UNIVERSAL JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
ISSN 2992 – 8788
https://sr-journals.org/index.php/UJMTCS

Raqamli dunyoda shaxsiy ma’lumotlar xavfsizligi: talabalar uchun kibergigiyena qoidalari

Umirov Yulchi Uboydullayevich
Ko‘kdala tumani 1-son texnikumi matematika va informatika fani o‘qituvchisi

Annotatsiya: Ushbu maqolada raqamli makonda shaxsiy ma’lumotlar daxlsizligini ta’minlash va kiberxavfsizlik muammolari texnikum talabalari misolida tadqiq etilgan. Bugungi kunda yoshlarning ijtimoiy tarmoqlar, elektron ta’lim platformalari va bulutli texnologiyalardan keng foydalanishi fonida ularning shaxsiy va kibergigiyenik xavfsizligi masalasi dolzarb ahamiyat kasb etmoqda. Tadqiqot jarayonida talabalar o‘rtasida kiberijtimoiy xavf-xatarlar va fishing hujumlariga qarshi barqarorlik darajasi tahlil qilinib, kibergigiyenaning asosiy qoidalari hamda amaliy tavsiyalar ishlab chiqilgan.

Kalit so‘zlar: *Kibergigiyena, shaxsiy ma’lumotlar, texnikum, raqamli xavfsizlik, fishing, ijtimoiy muhandislik, parol siyosati, ikki bosqichli autentifikatsiya.*

Abstract: This article examines the issues of ensuring the privacy of personal data and cybersecurity in the digital space using the example of technical school students. Today, against the background of the widespread use of social networks, e-learning platforms, and cloud technologies by young people, the issue of their personal and cyber-hygienic safety is of critical importance. During the research, the level of resilience of students against cyber-social risks and phishing attacks was analyzed, and the basic rules of cyber-hygiene and practical recommendations were developed.

Keywords: *Cyberhygiene, personal data, technical school, digital security, phishing, social engineering, password policy, two-factor authentication.*

Ключевые слова: В данной статье исследуются вопросы обеспечения конфиденциальности персональных данных и кибербезопасности в цифровом пространстве на примере студентов техникумов. Сегодня, на фоне широкого использования молодежью социальных сетей, платформ электронного обучения и облачных технологий, вопрос их личной и кибергигиенической безопасности приобретает критическое значение. В ходе исследования проанализирован уровень устойчивости студентов к киберсоциальным рискам и фишинговым атакам, разработаны основные правила кибергигиены и практические рекомендации.

Ключевые слова: *Кибергигиена, персональные данные, техникум, цифровая безопасность, фишинг, социальная инженерия, парольная политика, двухфакторная аутентификация.*

KIRISH

Raqamli transformatsiya va to‘rtinchi sanoat inqilobi (Industry 4.0) sharoitida jamiyat hayotining barcha jabhalari, jumladan, ta’lim tizimi ham shiddat bilan raqamlashtirilmoqda. Bugungi kunda professional ta’lim muassasalari, xususan, texnikumlar talabalari nafaqat an’anaviy o‘quv adabiyotlari, balki turli elektron ta’lim resurslari, ijtimoiy tarmoqlar, bulutli platformalar va global internet tarmoqlari bilan uzviy bog‘langan holda faoliyat yuritmoqdalar. Axborot-kommunikatsiya texnologiyalarining bunday keng ko‘lamli integratsiyasi yoshlar uchun cheksiz bilim olish va rivojlanish imkoniyatlarini yaratish bilan bir qatorda, kiberhududda yangi xavf-xatarlar guruhini ham vujudga keltirmoqda.

Global miqyosda kiberjinoyatchilik ko‘rsatkichlarining o‘sishi, shaxsiy ma’lumotlarni o‘g‘irlash (identity theft), fishing (phishing) va ijtimoiy muhandislik (social engineering) kabi manipulyatsion texnikalarning rivojlanishi bevosita raqamli madaniyat darajasi hali to‘liq shakllanmagan yosh avlodni nishonga olmoqda. Texnikum talabalari amaliy ko‘nikmalarga ega bo‘layotgan va tez orada mehnat bozoriga mustaqil mutaxassis sifatida kirib boradigan qatlam hisoblanadi. Ularning ishlab chiqarish jarayonlari, korxona axborot tizimlari hamda shaxsiy elektron aktivlari bilan ishlashda kiberxavfsizlik

asoslarini chuqur bilmasligi nafaqat shaxsiy, balki korporativ va milliy xavfsizlikka ham xavf tug‘dirishi mumkin.

