ISNN 3030-3907

2026
MAY
ISSUE - 5
VOLUME -12

DEVELOPMENT OF SCIENCE

scientific journal



Development of science

Ilmiy jurnal

MAY 2026
Issue - 5, VOLUME – 12

ISSN 3030 -3907

Ilmiy jurnal OAK rayosatining 2024 yil 27 sentabrdagi 361-son qaroriga asosan 02.00.00 kimyo fanlari hamda 2025 yil 12 fevral 367- son qaroriga asosan 05.00.00 texnika fanlari bo‘yicha falsafa doktori (PhD) va fan doktori (DSc) ilmiy darajasiga talabgorlarning dissertatsiya ishlari yuzasidan dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan milliy ilmiy nashrlar ro‘yxatiga kiritilgan.

BOSH MUHARRIR:
Temirov Alisher Hoshim o‘g‘li – texnika fanlari falsafa doktori (PhD),Dotsent.
TAHRIRIYAT KENGASH RAISI:
Fozilov Sadriddin Fayzullayevich – texnika fanlari doktori, professor
TAHRIRIYAT KENGASH A’ZOLARI

TEXNIKA FANLARI/ TECHNICAL SCIENCES/ ТЕХНИЧЕСКИЕ НАУКИ

Bozorov G‘ayrat Rashidovich
Buxoro Davlat Texnika Universiteti, professor
Abdurahmonov Olim Rustamovich
Buxoro Davlat Texnika Universiteti, professor
Adizov Bobur Zamirovich
O‘zbekiston Respublikasi Fanlar akademiyasi Umumiy va noorganik kimyo instituti, professor
Hayitov Ruslan Rustamjonovich
Buxoro Davlat Texnika Universiteti, professor
Jumayev Qayum Karimovich
Buxoro Davlat Texnika Universiteti, professor.
Berdiyev Dorob Murodovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor
Maxmudov Rafiq Amonovich
Buxoro Davlat Texnika Universiteti, professor.
Tilloyev Lochin Ismatilloyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Raxmonov Qahramon Sanakulovich
Buxoro Davlat Texnika Universiteti, dotsent.
Barakayev Nusratullo Rajabovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor.
Jo‘rayev Xayrullo Fayziyevich
Buxoro Davlat Texnika Universiteti, professor.
Panoyev Erali Rajabboyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Ataullayev Sherzod Nabiullyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Malik Negmurodovich
Buxoro Davlat Texnika Universiteti, dotsent.
Axmedova Ozoda Bahronovna
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti.
Safarov Bahri Jumayevich
Buxoro Davlat Texnika Universiteti, dotsent.
Xaydarov Axtam Amonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Safarov Jasur Alijon o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.

KIMYO FANLARI/ CHEMICAL SCIENCES/ ХИМИЧЕСКИЕ НАУКИ

Axmedov Voxid Nizomovich
Buxoro Davlat Texnika Universiteti, professor
Umarov Baqo Bafoyevich
Buxoro Davlat Universiteti, professor
Kodirov Abduaxad Abduraximovich
Qarshi davlat Universiteti, professor
Qurbonov Mingniqul Jumagulovich
Qarshi davlat Universiteti, dotsent
Turemuratov Sharibay Naurizbaevich
O‘zbekiston Respublikasi Fanlar akademiyasi Qoraqalpog‘iston bo‘limi Bosh ilmiy kotibi, professor
Tursunov Kaxor Shonazarovich
Qarshi davlat Universiteti, professor
Do‘stov Hamro
Buxoro Davlat Texnika Universiteti, professor
Panoyev Nodir Shavkatovich
Buxoro Davlat Texnika Universiteti, dotsent.
Olimov Bobur Bahodir o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Kasimov Sherzod Abduazimovich
Termiz Davlat Universiteti, professor.
Aliqulov Rustam Valiyevich
Termiz Davlat Universiteti, professor
Tropov Xamza Tursunovich
Samarqand Davlat Universiteti, professor

IQTISODIYOT FANLARI/ ECONOMICS/ ЭКОНОМИЧЕСКИЕ НАУКИ

Nizamov Aslitdin Badreddinovich
Buxoro Davlat Texnika Universiteti, professor.
Boboyev Akmal Choriyevich
Buxoro Davlat Texnika Universiteti, professor.
Ergashxojayeva Shaxnoza Djasurovna
Toshkent davlat iqtisodiyot universiteti, professor
Saidaxmedova Nodira Ilxomovna
Toshkent davlat iqtisodiyot universiteti, professor
Muxsinov Bekzod Toxirovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shakarov Qulmat Ashirovich
Renessans ta'lim universiteti,dotsent.
Jumaeva Zulfiya Qayumovna
Buxoro Davlat Texnika Universiteti, dotsent.
Norova Salomat Yusupovna
Buxoro Davlat Texnika Universiteti, dotsent.
Avezova Shaxnoza Maxmudjonovna
Buxoro Davlat Texnika Universiteti, dotsent.
Jalilov Jamshid G‘anijonovich
Toshkent davlat iqtisodiyot universiteti, dotsent
Xasanova Gulruh Djumanazarovna
Buxoro Davlat Texnika Universiteti, dotsent.

