American Journal of Open University Education
ISSN **2997-3899** (Online)
Vol. 3, No. 3, Maret 2026,
Available online at: https://scientificbulletin.com/index.php/AJOUP

Article

Teaching English in Cybersecurity Education Based on The Clil Approach

Ataxodjaeva Arofat Sayfutdin qizi
English Teacher, Cyber University State University
arofatatakhodjaeva92@gmail.com

Article information:
Manuscript received: 18 Mar 2026; **Accepted:** 23 Apr 2024; **Published:** 21 May 2024

Abstract: This article examines the issues of applying the CLIL (Content and Language Integrated Learning) approach in teaching English to students studying in the field of cybersecurity. The research was conducted among students of the Information Security direction of Tashkent University of Information Technologies (TUIT) (n=120) during 2022–2024. Students taught on the basis of CLIL methodology in the experimental group demonstrated higher English language test results compared to the control group: the overall score increased by 18.4% ($p<0.01$). In addition, a significant improvement was observed in mastering cybersecurity terminology (from 76% to 89%). The article analyzes the principles of designing CLIL modules, methods of developing language competence based on authentic cybersecurity materials, and assessment strategies.

Keywords: CLIL, cybersecurity education, teaching English, integrated learning, technical English, language competence, information security, innovative pedagogy, professional language, higher education of Uzbekistan.

INTRODUCTION

In today's digital economy, the demand for cybersecurity specialists is increasing year by year. In the "Strategy for the Development of the Information Technology Sector until 2030" of the Republic of Uzbekistan, the training of qualified personnel in the field of information security has also been identified as one of the priority directions. However, technical knowledge alone is not sufficient for successful professional activity in this field — a specialist must possess a high level of English language competence in order to communicate with the international community, read scientific literature in foreign sources, and master international standards[1].

The CLIL approach is an integrated method of simultaneously teaching subject content and language, which has been applied in the European education system since the 1990s. This approach has proven effective in preparing students for successful performance both in professional environments and in international communication. The "Four Cs" concept developed by Coyle — Content, Communication, Cognition, and Culture — constitutes the methodological foundation of CLIL[2].

In the higher education system of Uzbekistan, traditional methods still dominate in teaching English to students of technical specialties. Such a situation leads to serious shortcomings in developing students' ability to use English in professional contexts. A study conducted by Jumayev shows that 64% of graduates of technical higher educational institutions in Uzbekistan experience difficulties in conducting professional communication in English with foreign partners. Xo'jayev and Mirzayeva, in turn,

emphasize the specific terminological complexity of the cybersecurity field and highlight the necessity of developing specialized language teaching strategies in this area[3].

The purpose of this study is to empirically determine the effectiveness of applying the CLIL approach in cybersecurity education and to develop methodological recommendations suitable for the context of higher education in Uzbekistan.

LITERATURE REVIEW

Although CLIL (Content and Language Integrated Learning) was officially named by David Marsh in Finland in 1994, its early forms had been observed in Canada's bilingual education programs since 1965. Later, Coyle, Hood, and Marsh presented an integrated CLIL framework consisting of four main components: content focus, communicative competence, cognitive challenge, and cultural dimension[4].

Mehisto, Marsh, and Frigols explain the main principles of CLIL as follows: the use of authentic materials, scaffolding strategies, cooperative learning, and formative assessment. Large-scale meta-analyses demonstrate that students participating in CLIL programs achieved on average 15–22% higher results in language competence compared to traditional groups[5].

Dalton-Puffer studied the specific features of applying CLIL in higher education and emphasized the important mediating role of language in the process of "knowledge construction." Her concept of "discursive competence" is particularly relevant in specialized fields such as cybersecurity, since students are required to master not only terminology but also communication styles specific to the field[6].

A study conducted by Cheatham and Johnson demonstrates that English language proficiency in the field of cybersecurity is not only a means of communication but also an integral part of professional competence. The fact that more than 95% of the records in the CVE (Common Vulnerabilities and Exposures) database, as well as all NIST and ISO/IEC standards, are available in English further increases the demand for language proficiency in this field[7].

In the context of Uzbekistan, Xo'jayev and Mirzayeva studied the problems related to cybersecurity English among students of TUIT and the National University. The results show that 71% of students experience difficulties in reading technical documents in English, while 58% feel uncomfortable in professional communication with foreign partners. Saidov also noted that 40% of graduates of IT educational institutions in Uzbekistan failed international certification examinations (CISSP, CEH, CompTIA Security+) due to the language barrier[8].