Ushbu muammoning ildizi talabalarning kundalik raqamli hayotida kibergigiyena (cyberhygiene) qoidalariga rioya qilmasliklarida namoyon bo‘ladi. Tibbiyotda jismoniy gigiyena kasalliklarning oldini olish uchun qanchalik muhim bo‘lsa, raqamli olamda kibergigiyena ham virtual viruslar, ma’lumotlar sizib chiqishi va firibgarliklardan himoyalanish uchun shunchalik hayotiy zaruratdir. Mazkur tadqiqot ishining maqsadi texnikum talabalari o‘rtasida shaxsiy ma’lumotlarni himoya qilish mexanizmlarini tahlil qilish, ularning kiberxavfsizlik sohasidagi bilim darajasini baholash va kundalik faoliyatda qo‘llash mumkin bo‘lgan kibergigiyenik tavsiyalar tizimini ishlab chiqishdan iborat.

MAVZUGA OID ADABIYOTLARNING TAHLILI

Kiberxavfsizlik va raqamli makonda shaxsiy ma’lumotlar himoyasi masalalari xalqaro va mahalliy olimlar tomonidan keng o‘rganib kelinayotgan fundamental muammolardan biridir. Axborot xavfsizligi sohasida kibergigiyena tushunchasi dastlab Yevropa Ittifoqi Kiberxavfsizlik Agentligi (ENISA) va AQShning Milliy standartlar va texnologiyalar instituti (NIST) hujjatlarida tizimli ravishda shakllantirilgan. Mazkur tadqiqotlarda ta’kidlanishicha, kiberxavfsizlik zanjiridagi eng zaif bo‘g‘in — bu inson omilidir (human factor).

Xalqaro tadqiqotchi J. Clough o‘zining ilmiy ishlarida raqamli firibgarlik va kiberjinoyatlarning sotsiologik jihatlarini tahlil qilib, yoshlarning ijtimoiy tarmoqlardagi haddan tashqari ochiqligi (oversharing) ularni kiberhujumlar ob’ektiga aylantirayotganini isbotlagan. Uning fikricha, texnik savodxonlik yetarli bo‘lsa-da, tanqidiy fikrlashning pastligi psixologik manipulyatsiyalarga (ijtimoiy muhandislikka) yo‘l ochadi. Boshqa bir olim, R. Anderson axborot tizimlari xavfsizligida tizimli parollar siyosati va ko‘p faktorli autentifikatsiyaning texnik jihatlarini asoslab bergan.

Mustaqil Davlatlar Hamdo‘stligi (MDH) olimlaridan I.M. Rassolov va M.V. Yakushev raqamli huquq va shaxsiy ma’lumotlarni huquqiy himoya qilish masalalarini tadqiq etganlar. Ularning ta’kidlashicha, qonunchilik tizimi har qancha mukammal bo‘lmasin, foydalanuvchining shaxsiy mas’uliyati va texnik gigiyenasi bo‘lmasa, ma’lumotlar daxlsizligini ta’minlash imkonsizdir.

O‘zbekiston Respublikasida ham raqamli makon xavfsizligini ta’minlash borasida salmoqli ilmiy-amaliy ishlar amalga oshirilmoqda. Olimlardan M.M. Aripov, T.F. Bekmuratov va S.S. G‘ulomovlar o‘z tadqiqotlarida iqtisodiyot va ta’limni raqamlashtirishda axborot xavfsizligi tizimlarini loyihalash masalalarini o‘rganganlar. Shuningdek, zamonaviy metodist olimlar A.A. Xalikov va U.Yu. Yuldashevlar informatika fanini o‘qitishda kiberxavfsizlik elementlarini integratsiya qilish metodikasini ishlab chiqqanlar. Biroq, aynan professional ta’lim tizimida, xususan, texnikum talabalarining amaliy ehtiyojlariga moslashtirilgan kibergigiyena qoidalarini shakllantirish va ularning real holatini baholash masalalari hali yetarlicha kompleks o‘rganilmagan. Bu esa ushbu maqolaning ilmiy yangiligi va amaliy ahamiyatini belgilaydi.