PEDAGOGIKA FANLARI/ PEDAGOGICAL SCIENCES / ПЕДАГОГИЧЕСКИЕ НАУКИ

Siddiqova Sadoqat G‘afforovna
Buxoro Davlat Texnika Universiteti, dotsent.
Zoyirov Erkin Xalilovich
Buxoro Davlat Texnika Universiteti, DSc, professor
Gaffarov Feruz Hasanovich
Puchon Universiteti, *professor*
Ruziyev Davron Yuldashevich
Buxoro Davlat Universiteti, professor
Muradova Firuza Rashidovna
Buxoro Davlat Texnika Universiteti, professor.
Yunusova Gulandon Samiyevna
Buxoro Davlat Texnika Universiteti, professor.
To‘xtayeva Zebo Sharifovna
Buxoro Davlat Texnika Universiteti, professor.
Navro‘zova Gulchixra Nigmatovna
Buxoro Davlat Texnika Universiteti, dotsent.
Uzoqova Laylo Polvonovna
Buxoro muhandislik – texnologiya instituti, dotsent.
To‘raqulova Marjona Qiyom qizi
Buxoro Davlat Texnika Universiteti, dotsent.
Muradova Zarina Rashidovna
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Sanjar Aslonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shodiyev Jahongir Jo‘raqulovich
Buxoro Davlat Texnika Universiteti, dotsent
Gaffarov Laziz Hasanovich
Buxoro muhandislik – texnologiya instituti, dotsent.

Tahririyat a’zolarning to‘liq ro‘yxati jurnalning www.devos.uz saytida keltirilgan.

Tahririyat hay’ati a’zolarining tarkibini o‘zgartirish hamda qo‘shimcha kiritish yoki tahririyat a’zoligidan chiqarish bosh muharrir tomonidan amalga oshiriladi.

ISSN 3030-3907

Development of science ilmiy jurnali 2024 yil 15 aprel kuni №256445 sonli guvohnoma bilan Davlat ro‘yxatidan o‘tgan.

To‘plam elektron ko‘rinishda (pdf formatida) mualliflarga taqdim etiladi. To‘plamga kiritiladigan maqolalarning mazmuni, ulardagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligiga hamda har qanday fikr - mulohazalarga mualliflarning o‘zlari mas’ul hisoblanadilar. Talablarga javob bermaydigan maqolalar to‘plamga kiritilmaydi. Tashkiliy qo‘mita maqola matnini qisqartirish, qisman tuzatish kiritish, seksiyalarga joylashtirish huquqiga ega.

ISSN 3030-3907

ANALYZING THE CONCEPT AND COMPONENTS OF CYBER HYGIENE IN THE CONTEXT OF EDUCATIONAL INSTITUTIONS: USER BEHAVIOR, SECURITY AWARENESS, AND BEST PRACTICES IN UZBEKISTAN.

Omonov Odiljon Mirzaulug‘bek o‘g‘li
Sharda University Uzbekistan, Magistr talabasi
E-mail: odiljonqwerty1114@gmail.com

Annotatsiya. Ta'lim muhitining tezkor raqamlashtirilishi, kibergigienaning institutsional axborot xavfsizligining asosiy komponenti sifatidagi ahamiyatini oshirdi. Ushbu tadqiqot O‘zbekistondagi ta'lim muassasalaridagi kibergigienani o‘rganib, foydalanuvchilarning xatti-harakatlari, xavfsizlik haqida bilim-ko‘nikmalari hamda eng yaxshi amaliyotlarga e'tibor qaratdi. Aralash usullardan foydalangan holda, tadqiqot o‘rta va oliy ta'lim muassasalaridagi 487 respondent orasida kiberxavfsizlik amaliyotlarini baholadi. SPSS yordamida statistik tahlil parollarni boshqarishda sezilarli kamchiliklarni aniqladi, atigi 34,2% kuchli parollardan foydalangan va respondentlarning 62,8% orasida fishing haqida bilimlari cheklanganligi aniqlandi. Natijalar shuni ko‘rsatadiki, asosiy kiberxavfsizlik bilimlari mavjud bo‘lsa-da, amaliy qo‘llanilishi yetarli emas. Ushbu tadqiqot ta'lim muassasalarida kibergigiena madaniyatini oshirish bo‘yicha empirik dalillar va kontekstga xos tavsiyalar berish orqali ta’lim tizimlarida kiberxavfsizlik ta'limiga hissa qo‘shadi.

