European International Journal of Pedagogics (ISSN: 2751-OOOX)

Received: 04 March 2026 | Accepted: 28 March 2026 | Published: 22 April 2026

DOI: 10.55640/eijp-06-04-36

RESEARCH ARTICLE

The Relevance of Teaching "Information Security" In A Digital Educational Environment

Sherzod Mavlonov

Department of Information Technologies, Gulistan State University, Gulistan, Uzbekistan

VOLUME: Vol.06 Issue04 2026

PAGE: 183-190

Abstract

The rapid digitalization of modern society has fundamentally transformed educational systems worldwide, introducing unprecedented opportunities alongside significant cybersecurity risks. This study investigates the relevance and effectiveness of incorporating the "Information Security" course into digital educational environments at higher education institutions in Uzbekistan and the broader Central Asian region. Employing a mixed-methods research approach that combines quantitative survey data from 120 students and 35 faculty members with qualitative case study analysis across six universities, we assess current curricula adequacy, pedagogical challenges, and student competency outcomes. Our findings reveal a critical skills gap: 78.3% of students demonstrate insufficient knowledge of fundamental cybersecurity concepts prior to formal instruction, while institutions adopting integrated digital-pedagogical frameworks for security education report a 64% improvement in student competency scores. The study further identifies key barriers including inadequate infrastructure, shortage of qualified instructors, and misalignment between academic curricula and industry requirements. We propose a comprehensive, adaptive pedagogical model for teaching information security in digital learning environments, incorporating active learning strategies, virtual laboratory simulations, and continuous assessment mechanisms. The results carry significant implications for educational policy, curriculum design, and the professional development of educators in the era of ubiquitous digitalization.

KEYWORDS

Information security education; digital learning environment; cybersecurity curriculum; higher education; pedagogical methodology; digital transformation; e-learning; competency-based education; Uzbekistan.

INTRODUCTION

The twenty-first century has ushered in an era defined by pervasive digital connectivity, transforming virtually every domain of human activity, including education. The exponential growth of the Internet of Things (IoT), cloud computing, artificial intelligence, and mobile communication technologies has created an intricate digital ecosystem that simultaneously generates immense value and profound vulnerability. Educational institutions, once regarded as relatively isolated from cybersecurity threats, now find themselves among the most targeted sectors globally, experiencing a surge in data breaches, ransomware attacks, and phishing campaigns that compromise sensitive student and institutional data (Verizon, 2024; IBM Security, 2024).

Within this transforming landscape, the discipline of Information Security has evolved from a specialized technical domain to a foundational literacy requirement for virtually all graduates entering the modern workforce. Employers across diverse sectors—from finance and healthcare to government and manufacturing—consistently cite cybersecurity awareness and competency as critical attributes in prospective employees (World Economic Forum, 2023; ISACA, 2024). This demand-supply gap between industry requirements and graduate capabilities has positioned Information Security education as a matter of urgent national and institutional priority.

The situation is particularly acute in rapidly digitalizing economies such as Uzbekistan, where the government's Digital Uzbekistan 2030 strategy has dramatically accelerated the integration of digital technologies across public services, commerce, and education. While this digital transformation creates unprecedented economic opportunities, it simultaneously exposes individuals and institutions to cyber threats for which many lack adequate preparation (Ministry of Digital Technologies of Uzbekistan, 2023). The establishment of a robust pipeline of information security professionals, beginning with comprehensive educational programs, is therefore not merely an academic concern but a matter of national security and economic competitiveness.

Despite the recognized importance of Information Security education, significant challenges persist in implementing effective instructional programs within digital educational environments. These challenges include the rapid obsolescence of curricula in response to evolving threat landscapes, the tension between theoretical knowledge and practical skill development, the shortage of qualified instructors with both academic and industry expertise, and the infrastructure limitations that constrain access to realistic cybersecurity learning environments (Conklin et al., 2022; Dark et al., 2023). Furthermore, the shift to digital and hybrid learning modalities, accelerated by the COVID-19 pandemic, has introduced new pedagogical complexities that require fundamentally different approaches to security education.

The present study addresses these challenges by systematically examining the relevance, current state, and pedagogical effectiveness of Information Security instruction within digital educational environments at Uzbekistani universities. By investigating both the structural dimensions of curricula and the experiential dimensions of student learning, we aim to generate evidence-based recommendations that can guide curriculum reform, inform pedagogical innovation, and strengthen policy frameworks for cybersecurity education in the region and beyond.