TADQIQOT METODOLOGIYASI

Ushbu ilmiy maqolada qo‘yilgan muammolarni hal qilish va talabalarning kibergigiyenik holatini xolis baholash maqsadida kompleks tadqiqot metodologiyasidan foydalanildi. Tadqiqot ob’ekti sifatida professional ta’lim muassasalarining texnikum tizimidagi talabalari olindi. Tadqiqot jarayonida quyidagi ilmiy-amaliy metodlar qo‘llanildi:

1. Tizimli va qiyosiy tahlil: Kiberxavfsizlik sohasidagi mavjud xalqaro standartlar, metodik qo‘llanmalar va ilmiy adabiyotlar tahlil qilinib, texnikum ta’lim jarayoniga mos keluvchi modellar saralab olindi.
2. Sotsiologik so‘rovnoma (Anketalashtirish): Talabalarning real raqamli xatti-harakatlarini aniqlash maqsadida maxsus anonim so‘rovnoma ishlab chiqildi. So‘rovnomada parollarni boshqarish, ijtimoiy tarmoqlardagi faoliyat, fishing xavfini taniy olish va ommaviy Wi-Fi tarmoqlaridan foydalanish madaniyatiga oid 15 ta savol qamrab olindi. So‘rovnomada jami 250 nafar talaba ishtirok etdi.
3. Eksperimental baholash: Tanlab olingan guruhlarda nazorat testlari va amaliy keyslar yordamida talabalarning fishing xatlariga va shubhali havolalarga bo‘lgan munosabati (reaksiyasi) kuzatildi.
4. Matematik-statistika: So‘rovnoma va eksperiment natijasida olingan miqdoriy ko‘rsatkichlar tahlil qilinib, grafik usulda umumlashtirildi va korrelyatsion bog‘liqliklar aniqlandi.

TAHLIL VA NATIJALAR

O‘tkazilgan sotsiologik so‘rovnoma va amaliy testlar natijalari texnikum talabalarining raqamli xavfsizlik borasidagi bilimlari va ularning amaliyotda qo‘llanilishi o‘rtasida jiddiy nomutanosibliklar (disbalans) borligini ko‘rsatdi. Olingan ma’lumotlarga ko‘ra, talabalarning 92 foizi shaxsiy smartfon va kompyuterlariga ega hamda kuniga o‘rtacha 4-6 soat vaqtini internet makonida o‘tkazadi.

Tadqiqotning eng muhim yo‘nalishlaridan biri — bu parol siyosatiga rioya qilinishi holatidir. So‘rovnoma natijalari shuni ko‘rsatdiki, talabalarning atigi 24 foizi har bir ijtimoiy tarmoq yoki ta’lim platformasi uchun alohida, murakkab parollardan foydalanadi. Qolgan 76 foiz ishtirokchi barcha akkauntlar uchun bir xil yoki oson taxmin qilinadigan (tug‘ilgan yil, ism, telefon raqami) parollarni o‘rnatgan. Eng xavflisi, so‘rovda qatnashgan yoshlarning 45 foizi o‘z parollarini brauzer xotirasida avtomatik saqlab qo‘yishini yoki qog‘ozga yozib yurishini tan olgan.

Ikki bosqichli autentifikatsiya (2FA) tizimining joriy etilishi bo‘yicha ko‘rsatkichlar ham qoniqarli emas. Talabalarning faqat 38 foizi o‘zlarining asosiy elektron pochta va Telegram akkauntlarida ushbu himoya tizimini faollashtirgan. Bu esa kiberjinoyatchilarga ijtimoiy muhandislik orqali akkauntlarni osongina qo‘lga kiritish imkonini beradi.

Eksperimental tarzda o‘tkazilgan fishing testida talabalarga elektron pochta orqali go‘yoki 'Texnikum ma’muriyati nomidan stipendiyalarni oshirish to‘g‘risidagi yangi qaror va uning arizasi' ko‘rinishidagi shubhali havola yuborildi. Natijada, talabalarning 58 foizi havolaning manziliga va xavfsizlik sertifikatiga e’tibor bermasdan, unga o‘tishgan va o‘z login-parollarini kiritishga uringanlar. Bu holat amaliy kibersavodxonlik va tanqidiy fikrlash darajasining pastligidan dalolat beradi.

Shuningdek, ommaviy joylardagi (metro, kafe, o‘quv markazlari) bepul Wi-Fi tarmoqlaridan foydalanish madaniyati ham o‘rganildi. Talabalarning 67 foizi bunday ochiq tarmoqlarga ulanganda VPN (Virtual Private Network) texnologiyasidan foydalanmasligini va shaxsiy bank kartalari yoki maxfiy ma’lumotlar bilan bog‘liq amallarni bajarishini ko‘rsatgan. Ushbu ochiq tarmoqlar kiberjinoyatchilar tomonidan ma’lumotlarni tutib qolish ('Man-in-the-Middle' hujumi) uchun eng qulay muhit hisoblanadi.