Kalit so‘zlar: kibergigiena, kiberxavfsizlik haqida xabardorlik, foydalanuvchilarning xatti-harakati, ta'lim muassasalari, axborot xavfsizligi, raqamli savodxonlik.

Аннотация. Быстрая цифровизация образовательной среды повысила важность кибергигиены как фундаментального компонента информационной безопасности учреждений. В данном исследовании рассматривается кибергигиена в образовательных учреждениях Узбекистана, с акцентом на поведение пользователей, осведомленность о безопасности и передовые методы. Используя смешанный метод исследования, были оценены практики кибербезопасности среди 487 респондентов из средних и высших учебных заведений. Статистический анализ с помощью SPSS выявил значительные пробелы в управлении паролями: только 34,2% использовали надежные пароли, а осведомленность о фишинге была ограниченной у 62,8% респондентов. Результаты показывают, что, хотя базовые знания в области кибербезопасности существуют, их практическое применение остается недостаточным. Данное исследование вносит вклад в образование в области кибербезопасности в Центральной Азии, предоставляя эмпирические данные и рекомендации,

ISSN 3030-3907

специфичные для конкретного контекста, по повышению культуры кибергигиены в образовательных учреждениях.

Ключевые слова: кибергигиена, осведомленность о кибербезопасности, поведение пользователей, образовательные учреждения, информационная безопасность, цифровая грамотность.

Abstract. The rapid digitalization of educational environments has heightened the importance of cyber hygiene as a fundamental component of institutional information security. This study examines cyber hygiene within educational institutions in Uzbekistan, focusing on user behavior, security awareness, and best practices. Employing a mixed-methods design, the study assessed cybersecurity practices among 487 respondents across secondary and higher education institutions. Statistical analysis using SPSS revealed significant gaps in password management, with only 34.2% utilizing strong passwords, and limited phishing awareness among 62.8% of respondents. The findings indicate that while basic cybersecurity knowledge exists, practical implementation remains inadequate. This research contributes to cybersecurity education in Central Asia by providing empirical evidence and context-specific recommendations for enhancing cyber hygiene culture in educational settings.

Keywords: cyber hygiene, cybersecurity awareness, user behavior, educational institutions, information security, digital literacy.

1. INTRODUCTION.

Cyber hygiene encompasses the practices and protocols that individuals and organizations employ to maintain digital security. In educational institutions, where diverse user populations interact with complex technological infrastructures, cyber hygiene has emerged as a critical determinant of organizational resilience against cyber threats. The contemporary educational landscape, characterized by widespread adoption of e-learning platforms and bring-your-own-device policies, has substantially expanded the attack surface available to malicious actors.

Educational institutions face distinctive cybersecurity challenges including heterogeneous user populations with varying technical proficiency, limited IT budgets, open network architectures, and the necessity of protecting sensitive student data. Common vulnerabilities include weak password practices, susceptibility to phishing attacks, use of unsecured networks, and inadequate software update procedures.

Despite global recognition of cybersecurity importance in education, empirical research examining cyber hygiene practices in Central Asian contexts remains limited. Uzbekistan, implementing ambitious digital transformation under the Digital Uzbekistan 2030 strategy, presents a compelling case for

ISSN 3030-3907

investigating the intersection of technological modernization and cybersecurity preparedness. This research addresses the critical gap in understanding how cyber hygiene concepts manifest within Uzbekistan's educational sector.

The object of this study comprises the information security environment of educational institutions in Uzbekistan, while the subject encompasses cyber hygiene practices, user behavioral patterns, and security awareness levels. This study contributes original empirical data and context-specific analysis to inform policy development and institutional practice.

2. METHODS.

2.1 Research Design and Sampling

This study employed a mixed-methods research design, integrating quantitative surveys with qualitative analysis. The sampling frame included students, teaching faculty, administrative personnel, and IT staff from secondary schools and higher education institutions. A total of 487 valid responses were collected: 268 students (55.0%), 127 teachers (26.1%), 62 administrative staff (12.7%), and 30 IT professionals (6.2%). Respondents were distributed across urban (72.3%) and regional (27.7%) institutions.