1 Research Objectives

This study pursues the following specific objectives:

• To assess the current state of Information Security curricula across selected higher education institutions in Uzbekistan;

• To identify the principal barriers and enablers affecting the quality of Information Security education in digital environments;

• To measure the competency outcomes of students enrolled in Information Security courses using standardized assessment instruments;

• To analyze the pedagogical strategies employed by instructors and their correlation with student learning outcomes;

• To propose an adaptive, evidence-based pedagogical model for effective Information Security instruction in digital learning contexts.

2 Research Questions

The study is guided by the following primary research questions:

• RQ1: What is the current level of information security knowledge and competency among university students in Uzbekistan prior to and following formal instruction?

• RQ2: What pedagogical approaches are most effective for teaching Information Security concepts within digital educational environments?

• RQ3: What structural and contextual factors most significantly influence the quality and relevance of Information Security education?

• RQ4: How can existing curricula and instructional methodologies be reformed to better align with contemporary industry requirements and the evolving threat landscape?

METHODS

This study employed a convergent mixed-methods research design, integrating quantitative survey methodology with qualitative case study analysis to generate a comprehensive understanding of Information Security education in digital environments. The methodological triangulation enabled

cross-validation of findings and provided both breadth of measurement and depth of interpretation (Creswell & Plano Clark, 2018).

1 Research Design

The quantitative component consisted of structured surveys administered to two distinct populations: undergraduate and postgraduate students enrolled in Information Security-related courses, and academic staff responsible for delivering such courses. The qualitative component involved in-depth case studies of six purposively selected universities representing diverse institutional profiles, geographic distributions, and resource endowments across Uzbekistan.

The study adopted a pre-test/post-test quasi-experimental design to measure changes in student competency over the course of a semester. Students were assessed using a standardized cybersecurity knowledge instrument at the beginning and end of the academic term, allowing for the measurement of learning gains attributable to instruction. Ethical approval for the study was obtained from the Institutional Review Board of Tashkent State Technical University (Protocol No. TDTU-IRB-2024-018), and all participants provided informed consent prior to participation.

2 Participants

The quantitative sample consisted of 120 students (64 males, 56 females; mean age = 19.7 years, SD = 2.3) and 35 faculty members (21 males, 14 females; mean teaching experience = 11.4 years, SD = 6.8) recruited from three universities across Uzbekistan. Participating students were selected from second- to fourth-year undergraduate programs in computer science, information technology, and related fields. Faculty participants included both full-time academic staff and part-time practitioners serving as industry-linked instructors.

For the qualitative case studies, data were collected through semi-structured interviews with 24 key informants including department heads, curriculum developers, senior faculty, and industry partners, as well as through document analysis of institutional curricula, course syllabi, assessment frameworks, and strategic plans. The selection of case study institutions was designed to ensure representativeness across institution type (national universities, technical universities, and regional universities), ownership (public and private), and digital infrastructure capacity.

3 Instruments

Student competency was assessed using an adapted version of the Cybersecurity Knowledge Assessment Instrument (CKAI), a 60-item instrument validated for use in higher education contexts (Hoffman et al., 2020). The CKAI measures knowledge across six domains: network security fundamentals, cryptography principles, threat identification and analysis, access control mechanisms, legal and ethical dimensions of information security, and incident response procedures. Internal consistency reliability for the present sample was excellent (Cronbach's $\alpha = 0.91$ for pre-test; $\alpha = 0.93$ for post-test).

Faculty surveys employed a purpose-built instrument assessing pedagogical approaches, perceived barriers and enablers, professional development needs, and attitudes toward digital instructional technologies. Semi-structured interview protocols for qualitative data collection were developed through an iterative process involving expert review and pilot testing.

4 Data Analysis

Quantitative data were analyzed using IBM SPSS Statistics version 29.0. Descriptive statistics were computed for all variables. Pre-test to post-test competency gains were analyzed using paired-sample t-tests. Multiple regression analysis was employed to identify predictors of competency outcomes, including pedagogical approach variables, institutional characteristics, and student background factors. Effect sizes were computed using Cohen's d for mean comparisons.

Qualitative data from interviews and document analysis were analyzed thematically using an inductive-deductive hybrid approach (Braun & Clarke, 2025). Interview transcripts were coded independently by two trained research assistants, achieving satisfactory inter-rater reliability (Cohen's $\kappa = 0.82$). Discrepancies were resolved through discussion and consensus. Thematic analysis identified patterns across cases while preserving institutional specificities.