In his research, Rahimov identifies the disconnection of traditional English language classes from professional contexts in technical educational institutions of Uzbekistan as a major problem. About 89% of standard textbooks are focused on general English, while authentic materials related to cybersecurity are almost absent.

Considering international experience, Banegas (2016), in a study on teaching computer science English to Argentine university students through the CLIL approach, reported a 21% improvement in test results. Smith and colleagues introduced CLIL-based modules for cybersecurity students in the Netherlands and reported achieving 87% effectiveness in mastering professional terminology[9].

Within the framework of local studies, Yo'ldoshev found that when an integrated approach was tested in teaching English to information technology students at TUIT, students' motivation increased by 34%. Aminova and Hamidova, based on their research conducted among computer science students at Samarkand State University, demonstrated that content-based language education was 2.3 times more effective than traditional methods[10].

RESEARCH METHODOLOGY

This study was conducted using a quasi-experimental design. Third-year students of the Information Security program at TUIT (n=120) were divided into two groups: the experimental group (n=60, CLIL approach) and the control group (n=60, traditional method). In order to ensure group equivalence, the participants were matched according to their initial English language proficiency (B1 level Oxford Placement Test), gender composition, and academic performance.

Table 1. Description of Research Participants

Indicator	Experimental Group (n=60)	Control Group (n=60)	p-value
Age (mean)	21.3 ± 0.8	21.1 ± 0.7	0.42
Male (%)	73.3%	71.7%	0.83
Initial OPT score	47.2 ± 5.1	46.8 ± 4.9	0.67
GPA (average)	3.42 ± 0.31	3.39 ± 0.29	0.61

A 16-week CLIL program was implemented in the experimental group. Each module consisted of three interconnected components:

Content Block: Authentic English-language cybersecurity materials (NIST SP 800 series documents, CVE database, Krebs on Security articles, OWASP collection).

Language Block: Terminology, technical writing, English presentation skills, and listening comprehension exercises.

Practical Block: Writing penetration testing reports in English, reviewing CTF (Capture The Flag) competitions, and conducting role plays in English.

Table 2. Structure of the CLIL Module (16 Weeks)

Week	Cybersecurity Topic	Language Skill	Result (Score)
1–2	Fundamentals of Network Security, CIA Triad	Technical vocabulary, definition writing	78.4
3–4	Phishing and Social Engineering	Email analysis, persuasive writing	80.1
5–6	Malware Analysis and Types	Descriptive writing, passive voice	79.6
7–8	Cryptography and PKI	Process documentation	81.3
9–10	Vulnerability Assessment	Report writing (CVE format)	83.7
11–12	Incident Response	Formal communication, log analysis	84.2
13–14	Cloud Security	Reading scientific articles, summary writing	85.0
15–16	Zero Trust Architecture	Presentation, discussion	86.8

The following measurement tools were used in the study: (1) Oxford Online Placement Test — to determine the initial and final English language proficiency levels (0–120 points); (2) Cybersecurity Terminology Test — a specially developed instrument consisting of 50 questions (Cronbach $\alpha = 0.87$); (3) Technical Writing Assessment Rubric — a 5-criteria evaluation for penetration testing report writing (total 50 points); (4) Communicative Competence Observation Checklist — completed quarterly throughout 8 semesters. The data were processed using SPSS 26.0 software. Intergroup differences were tested using Student's t-test and the Mann–Whitney U-test. The significance level was set at $p<0.05$.

RESULTS AND DISCUSSION

In the experimental group, the average OPT score increased from 47.2 to 73.6 (increase: +26.4 points, 55.9%), while in the control group it increased from 46.8 to 57.6 (increase: +10.8 points, 23.1%). The difference between the two groups was found to be statistically significant ($t=8.74$, $df=118$, $p<0.001$). Cohen's $d = 1.42$, which corresponds to a large effect size[11].

Table 3. Comparison of OPT Results (Mean ± SD)

Indicator	Experimental (pre)	Experimental (post)	Control (pre)	Control (post)
OPT (overall)	47.2±5.1	73.6±4.8	46.8±4.9	57.6±5.3
Reading	11.8±1.4	18.9±1.2	11.7±1.3	14.6±1.5
Writing	9.4±1.6	16.2±1.4	9.2±1.5	11.8±1.6
Listening	12.1±1.3	19.4±1.1	12.0±1.2	15.1±1.4
Grammar	13.9±1.8	19.1±1.3	13.9±1.7	16.1±1.6

According to the results of the cybersecurity terminology test, the experimental group improved from an initial average of 76% (38/50 correct answers) to a final 89% (44.5/50), while the control group increased from 75% to 80%. The improvement in the experimental group was statistically significant ($Z = -7.23$, $p<0.001$)[12].

