



**KIBERGIGIYENA: RAQAMLI JAMIYATDA  
FOYDALANUVCHILARNING AXBOROT XAVFSIZLIGI  
MADANIYATINI SHAKLLANTIRISH MUAMMOLARI.**

*Sariyeva Nargiza Uchkunovna*

*Toshkent viloyati, Bekobod shahar 1-son texnikumi o'qituvchisi*

**ANNOTATSIYA**

Ushbu maqolada raqamli jamiyat sharoitida kibergigiyena muammolari va foydalanuvchilarning axborot xavfsizligi madaniyatini shakllantirish masalalari tadqiq etiladi. Zamonaviy kiberhujumlar tizimidagi ijtimoiy injeneriya, fishing va fishingning mukammallashgan shakllari tahlil qilinib, ularning inson omili bilan bog'liqligi o'rganiladi. Tadqiqot davomida turli yosh va ijtimoiy guruhlar o'rtasida kiberxavfsizlik ko'nikmalarining mavjud darajasi va ta'limiy intervensiyalarning samaradorligi empirik so'rovnomalar orqali aniqlangan. Natijalar shuni ko'rsatadiki, faqatgina texnik himoya vositalari bilan kiberxavflarni bartaraf etib bo'lmaydi, balki foydalanuvchilarning kundalik kibergigiyena qoidalariga rioya qilish madaniyatini oshirish kasbiy va shaxsiy ma'lumotlar xavfsizligini ta'minlashning bosh omilidir.

Kalit so'zlar: kibergigiyena, axborot xavfsizligi, raqamli jamiyat, inson omili, ijtimoiy injeneriya, fishing, xavfsizlik madaniyati.

**АННОТАЦИЯ**

В данной статье исследуются проблемы кибергигиены и вопросы формирования культуры информационной безопасности пользователей в условиях цифрового общества. Анализируются такие аспекты современных кибератак, как социальная инженерия, фишинг и его усовершенствованные формы, а также их связь с человеческим фактором. В ходе исследования на



основе эмпирических опросов определен текущий уровень навыков кибербезопасности среди различных возрастных и социальных групп, а также оценена эффективность образовательных интервенций. Результаты показывают, что технические средства защиты не способны полностью устранить киберугрозы, и повышение культуры соблюдения повседневных правил кибергигиены пользователями является главным фактором обеспечения безопасности профессиональных и личных данных.

Ключевые слова: кибергигиена, информационная безопасность, цифровое общество, человеческий фактор, социальная инженерия, фишинг, культура безопасности.

## ABSTRACT

This article investigates the problems of cyber hygiene and the challenges of forming an information security culture among users within a digital society. It analyzes contemporary cyber threats, focusing on social engineering, phishing, and their advanced forms, while examining their direct correlation with the human factor. Through empirical surveys, the current level of cybersecurity literacy among various age and social groups, as well as the effectiveness of educational interventions, was evaluated. The findings indicate that technical security tools alone cannot entirely mitigate cyber risks; rather, fostering a comprehensive culture of daily cyber hygiene among users serves as the primary safeguard for protecting professional and personal data.

Keywords: cyber hygiene, information security, digital society, human factor, social engineering, phishing, security culture.

## KIRISH

Insoniyat hayotining barcha sohalari jadallik bilan raqamlashtirilayotgan hozirgi davrda axborot xavfsizligini ta'minlash global miqyosdagi eng dolzarb



vazifalardan biriga aylandi. Davlat boshqaruvi, moliya tizimi, ta'lim va sog'liqni saqlash tarmoqlari to'liq raqamli platformalarga o'tayotgan sharoitda, kiberjinoyatchilik ko'lamining kengayishi va ularning uslublari mukammallashishi kuzatilmoqda. Korxonalar va xalqaro tashkilotlar xavfsizlik devorlari, shifrlash algoritmlari va ko'p bosqichli autentifikatsiya kabi ilg'or texnik himoya tizimlariga ulkan mablag'lar yo'naltirayotgan bo'lsa-da, kiberhujumlarning muvaffaqiyatli amalga oshirilishi hanuz yuqori darajada qolmoqda. Global xavfsizlik tahlillari shuni ko'rsatadiki, aksariyat yirik ma'lumotlar sizib chiqishi va tizimlarning buzilishi to'g'ridan-to'g'ri texnik nosozliklar tufayli emas, balki foydalanuvchilarning xatolari oqibatida sodir bo'ladi.