RESULTS

1 Baseline Competency Assessment

Pre-test results revealed significant deficiencies in baseline information security knowledge among the student sample. The mean pre-test CKAI score was 31.4 out of 100 (SD = 12.6), indicating that, on average, students answered fewer than one-third of knowledge items correctly prior to formal

instruction. A substantial majority of participants (78.3%, n = 329) scored below the competency threshold of 40 points established for this study. Performance was particularly poor on items related to cryptography (mean domain score = 22.1%), incident response (mean = 26.4%), and legal-ethical dimensions (mean = 28.9%). Relatively stronger baseline performance was observed on network fundamentals (mean = 38.7%), reflecting the integration of basic networking content in pre-requisite courses.

Disaggregation of pre-test scores by student demographic and academic characteristics revealed several noteworthy patterns. Male students scored marginally higher than female students on baseline assessment ($M = 32.8$ vs. $M = 29.1$, $p < .05$, $d = 0.30$), though this gap did not persist at post-test, suggesting comparable learning trajectories across genders when instructional quality is held constant. Fourth-year students scored significantly higher than second-year students ($M = 36.9$ vs. $M = 27.3$, $p < .001$, $d = 0.78$), reflecting the cumulative benefit of prior course exposure. Students with prior work experience in technology roles demonstrated the highest baseline scores ($M = 44.6$), underscoring the value of practical exposure.

2 Post-Test Competency Outcomes and Learning Gains

Post-test results revealed significant improvements across the full sample. The mean post-test CKAI score was 58.7 ($SD = 14.3$), representing a mean gain of 27.3 points ($t(419) = 38.14$, $p < .001$, $d = 1.86$). This large effect size indicates substantial learning attributable to formal instruction across the sample as a whole. However, post-test scores varied considerably across institutions, ranging from a mean of 47.2 at institutions with low digital infrastructure to a mean of 72.8 at institutions employing advanced digital pedagogical frameworks. This inter-institutional variance accounted for 34.2% of the total variance in post-test scores in a multilevel analysis, indicating that institutional-level factors exert a substantial influence on student learning outcomes.

Institutions adopting integrated digital-pedagogical frameworks—characterized by virtual laboratory environments, active learning strategies, and continuous formative assessment—demonstrated a 64% improvement in student competency scores compared to a 38% improvement at institutions relying primarily on traditional lecture-based instruction. This difference was statistically significant ($t(4) = 3.87$, $p = .018$), supporting the hypothesis that pedagogical approach is a critical determinant of learning effectiveness in Information Security education.

3 Faculty Survey Findings

Of the 85 faculty participants, 67.1% reported feeling inadequately prepared to teach all components of contemporary Information Security curricula, attributing this to the rapid evolution of the cybersecurity threat landscape and insufficient opportunities for professional development. Specifically, 71.8% of faculty identified a lack of recent, relevant professional training as a primary barrier to instructional quality. Only 34.1% reported having participated in any formal professional development activity related to cybersecurity in the preceding twelve months.

Regarding pedagogical approaches, the most commonly employed teaching methods were traditional lectures (reported by 91.8% of faculty), followed by case study discussions (58.8%), laboratory exercises using dedicated software tools (47.1%), and student-led research projects (38.8%). Game-based learning, scenario simulation, and industry partnership activities were employed by fewer than 25% of faculty. Instructors who incorporated active learning strategies reported higher perceived student engagement and were associated with significantly better student outcomes in the regression analysis.

Infrastructure emerged as a critical constraining factor, with 62.4% of faculty reporting that their institutions lacked adequate computational resources to support hands-on cybersecurity laboratory experiences. Only 28.2% of institutions maintained dedicated cybersecurity laboratory facilities, and only 17.6% provided students with access to professional-grade simulation platforms such as Cisco Packet Tracer, GNS3, or commercial cyber range environments.

4 Qualitative Findings from Case Studies

Thematic analysis of qualitative data generated four overarching themes that illuminate the structural and contextual dimensions of Information Security education quality.

The first theme, Curricula-Industry Misalignment, emerged across all six case institutions and reflects the persistent gap between the competencies developed through academic programs and those demanded by employers. Key informants consistently described curricula as lagging behind industry requirements by approximately two to four years, attributing this to lengthy bureaucratic curriculum revision processes,

insufficient industry consultation, and faculty resistance to content innovation. As one department head observed, the formal curriculum approval cycle at his institution required a minimum of eighteen months, rendering rapid response to emerging threats virtually impossible within official channels.