2.2 Data Collection and Analysis

Data collection employed a structured questionnaire adapted from established cybersecurity assessment instruments, translated into Uzbek and Russian. The instrument assessed user behavior (password practices, device security, online habits), security awareness (threat recognition, training exposure), and best practices implementation (policy compliance, software maintenance, access control). Data were analyzed using SPSS version 26.0, with reliability analysis confirming instrument consistency (Cronbach's alpha = 0.847). Correlation analysis examined relationships between awareness levels and behavioral outcomes.

3. RESULTS

3.1 User Behavior Patterns

Password management practices demonstrated substantial room for improvement. Only 34.2% of participants reported using strong passwords, while 41.6% acknowledged password reuse across multiple accounts. Multi-factor authentication adoption remained low at 18.3% among general users, though IT staff demonstrated significantly higher implementation (73.3%). Device security practices varied, with 56.4% reporting regular screen locking and only 29.1% enabling automatic updates.

3.2 Security Awareness and Best Practices

Security awareness assessment revealed moderate baseline knowledge with significant knowledge-action gaps. While 71.4% correctly identified phishing as

ISSN 3030-3907

a common threat, only 38.9% reported confidence in recognizing phishing attempts. Formal cybersecurity training participation was limited, with 67.5% of teachers and 82.1% of students indicating no prior training. Correlation analysis revealed a significant positive relationship between training participation and secure behavior ($r = 0.412$, $p < 0.001$). Institutional best practices showed inconsistent implementation: documented acceptable use policies existed in 54.2% of institutions, while formal incident response procedures existed in only 31.8%.

4. DISCUSSION AND CONCLUSION.

The findings illuminate both the current state and critical gaps in cyber hygiene practices within Uzbekistan's educational institutions. The identified patterns align with global trends indicating that awareness alone does not translate into secure behavior, highlighting the persistent knowledge-action gap documented in cybersecurity research worldwide.

Several strengths merit acknowledgment, including near-universal antivirus adoption and the validated correlation between training and secure behavior. However, significant weaknesses demand attention, particularly low rates of strong password usage, limited multi-factor authentication adoption, and inadequate formal training exposure.

Study limitations include its cross-sectional design and geographic focus on Uzbekistan, potentially limiting generalizability. Future research should examine longitudinal outcomes of intervention programs and explore artificial intelligence-based monitoring systems for enhancing institutional cybersecurity.

In conclusion, cyber hygiene in Uzbekistan's educational institutions requires systematic enhancement across behavioral, awareness, and policy dimensions. Development of comprehensive training programs, implementation of robust institutional policies, and integration of cybersecurity concepts into educational curricula represent essential pathways toward sustainable digital education security. Prioritizing cyber hygiene culture development will prove fundamental to protecting institutional assets and ensuring educational integrity in an increasingly interconnected world.

REFERENCES

1. Cyber Hygiene ENISA. (2024). Cyber Hygiene Practices for Educational Institutions. European Union Agency for Cybersecurity.
2. Cybersecurity Awareness Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2023). Cyber security awareness, knowledge, and behavior in educational environments. Journal of Computer Information Systems, 63(2), 210–224.

ISSN 3030-3907

3. Behavioral Cybersecurity Wash, R., & Cooper, M. M. (2023). Understanding user behavior and cyber hygiene practices in digital environments. Computers & Security, 128, 103157.
4. Educational Cybersecurity Cisco. (2024). Cybersecurity Readiness Index 2024: Education Sector Report. Cisco Security Publications.
5. Security Awareness Training Bada, M., & Nurse, J. R. C. (2024). Developing cybersecurity awareness programs in higher education institutions. Education and Information Technologies, 29(4), 4551–4573.
6. Artificial Intelligence in Cybersecurity Garcia, R., Falkner, K., & Vitale, J. (2023). AI in educational assessment: Opportunities and challenges. Computers and Education: Artificial Intelligence, 4, 100123.
7. Responsible AI Milano, S., McGrane, J. A., & Leonelli, M. (2023). AI and responsible innovation in education. AI & Society, 38(2), 913–925.
8. Academic Integrity Liang, W., Yuksekgonul, M., Mao, Y., Wu, E., & Zou, J. (2023). GPT detectors are biased against non-native English writers. Patterns, 4(7), 100779.
9. Cybersecurity Policies Ministry of Digital Technologies of the Republic of Uzbekistan. (2025). Cybersecurity Strategy for Digital Educational Infrastructure 2025–2030.
10. Educational Information Security Kaspersky. (2024). Cybersecurity in Education: Threat Landscape and Security Awareness Report 2024.
11. Phishing Awareness Hadlington, L., & Murphy, J. (2024). User behavior, phishing susceptibility, and cyber hygiene awareness in academic institutions. Computers & Security, 132, 103412.

ISSN 3030-3907