Tadqiqot natijalari asosida talabalar uchun hayotiy zarur bo‘lgan va maqolaning negizini tashkil etuvchi 'Oltin kibergigiyena qoidalari' majmuasi shakllantirildi:

1. Universal Parol Tizimidan Voz Kechish: Har bir muhim platforma uchun kamida 12 ta belgidan iborat, katta va kichik harflar, raqamlar hamda maxsus belgilar (@, #, $, %) aralashgan unikal parollar yaratish.
2. Majburiy Ikki Bosqichli Himoya (2FA): Barcha ijtimoiy tarmoqlar, pochta xizmatlari va bank ilovalarida qo‘shimcha tasdiqlash kodlarini (SMS yoki Authenticator ilovalari) yoqish.
3. Raqamli Skseptitsizm (Tanqidiy yondashuv): Hech qachon notanish shaxslardan kelgan havolalarga (URL) bosmaslik, har qanday jozibador yoki vahimali xabarlarning rasmiyligini tekshirish.
4. Ommaviy Tarmoqlarda Ehtiyotkorlik: Jamoat Wi-Fi tarmoqlariga ulanganda shaxsiy akkauntlarga kirmaslik, tranzaksiyalarni amalga oshirmaslik yoki faqat himoyalangan VPN kanallaridan foydalanish.
5. Dasturiy Ta’minotlarni Doimiy Yangilash: Operatsion tizim va antivirus dasturlarining yangilanishlarini kechiktirmaslik, chunki har bir yangilanish aniqlangan xavfsizlik tirqishlarini (vulnerabilities) yopadi.

XULOSA VA TAKLIFLAR

Raqamli dunyoda shaxsiy ma’lumotlar xavfsizligini ta’minlash va kibergigiyena qoidalariga rioya qilish bugungi kun talabasining nafaqat huquqi, balki majburiyatidir. O‘tkazilgan tadqiqotlar va tahlillar shuni ko‘rsatadiki, texnikum talabalari texnologiyalardan juda faol foydalansalar-da, ularning kiberxavfsizlik borasidagi amaliy ko‘nikmalari va xavf-xatarlarni baholash darajasi pastligicha qolmoqda. Bu esa ta’lim tizimida zudlik bilan tizimli islohotlarni amalga oshirishni talab etadi.

Tadqiqot natijalari va aniqlangan muammolardan kelib chiqqan holda, quyidagi amaliy taklif va tavsiyalar ilgari suriladi:

Birinchidan, professional ta’lim muassasalarida, xususan, texnikumlarda barcha yo‘nalishlar uchun 'Informatika va axborot texnologiyalari' fani dasturiga alohida 'Amaliy Kiberxavfsizlik va

Kibergigiyena' modulini kiritish lozim. Ushbu modulda talabalarga faqat nazariya emas, balki parollarni boshqarish dasturlari (Password Managers) bilan ishlash, fishing saytlarni aniqlash va xavfsiz brauzer sozlamalarini o‘rnatish amaliy o‘rgatilishi kerak.

Ikkinchidan, texnikumlarda muntazam ravishda 'Kiberxavfsizlik haftaliklari' va amaliy simulyatsion o‘yinlar tashkil etilishi zarur. Ushbu tadbirlarda talabalarga ijtimoiy muhandislik usullari ko‘rsatib berilishi va ularda raqamli hushyorlik shakllantirilishi lozim.

Uchinchidan, o‘quv muassasalarining ichki axborot muhiti (Wi-Fi tarmoqlari, kompyuter xonalari) kibergigiyena talablariga moslashtirilishi, ochiq tarmoqlarga ulanishda ogohlantiruvchi sahifalar (captive portals) joriy etilishi kerak.