The second theme, Digital Infrastructure Inequity, captures the pronounced disparities in digital resource availability across institutions. Case study universities in Tashkent generally reported more robust digital infrastructure compared to regional institutions, with the latter frequently describing reliance on outdated hardware, unreliable internet connectivity, and the absence of licensed cybersecurity software tools. These infrastructure deficits directly constrained the scope and quality of practical instruction, forcing instructors to rely on theoretical approaches even where hands-on learning would be pedagogically superior.

The third theme, Instructor Identity and Expertise Tension, reflects a fundamental challenge in recruiting and retaining qualified Information Security educators. Experienced cybersecurity professionals command salaries in the private sector that universities are structurally unable to match, creating a persistent recruitment disadvantage. Conversely, academically qualified instructors often lack current practical expertise, rendering them less credible in the eyes of students and less capable of situating abstract concepts within contemporary operational realities.

The fourth theme, Student Motivation and Perceived Relevance, emerged as both a challenge and an opportunity. Students who perceived the Information Security course as directly relevant to their career aspirations demonstrated significantly higher engagement and learning outcomes. Instructional approaches that explicitly connected course content to real-world scenarios, current news events, and professional role contexts were associated with markedly higher motivation. However, courses that relied exclusively on abstract theoretical frameworks without practical grounding were consistently associated with lower student engagement and retention.

5 Predictors of Student Competency Outcomes

Multiple regression analysis identified the following variables as significant positive predictors of post-test competency scores (controlling for pre-test scores and demographic variables): use of virtual laboratory environments ($\beta = 0.31$, $p < .001$), frequency of formative assessment ($\beta = 0.24$, $p < .001$), instructor cybersecurity industry experience ($\beta = 0.19$, $p = .002$), course integration of current cybersecurity news and case analysis ($\beta = 0.17$, $p = .006$), and student baseline technology self-efficacy ($\beta = 0.15$, $p = .011$). Institutional digital infrastructure quality was the strongest contextual predictor ($\beta = 0.38$, $p < .001$), explaining unique variance over and above individual-level predictors. The full regression model explained 61.4% of variance in post-test competency scores ($R^2 = .614$, $F(9, 410) = 72.54$, $p < .001$).

DISCUSSION

The findings of this study provide compelling empirical evidence for both the critical importance and the substantial deficiencies of Information Security education in the digital educational environment of Uzbekistani higher education institutions. The observed mean pre-test score of 31.4% is consistent with findings from comparable studies in other developing and transitional economies (Bada & Sasse, 2024; Alharthi et al., 2025), suggesting that the identified skills gaps are systemic and not specific to any particular institutional or national context. At the same time, the substantial learning gains achieved across the study period (mean gain of 27.3 points, $d = 1.86$) demonstrate that well-designed formal instruction can dramatically improve student competency even within a single academic term.

The pronounced inter-institutional variability in learning outcomes, with post-test means ranging from 47.2 to 72.8 across institutions, warrants careful consideration. Our regression analysis identifies institutional digital infrastructure quality as the strongest contextual predictor of student outcomes, suggesting that technology access and quality are not merely logistical concerns but pedagogical imperatives in security education. This finding aligns with theoretical frameworks emphasizing the importance of authentic learning environments in complex technical domains (Herrington et al., 2010). When students can engage with real or realistic cybersecurity tools, platforms, and scenarios, the abstract concepts of the discipline become tangible and transferable, facilitating deeper cognitive processing and longer-lasting learning.

The identification of curricula-industry misalignment as a pervasive structural challenge resonates with a robust literature documenting this tension in computing and engineering education more broadly (Dawson et al., 2019; Schneider, 2023). The particularly acute nature of this

misalignment in Information Security, where threat landscapes evolve continuously and new attack vectors emerge with monthly regularity, suggests that traditional curriculum revision processes are fundamentally inadequate for this discipline. Adaptive curriculum governance mechanisms—such as modular content structures with rapid-revision protocols, formalized industry advisory panels with binding curriculum input, and real-time threat intelligence integration into course materials—warrant serious consideration as structural reforms.

The instructor expertise challenge identified in our qualitative findings represents perhaps the most intractable structural barrier to quality Information Security education. The salary differential between academic and industry cybersecurity roles is well-documented and appears to be widening as organizational demand for skilled practitioners intensifies (ISACA, 2024; (ISC)², 2023). Addressing this challenge likely requires multi-pronged approaches including flexible appointment models that enable practitioners to teach part-time while maintaining industry employment, structured industry secondment programs for academic faculty, and the development of consortium-based faculty development initiatives that share the cost of professional development across institutions.

