababli global tajriba asosida profilaktik tizimlarni rivojlantirish dolzarb vazifalardan biri hisoblanadi. Tadqiqot davomida olingan yana bir muhim xulosa shuki, kiberfiribgarlikni to‘liq yo‘q qilish mumkin emas, biroq uning xavf darajasini sezilarli darajada kamaytirish mumkin. Buning uchun texnologik, huquqiy, ijtimoiy va ta’limiy yo‘nalishlarda

kompleks chora-tadbirlar amalga oshirilishi zarur. Faqatgina bir yo‘nalishdagi yondashuv yetarli emas, balki barcha tizimlar o‘zaro uyg‘unlikda ishlashi lozim. Shuningdek, tadqiqot natijalari kiberxavfsizlik sohasida sun’iy intellekt va zamonaviy texnologiyalarni keng joriy etish muhimligini ko‘rsatdi. Ushbu texnologiyalar yordamida kiberhujumlarni erta aniqlash, shubhali faoliyatni monitoring qilish va avtomatik himoya tizimlarini yaratish mumkin. Biroq shu bilan birga, firibgarlar ham ushbu texnologiyalardan foydalanayotgani sababli doimiy innovatsion rivojlanish zarur bo‘lib qolmoqda. Umuman olganda, kiberfiribgarlik global raqamli muhitning ajralmas qismi bo‘lib, uning ta’siri kelajakda yanada kengayishi ehtimoldan xoli emas. Shu sababli har bir foydalanuvchi, tashkilot va davlat ushbu xavfga jiddiy yondashishi, o‘zining raqamli xavfsizligini ta’minlash bo‘yicha doimiy choralar ko‘rib borishi lozim.

Yakuniy xulosa sifatida shuni aytish mumkinki, kiberfiribgarlikka qarshi kurashishda eng muhim omil bu — **raqamli madaniyat va ogohlikdir**. Foydalanuvchilarning bilim darajasi qanchalik yuqori bo‘lsa, kiberfiribgarlikning muvaffaqiyat darajasi shunchalik past bo‘ladi. Shu bois kelajakda kiberxavfsizlikni ta’minlash nafaqat texnik, balki ijtimoiy strategik ustuvor yo‘nalish sifatida rivojlantirilishi lozim.

Foydalanilgan adabiyotlar

O‘zbekiston Respublikasi qonunchiligi

1. O‘zbekiston Respublikasi Jinoyat kodeksi (2025-yil tahriri).
2. O‘zbekiston Respublikasi “Axborotlashtirish to‘g‘risida”gi Qonun. 2003-yil (o‘zgartirish va qo‘shimchalar bilan).
3. O‘zbekiston Respublikasi “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi Qonun. 2002-yil.
4. O‘zbekiston Respublikasi “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun. 2019-yil.
5. O‘zbekiston Respublikasi Vazirlar Mahkamasining kiberxavfsizlik va axborot himoyasiga oid qarorlari va normativ hujjatlari.
6. O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi. Kiberxavfsizlikni rivojlantirish strategiyasi. 2023-yil.
7. TATU (Toshkent axborot texnologiyalari universiteti). Axborot xavfsizligi asoslari o‘quv qo‘llanma. Toshkent, 2022.

Xorijiy adabiyotlar va manbalar

8. Stallings, W. Cryptography and Network Security: Principles and Practice. Pearson Education, 2021.
9. Whitman, M. E., Mattord, H. J. Principles of Information Security. Cengage Learning, 2022.
10. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020.
11. ENISA. Threat Landscape Reports (2023–2025). https://www.enisa.europa.eu
12. FBI Internet Crime Complaint Center (IC3). Annual Internet Crime Report (2024). https://www.ic3.gov
13. NIST. Cybersecurity Framework (2024). https://www.nist.gov
14. Kaspersky Lab. Global Cyber Threat Intelligence Report (2023–2025). https://www.kaspersky.com

15. Microsoft Security. Digital Defense Report (2024). https://www.microsoft.com
16. INTERPOL. Cybercrime Analysis Report (2024). https://www.interpol.int
17. OECD. Digital Security Risk Management Report (2023).