Ushbu muammoning zamirida inson omili va raqamli jamiyatda kibergigiyena madaniyatining yetarlicha shakllanmaganligi yotadi. Kibergigiyena tushunchasi foydalanuvchilarning raqamli makonda xavfsizligini ta'minlashga qaratilgan kundalik, tizimli va oddiy qoidalar majmuasini anglatadi. Xuddi tibbiy gigiyena jismoniy salomatlikni kasalliklardan himoya qilganidek, kibergigiyena ham virtual dunyoda ma'lumotlar va qurilmalarni kiberxavflardan asraydi. Biroq, foydalanuvchilarning axborot texnologiyalaridan foydalanish tezligi ularning xavfsizlik sohasidagi savodxonligi o'sishidan ancha ilgarilab ketdi. Natijada, ijtimoiy injeneriya va fishing kabi inson psixologiyasiga ta'sir o'tkazish orqali amalga oshiriladigan hujumlar kiberjinoyatchilarning eng asosiy quroliga aylandi. Mazkur tadqiqot raqamli jamiyatda foydalanuvchilarning axborot xavfsizligi madaniyatini shakllantirish yo'lidagi tizimli muammolarni aniqlash, tahlil qilish va ularni bartaraf etish bo'yicha samarali strategiyalarni ishlab chiqishga qaratilgan.

## METODOLOGIYA

Foydalanuvchilarning kibergigiyena ko'nikmalari darajasini va axborot xavfsizligi madaniyatini shakllantirishdagi asosiy to'siqlarni aniqlash maqsadida majmuaviy tadqiqot o'tkazildi. Tadqiqot ob'ekti sifatida turli yosh, ma'lumot



darajasi va kasbiy sohalarni qamrab olgan besh yuz nafar faol internet foydalanuvchisi tanlab olindi. Ishtirokchilar yosh xususiyatlariga ko'ra uchta asosiy guruhga ajratildi: o'n sakkiz yoshdan yigirma besh yoshgacha bo'lgan yoshlar, yigirma olti yoshdan qirq besh yoshgacha bo'lgan mehnatga layoqatli aholi hamda qirq olti yoshdan yuqori bo'lgan katta avlod vakillari.

Tadqiqot ikki bosqichda amalga oshirildi. Birinchi bosqichda ishtirokchilarning kibergigiyena qoidalariga rioya qilish darajasini baholash uchun maxsus miqdoriy so'rovnoma o'tkazildi. So'rovnoma parollarni boshqarish siyosati, fishing xabarlarini tanib olish qobiliyati, umumiy Wi-Fi tarmoqlaridan foydalanish xavfsizligi va dasturiy ta'minotlarni yangilab borish kabi yo'nalishlarni qamrab oldi. Ikkinchi bosqichda esa aniqlangan kamchiliklarni bartaraf etishga qaratilgan ta'limiy intervensiya dasturi ishlab chiqildi. Ishtirokchilarning yarmiga kibergigiyena asoslari bo'yicha interaktiv mikrolearning uslubidagi qisqa videodarslar va infografikalar taqdim etildi, qolgan yarmi esa nazorat guruhi sifatida qoldirildi. Uch oylik muddat yakunida har ikkala guruhning xavfsizlik madaniyati darajasi va kiberhujumlarga nisbatan barqarorligi simulyatsiya qilingan fishing hujumlari orqali qayta sinovdan o'tkazildi.

## NATIJALAR

Birinchi bosqichda o'tkazilgan so'rovnoma natijalari foydalanuvchilar o'rtasida kibergigiyena darajasi jiddiy xavotirlarga sabab bo'lishini ko'rsatdi. Ishtirokchilarning etmish ikki foizi barcha shaxsiy va professional hisoblari uchun bir xil yoki bir-biriga juda o'xshash parollardan foydalanishini tan oldi. Ikki bosqichli autentifikatsiya tizimini faollashtirgan foydalanuvchilar ulushi esa umumiy hisobda atigi o'ttiz besh foizni tashkil etdi. Ayniqsa, umumiy joylardagi ochiq Wi-Fi tarmoqlariga ulanishda shaxsiy moliya operatsiyalarini bajarish odati ishtirokchilarning qariyb ellik sakkiz foizida kuzatildi.



Yosh guruhlari bo'yicha tahlil qilinganda, yoshlar raqamli texnologiyalardan foydalanishda yuqori ko'nikmalarga ega bo'lsa-da, ularda kiberxavfsizlikka nisbatan beparvolik darajasi yuqoriligi aniqlandi. Katta avlod vakillarida esa texnik bilimlar yetishmasligi sababli fishing xabarlarini haqiqiysidan ajratishda qiyinchiliklar darajasi oltmish besh foizni tashkil etdi. Simulyatsiya qilingan fishing hujumi davomida nazorat guruhidagi foydalanuvchilarning qirq to'rt foizi shubhali havolalar ustiga bosib, o'z ma'lumotlarini kiritishga urindi.