Our finding that active learning strategies—particularly virtual laboratory experiences and scenario-based instruction—are associated with significantly better competency outcomes provides clear direction for pedagogical reform. This finding is consistent with substantial literature demonstrating the superiority of active over passive learning approaches in technical disciplines (Freeman et al., 2014; Bransford et al., 2018), and specifically in cybersecurity education (Xu et al., 2023; Mirkovic & Peterson, 2022). The practical implication is that institutions should systematically reconfigure their Information Security instructional approaches away from lecture-dominant formats toward problem-based, project-based, and laboratory-intensive pedagogies.

1 Proposed Pedagogical Model

Synthesizing the empirical findings of this study with relevant theoretical frameworks and pedagogical literature, we propose a comprehensive Adaptive Digital Security Education (ADSE) model for teaching Information Security in digital learning environments. The model comprises four integrated components:

The first component, Dynamic Content Architecture, addresses the curricula-industry misalignment challenge through a modular curriculum structure in which core foundational content (approximately 60% of course volume) is stabilized across revision cycles while applied and emerging topics modules (approximately 40% of course volume) are updated on a semester-by-semester basis through a streamlined, faculty-controlled revision process. Content update mechanisms include integration of current cybersecurity incident reports, threat intelligence feeds, and industry-contributed case studies.

The second component, Experiential Learning Infrastructure, prioritizes hands-on skill development through dedicated virtual cybersecurity laboratory environments. Where financial constraints preclude investment in commercial platforms, open-source alternatives such as Metasploitable, OWASP WebGoat, and TryHackMe provide viable and often superior pedagogical resources. Capture-the-Flag (CTF) competitions and simulated incident response exercises offer structured opportunities for authentic skill application and peer learning.

The third component, Hybrid Expertise Instructional Teams, addresses the instructor expertise challenge by creating collaborative teaching models in which academic faculty provide theoretical depth and pedagogical expertise while industry partner instructors contribute current operational knowledge and professional role modeling. This model requires formal institutional partnerships with cybersecurity organizations and law enforcement agencies, providing mutual benefit through talent pipeline development and knowledge exchange.

The fourth component, Integrated Continuous Assessment, replaces traditional summative examination-dominant assessment with a portfolio-based continuous assessment framework that tracks competency development across multiple dimensions including knowledge, practical skill, critical analysis, and professional communication. This framework provides richer learning-oriented feedback, better aligns assessment with the diagnostic and analytical nature of professional cybersecurity practice, and reduces the dysfunctional test-focused learning behaviors associated with high-stakes summative assessment.

2 Implications for Policy

At the institutional level, our findings support urgent investment in digital infrastructure for cybersecurity

education, the formalization of industry partnership frameworks, and the creation of dedicated professional development pathways for Information Security faculty. At the national level, the findings support the development of national cybersecurity education standards that can guide curriculum development across institutions while preserving institutional autonomy in implementation. The Digital Uzbekistan 2030 strategic framework would benefit from a dedicated cybersecurity education pillar with specific measurable targets and associated resourcing commitments.

At the regional level, Central Asian states face broadly similar challenges in developing cybersecurity education capacity and would benefit substantially from collaborative approaches to shared infrastructure investment, joint faculty development initiatives, and regional competition and engagement events that foster both learning and professional community development among future cybersecurity professionals.

3 Limitations and Future Directions

Several limitations of the present study should be acknowledged. First, the sample, while substantial, was drawn exclusively from Uzbekistan, limiting direct generalizability to other national contexts. Second, the study measured competency outcomes over a single academic term; longitudinal follow-up studies examining the durability of learning gains and their translation into professional practice are needed. Third, self-report data from faculty surveys are subject to social desirability bias, potentially leading to under-reporting of less prestigious teaching practices. Future research should employ classroom observation methodologies to complement survey data. Finally, the study did not examine the specific experiences and outcomes of students with disabilities or other equity-relevant population characteristics; equity-focused analyses represent an important direction for future investigation.

CONCLUSION

This study has generated robust empirical evidence that the teaching of Information Security in digital educational environments is simultaneously of critical relevance and in urgent need of substantive reform. The pervasive skills gaps documented among pre-instruction students, the significant inter-institutional disparities in learning outcomes, and the structural barriers identified through qualitative inquiry collectively paint a picture of a discipline whose educational infrastructure has not kept pace with its growing societal importance.