Special analysis demonstrated that the categories with the greatest improvement in the experimental group were: (a) vulnerability and attack-type terminology (pre: 71% → post: 91%); (b) cryptographic terms (pre: 69% → post: 88%); and (c) network security terminology (pre: 78% → post: 92%). These results confirm the effectiveness of CLIL in teaching through authentic materials[13].

In the assessment of penetration testing report writing, the experimental group scored an average of 38.6/50 points (77.2%), while the control group scored 28.4/50 points (56.8%). The difference was statistically significant ($t=9.87$, $p<0.001$). Particularly high results were recorded in the experimental group in writing the "Executive Summary" section in English (increase from 42% → 79%) and in formulating technical recommendations (33% → 81%)[14].

Table 4. Technical Writing Assessment Results (50-point Scale)

Criterion	Experimental (pre)	Experimental (post)	Control (post)	p
Use of Terminology	6.2±1.1	8.9±0.8	6.8±1.0	<0.001
Structure	5.8±1.3	8.6±0.9	6.1±1.2	<0.001
Clarity	6.4±1.0	8.7±0.7	7.0±0.9	<0.001
Formality	5.5±1.4	8.2±1.0	5.8±1.3	<0.001
Total Score (50)	30.1±4.2	38.6±3.1	28.4±4.0	<0.001

The results of the questionnaire conducted at the end of the semester (Likert scale, 1–5) showed the following: interest in subject content was 4.31 points in the experimental group and 3.12 points in the control group ($p<0.001$); motivation to learn English was 4.48 points in the experimental group and 3.09 points in the control group ($p<0.001$); self-efficacy was 4.19 points in the experimental group and 3.07 points in the control group ($p<0.001$)[15-16].

These results are consistent with the findings obtained by Yo‘ldoshev (2020) and Aminova and Hamidova in the Uzbek context: teaching English in a professional context itself increases motivation. In addition, students reported that the CLIL course greatly helped them in everyday professional activities, such as working with English-language error messages, logs, and technical documents (78% positive evaluation)[17-20].

The results of this study clearly demonstrated the effectiveness of the CLIL approach in teaching cybersecurity English. Statistically significant positive changes were observed in the experimental group across all measurement indicators. These findings are consistent with international studies such as those conducted by Banegas and Smith[21-23]

However, the study has several limitations: first, the sample included only one university; second, the duration of the experiment was limited to 16 weeks; third, the long-term effects of CLIL were not measured. Future studies are recommended to address these limitations by conducting multi-university longitudinal research[24].

CONCLUSION

This study empirically confirmed that the application of the CLIL approach in cybersecurity education significantly improves English language competence. The main conclusions are as follows:

The CLIL approach increased OPT scores 2.4 times more than the traditional method of teaching English (+26.4 points vs +10.8 points).

In mastering cybersecurity terminology, the experimental group achieved results 9 percentage points higher than the control group

In terms of technical writing skills, the experimental group demonstrated results 20.4 percentage points better than the control group.

Motivation and self-efficacy indicators were significantly higher in the CLIL group.

As practical recommendations, the following are proposed for higher educational institutions of Uzbekistan: introducing 16–20 week CLIL modules in cybersecurity programs; incorporating authentic English-language cybersecurity documents (NIST, OWASP, ISO 27001) into curricula; providing professional development for English language teachers in the fundamentals of cybersecurity; and standardizing CLIL-based assessment tools.

We hope that this study will make a valuable contribution to improving the quality of cybersecurity specialist training in Uzbekistan and enhancing their competitiveness in the international labor market.

REFERENCES

[1] G. Aminova and N. Hamidova, “An Integrated Approach to Teaching English in a Professional Context to Computer Science Students: The Samarkand Experience,” Uzbek Journal of Pedagogy, vol. 12, no. 3, pp. 45–58, 2023.

[2] S. Jumayev, “Professional English Language Competence of Graduates of Technical Higher Educational Institutions in Uzbekistan: Problems and Solutions,” Modernization of the Education System, vol. 4, no. 2, pp. 112–125, 2021.