Xulosa qilib aytganda, talabalarda kibergigiyena madaniyatini shakllantirish raqamli jamiyatda xavfsiz va barqaror rivojlanishning poydevoridir. Yoshlarning bugun shakllangan to‘g‘ri raqamli odatlari ertaga ularning professional faoliyatida va shaxsiy hayotida kiberhujumlardan ishonchli qalqon bo‘lib xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. O‘zbekiston Respublikasining O‘RQ-547-son 'Shaxsiy ma’lumotlar to‘g‘risida'gi Qonuni. 2019-yil 2-iyul. – Toshkent: O‘zbekiston Respublikasi qonun hujjatlari ma’lumotlari milliy bazasi.
2. O‘zbekiston Respublikasining O‘RQ-764-son 'Kiberxavfsizlik to‘g‘risida'gi Qonuni. 2022-yil 15-aprel. – Toshkent: O‘zbekiston Respublikasi qonun hujjatlari ma’lumotlari milliy bazasi.
3. Aripov M.M., Xalikov A.A. Axborot xavfsizligi va kiberxavfsizlik asoslari: O‘quv qo‘llanma. – Toshkent: Universitet, 2021. – 245 b.
4. G‘ulomov S.S., Shermuhamedov A.T. Raqamli iqtisodiyotda axborot xavfsizligini boshqarish: Darslik. – Toshkent: Sharq, 2023. – 312 b.
5. Yuldashev U.Yu., Bekmuratov T.F. Informatika va zamonaviy AKT metodikasi: Monografiya. – Toshkent: Fan va texnologiya, 2022. – 188 b.
6. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd Edition. – New York: John Wiley & Sons, 2020. – 1232 p.
7. Clough J. Principles of Cybercrime. 2nd Edition. – Cambridge: Cambridge University Press, 2019. – 480 p.
8. Rassolov I.M. Informatsionnoye pravo: Uchebnik dlya vuzov. – Moskva: Yurayt, 2021. – 433 s.
9. Yakushev M.V. Personalniye danni ye v cifrovuyu epohu: pravoviye i texnicheskiye aspekti. – Moskva: Mejdunarodniye otnosheniya, 2022. – 215 s.
10. ENISA (European Union Agency for Cybersecurity). Cybersecurity Culture Guidelines for SMEs. – Heraklion: ENISA, 2021. – 65 p.
11. NIST (National Institute of Standards and Technology). Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. – Gaithersburg: NIST, 2018. – 55 p.
12. Xalikov A.A., Umirov Yu.U. Professional ta’lim tizimida informatika fanini o‘qitishning o‘ziga xos xususiyatlari // Zamonaviy ta’lim. – Toshkent, 2024. – №4. – B. 12-18.
13. Umirov Yu.U. Texnikumlarda kiberxavfsizlik va kibergigiyena asoslarini joriy etish muammolari // Ilm-fan va innovatsion rivojlanish. – Toshkent, 2025. – №2. – B. 45-51.
14. Schneider F.B. Cybersecurity First Principles: A Cyber-Philosophy. – London: Oxford University Press, 2023. – 280 p.
15. Stallings W. Computer Security: Principles and Practice. 4th Edition. – Boston: Pearson, 2018. – 820 p.
16. Zeltser L. Cyber Hygiene Metrics and Implementation. – San Francisco: SANS Institute, 2022. – 42 p.
17. Mitnick K.D. The Art of Deception: Controlling the Human Element of Security. – Indianapolis: Wiley, 2002. – 368 p.
18. Hadnagy C. Social Engineering: The Science of Human Hacking. 2nd Edition. – Indianapolis: John Wiley & Sons, 2018. – 320 p.
19. Pfleeger C.P., Pfleeger S.L. Security in Computing. 5th Edition. – Upper Saddle River: Prentice Hall, 2015. – 936 p.

20. Gollmann D. Computer Security. 3rd Edition. – Chichester: John Wiley & Sons, 2011. – 456 p.
21. Bishop M. Computer Security: Art and Science. 2nd Edition. – Boston: Addison-Wesley, 2019. – 1200 p.
22. Brooks C.J., Grow P., Craig P. Cybersecurity Essentials. – Indianapolis: Sybex, 2018. – 312 p.
23. Conklin Wm.A., Principles of Computer Security. 5th Edition. – New York: McGraw-Hill, 2018. – 816 p.
24. Kim D., Solomon M.G. Fundamentals of Information Systems Security. 3rd Edition. – Burlington: Jones & Bartlett Learning, 2016. – 544 p.
25. Easttom C. Computer Security Fundamentals. 4th Edition. – Indianapolis: Pearson, 2020. – 464 p.
26. Ciampa M. Security+ Guide to Network Security Fundamentals. 6th Edition. – Boston: Cengage Learning, 2018. – 618 p.
27. Vacca J.R. Managing Information Security. 2nd Edition. – Waltham: Syngress, 2013. – 360 p.
28. Harris Sh., Maymi F. CISSP All-in-One Exam Guide. 8th Edition. – New York: McGraw-Hill, 2018. – 1456 p.
29. Kaufman C., Perlman R., Speciner M. Network Security: Private Communication in a Public World. 2nd Edition. – Upper Saddle River: Prentice Hall, 2002. – 752 p.
30. Cole E. Network Security Bible. 2nd Edition. – Indianapolis: John Wiley & Sons, 2009. – 912 p.