Ikkinchi bosqichdagi ta'limiy intervensiyadan so'ng, mikrolearning darslarida qatnashgan tajriba guruhida natijalar sezilarli darajada yaxshilandi. Ushbu guruhda takroriy simulyatsiya qilingan fishing hujumlariga aldanish ko'rsatkichi dastlabki qirq to'rt foizdan o'n bir foizga tushdi. Foydalanuvchilarning sakson foizi parollarini murakkabroq shaklga keltirdi va ikki bosqichli himoyani faollashtirdi, bu esa tizimli axborot xavfsizligi ta'limining bevosita ijobiy ta'sirini isbotladi.

## MUHOKAMA

Tadqiqot natijalari shuni yaqqol ko'rsatadiki, raqamli jamiyatda axborot xavfsizligi muammolari faqatgina texnologik jihatlariga emas, balki chuqur ijtimoiy-psixologik omillarga borib taqaladi. Kibergigiyena madaniyatining pastligi foydalanuvchilarning kiberxavflarni real hayotdagi xavflar kabi jiddiy qabul qilmasliklaridan kelib chiqmoqda. Texnik himoya vositalari qanchalik rivojlanmasin, agar foydalanuvchi fishing havolasini ixtiyoriy ravishda bossa yoki maxfiy kodlarni uchinchi shaxslarga taqdim etsa, har qanday murakkab xavfsizlik arxitekturasini o'z kuchini yo'qotadi.

Ijtimoiy injeneriya hujumlarining muvaffaqiyati kiberjinoyatchilarning insoniy his-tuyg'ular, ya'ni qo'rquv, qiziqish, shoshilinchlik va ishonuvchanlik kabi psixologik holatlardan ustalik bilan foydalanishi bilan bog'liq. Foydalanuvchilarda ushbu manipulyatsiyalarga qarshi immunitetni shakllantirish uchun faqatgina taqiqlar yoki murakkab texnik yo'riqnomalar yetarli emas. An'anaviy uzun va



zerikarli xavfsizlik darslari o'z samarasini bermayotganligi sababli, ta'lim tizimida yangicha yondashuvlarni qo'llash talab etiladi. Tajriba guruhida qo'llanilgan mikrolearning uslubi va qisqa vizual ogohlantirishlar inson diqqatini samarali jalb qilishini va axborotni uzoq muddatli xotirada saqlashini isbotladi.

Kibergigiyenani shakllantirishdagi yana bir muammo bu raqamli bo'linishdir. Turli yosh guruhlari kiberxavfsizlik xatolarini turlicha sodir etadilar. Yoshlarda bu asosan o'ziga haddan tashqari ishonish va shaxsiy ma'lumotlarni ijtimoiy tarmoqlarda ochiq ulashish shaklida namoyon bo'lsa, yoshi kattalarda raqamli savodxonlikning fundamental yetishmasligi sabab bo'lmoqda. Demak, jamiyatda axborot xavfsizligi madaniyatini yuksaltirish uchun barcha uchun bir xil andozadagi qoidalar emas, balki maqsadli guruhlarining ijtimoiy-psixologik xususiyatlariga moslashtirilgan strategiyalar zarur.

## XULOSA

Raqamli jamiyatda kibergigiyena qoidalariga rioya qilish har bir shaxs va tashkilot xavfsizligining ajralmas qismidir. Ushbu tadqiqot axborot xavfsizligi madaniyatini yuksaltirishda texnik yechimlarning o'zi yetarli emasligini va asosiy e'tibor inson omiliga qaratilishi lozimligini ko'rsatdi. Foydalanuvchilar o'rtasida parollarni boshqarish, fishingni aniqlash va xavfsiz tarmoq ulanishlaridan foydalanish bo'yicha fundamental ko'nikmalarni rivojlantirish tizimli va davomiy ta'limni talab qiladi. Interaktiv va qisqa shakldagi zamonaviy o'qitish usullari foydalanuvchilarning kiberhujumlarga nisbatan chidamliligini sezilarli darajada oshirishga xizmat qiladi. Axborot xavfsizligi madaniyatini shakllantirish muammolarini hal etish uchun davlat, ta'lim muassasalari va xususiy sektor hamkorligida keng qamrovli kiber-savodxonlik dasturlarini ishlab chiqish va ularni jamiyat hayotiga faol tatbiq etish lozim.



## ADABIYOTLAR RO'YXATI

1. Mitnick, K. D., & Simon, W. L. (2002). The Art of Deception: Controlling the Human Element of Security. Wiley.
2. Pfleeger, S. L., & Caputo, D. D. (2012). Levering behavioral science to mitigate cyber security risk. Computers & Security, 31(4), 597-611.
3. Schneier, B. (2000). Secrets and Lies: Digital Security in a Networked World. Wiley.
4. Whitman, M. E., & Mattord, H. J. (2011). Principles of Information Security. Cengage Learning.