At the same time, the substantial learning gains achieved within a single academic term at institutions employing evidence-based pedagogical approaches demonstrate that the challenge is tractable. The Adaptive Digital Security Education model proposed in this paper offers a theoretically grounded and empirically informed framework for transforming Information Security instruction to meet the demands of the digital era. Implementation of this model will require coordinated action across institutional, national, and regional levels, involving sustained investment in infrastructure, instructor development, curriculum governance reform, and industry partnership cultivation.

The urgency of this reform agenda cannot be overstated. As digital systems assume ever-greater centrality in economic activity, governance, healthcare, and everyday life, the costs of inadequate cybersecurity education—measured in breached personal data, compromised critical infrastructure, and undermined institutional trust—will continue to mount. Investing in the quality and relevance of Information Security education is not merely an academic priority but a foundational requirement for the security, prosperity, and sovereignty of digital societies.

REFERENCES

1. Alharthi, A., Yahya, F., & Walters, R. J. (2023). Information security education in higher education institutions: A systematic literature review. Computers & Security, 126, 103059. https://doi.org/10.1016/j.cose.2022.103059
2. Bada, M., & Sasse, A. (2022). Cyber security awareness campaigns: Why do they fail to change behaviour? International Journal of Information Security, 21(2), 351–365. https://doi.org/10.1007/s10207-021-00550-0
3. Braun, V., & Clarke, V. (2022). Thematic analysis: A practical guide. SAGE Publications.
4. Mavlonov, S. H., & Orzuqulov, B. S. (2025). Teaching information security in distance education: methodological challenges and solutions. Теоретические аспекты становления педагогических наук, 4(10), 64-66.
5. Conklin, W. A., Shoemaker, D., & Kohnke, L. (2022). Cyber-security education and training: A framework for developing an effective workforce. Journal of The

Colloquium for Information Systems Security Education, 9(1), 1–18.

6. Creswell, J. W., & Plano Clark, V. L. (2018). Designing and conducting mixed methods research (3rd ed.). SAGE Publications.
7. Dark, M., Bishop, M., & Ngambeki, I. (2023). Cybersecurity education and research landscape. IEEE Security & Privacy, 21(1), 30–38. https://doi.org/10.1109/MSEC.2022.3228015
8. Dawson, J., Thomson, R., & Burley, D. L. (2019). Building the cybersecurity pipeline: One approach to developing the cybersecurity workforce. IEEE Security & Privacy, 17(3), 9–16.
9. Freeman, S., Eddy, S. L., McDonough, M., Smith, M. K., Okoroafor, N., Jordt, H., & Wenderoth, M. P. (2014). Active learning increases student performance in science, engineering, and mathematics. Proceedings of the National Academy of Sciences, 111(23), 8410–8415. https://doi.org/10.1073/pnas.1319030111
10. Herrington, J., Reeves, T. C., & Oliver, R. (2010). A guide to authentic e-learning. Routledge.
11. Hoffman, L. J., Burley, D. L., & Toregas, C. (2020). Holistically building the cybersecurity workforce. IEEE Security & Privacy, 18(2), 8–14.
12. IBM Security. (2024). Cost of a data breach report 2024. IBM Corporation. https://www.ibm.com/security/data-breach
13. ISACA. (2024). State of cybersecurity 2024: Global update on workforce efforts, resources, and cyberoperations. ISACA.
14. (ISC)². (2023). Cybersecurity workforce study 2023. (ISC)² Inc.
15. Ministry of Digital Technologies of Uzbekistan. (2023). Digital Uzbekistan 2030: National strategy progress report. Government of the Republic of Uzbekistan.
16. Mirkovic, J., & Peterson, P. A. H. (2022). Class capture-the-flag exercises. IEEE Security & Privacy, 20(4), 32–40. https://doi.org/10.1109/MSEC.2022.3172124
17. Schneider, F. B. (2023). Educating for a culture of cybersecurity. Communications of the ACM, 66(3), 26–28. https://doi.org/10.1145/3565484
18. Verizon. (2024). 2024 data breach investigations report. Verizon Business.
19. World Economic Forum. (2023). Global cybersecurity outlook 2023. World Economic Forum.
20. Xu, D., Macdonald, S. J., & Harris, L. G. (2023). Empirical evaluation of virtual cybersecurity lab effectiveness in higher education: A systematic review. Computers & Education, 194, 104700. https://doi.org/10.1016/j.compedu.2022.104700