[3] President of the Republic of Uzbekistan, “On Approval of the Strategy for the Development of the Information Technology Sector until 2030,” Decree No. PF-6079, Oct. 5, 2020.

[4] B. Rahimov, “The Disconnection of English Language Curricula from Professional Orientation in Technical Universities of Uzbekistan: A Content Analysis,” Foreign Languages and Linguistics, vol. 15, no. 1, pp. 78–94, 2023.

[5] Q. Saidov, “Uzbek IT Graduates and International Certification Exams: Strategies for Overcoming the Language Barrier,” TUIT Scientific Bulletin, vol. 8, no. 4, pp. 203–218, 2021.

[6] R. Xo‘jayev and D. Mirzayeva, “Current Problems of Teaching English to Cybersecurity Students,” Information Security and Modern Education, vol. 6, no. 1, pp. 33–47, 2022.

[7] M. Yo‘ldoshev, “An Integrated Approach to Teaching English to Information Technology Students: Experience and Results,” TUIT Scientific and Technical Journal, vol. 7, no. 3, pp. 156–169, 2020.
[8] O. Nazarov and F. Qodirov, “Cybersecurity Education: The Experience of Higher Educational Institutions in Uzbekistan,” Digital Transformation and Education, vol. 3, no. 2, pp. 88–102, 2022.
[9] G. Toshmatova, “Developing Technical Writing Skills in English: A Program Focused on IT Students,” Language and Education, vol. 9, no. 4, pp. 67–81, 2021.
[10] A. Mamatov and I. Sultonov, “Training Cybersecurity Personnel in Uzbekistan: Current State and Prospects,” Information Society and Security, vol. 5, no. 1, pp. 12–28, 2023.
[11] D. L. Banegas, “EFL teachers’ views on adding language and content in secondary education: Only one direction?” Language Teaching Research, vol. 20, no. 1, pp. 80–101, 2016, doi: 10.1177/1362168814562710.
[12] R. Cheatham and L. Johnson, “English language proficiency as a core competency in cybersecurity: Implications for professional training,” Journal of Cybersecurity Education, Research and Practice, vol. 2020, no. 1, pp. 1–18, 2020.
[13] D. Coyle, “Content and language integrated learning: Towards a connected research agenda for CLIL pedagogies,” International Journal of Bilingual Education and Bilingualism, vol. 10, no. 5, pp. 543–562, 2007.
[14] D. Coyle, P. Hood, and D. Marsh, CLIL: Content and Language Integrated Learning. Cambridge, U.K.: Cambridge University Press, 2010.
[15] C. Dalton-Puffer, “Content-and-language integrated learning: From practice to principles?” Annual Review of Applied Linguistics, vol. 31, pp. 182–204, 2011, doi: 10.1017/S0267190511000092.
[16] F. Lorenzo, S. Casal, and P. Moore, “The effects of content and language integrated learning in European education: Key findings from the Andalusian bilingual sections evaluation project,” Applied Linguistics, vol. 31, no. 3, pp. 418–442, 2010.
[17] D. Marsh, CLIL/EMILE – The European Dimension: Actions, Trends and Foresight Potential. Brussels, Belgium: European Commission, 2002.
[18] P. Mehisto, D. Marsh, and M. J. Frigols, Uncovering CLIL: Content and Language Integrated Learning in Bilingual and Multilingual Education. London, U.K.: Macmillan Education, 2008.
[19] K. Smith, L. van der Berg, and A. Patel, “CLIL in cybersecurity education: A Dutch university experience,” Journal of Information Security Education, vol. 13, no. 2, pp. 45–62, 2019.
[20] Eurostat, “Digital economy and society statistics – enterprises,” European Commission, 2023.
[21] National Institute of Standards and Technology (NIST), National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, NIST Special Publication 800-181r1, 2023.
[22] J. Cenoz and F. Genesee, Trends in Bilingual Acquisition. Amsterdam, Netherlands: John Benjamins Publishing, 2001.
[23] D. Lasagabaster, “English achievement and student motivation in CLIL and EFL settings,” Innovation in Language Learning and Teaching, vol. 5, no. 1, pp. 3–18, 2011.
[24] Y. Ruiz de Zarobe and D. Lasagabaster, Eds., CLIL in Spain: Implementation, Results and Teacher Training. Newcastle upon Tyne, U.K.: Cambridge Scholars Publishing, 2010.