THE ROLE OF AI IN TEACHING ENGLISH AS A SECOND LANGUAGE FOR CYBERSECURITY STUDENTS

Xushmamatova Aminaxon Rustam qizi
"Cyber University" State University,
Senior teacher, Department of "Foreign Languages and Humanities"
aminaxon.xushmamatova@gmail.com
https://doi.org/10.5281/zenodo.20303846

Annotation

This thesis investigates the role of AI in teaching English as a second language for Cybersecurity students by connecting language instruction to authentic security communication tasks. Through analytical synthesis and didactic modeling, it outlines AI-supported activities for technical vocabulary, reading threat intelligence, and producing incident documentation. The novelty is a domain-specific framework that combines adaptive feedback, cybersecurity corpora, and academic integrity safeguards to raise communicative precision and employability.

Keywords: *artificial intelligence; English for Specific Purposes; cybersecurity communication; adaptive learning systems; NLP feedback; technical vocabulary acquisition; incident response writing*

Introduction. Artificial intelligence in language education can be defined as the use of computational methods, especially natural language processing and machine learning, to generate, evaluate, and adapt linguistic input and feedback for learners in real time. The mechanism that makes AI pedagogically relevant is its capacity to model patterns in large datasets of authentic language and then provide individualized prompts, corrections, and progression paths that a single instructor cannot sustain at scale. For Cybersecurity students, a typical example is an AI tutor that presents a simulated phishing email, asks the learner to classify intent and risk, and then guides the student to write a concise report using correct modality, hedging, and technical terms. In practice-oriented programs, internal monitoring of student engagement often shows that short, frequent AI-guided writing cycles can increase the number of produced words per week by roughly two to three times compared to purely classroom-based drafting, which matters because writing volume strongly correlates with accuracy gains over time. Scientifically, this aligns with the view that language acquisition benefits from repeated noticing of form–meaning mappings under conditions of immediate feedback, while domain authenticity strengthens transfer from classroom performance to professional communication.

Main part. Teaching English as a second language for Cybersecurity students is best conceptualized as English for Specific Purposes in which linguistic competence is inseparable from operational discourse, such as incident response communication, vulnerability descriptions, and policy compliance statements. The mechanism of difficulty is that cybersecurity discourse compresses meaning through acronyms, nominalizations, and controlled ambiguity, and students must learn not only vocabulary but also rhetorical structures such as executive summaries, mitigation steps, and evidence chains. An example is the difference between everyday English "the system was hacked" and professionally adequate language "the host was compromised via credential stuffing; indicators of compromise include repeated failed authentication events and anomalous outbound traffic," which requires precise collocations and passive constructions. Empirically, ESP programs frequently report that lexical coverage thresholds for technical reading are higher than in general ESL, and learners often need familiarity with several thousand domain

terms and multiword units to read threat reports efficiently, especially when texts include CVE identifiers, log excerpts, and configuration snippets. Scientifically, this supports integrating vocabulary acquisition with genre-based instruction, because cybersecurity students must master both the micro-level of terminology and the macro-level of communicative intent in professional texts.

A central role of AI is diagnostic personalization, defined as the automated identification of a learner's current language profile and the targeted adjustment of tasks to close specific gaps. The mechanism relies on learner analytics, such as error tagging in writing, speech-to-text analysis for pronunciation and fluency, and adaptive sequencing based on response time and accuracy patterns. For instance, an AI system can detect that a student overuses simple present and underuses modality, then generate micro-tasks requiring "may," "might," "must," and "should" to express risk assessment in security advisories. In many digital language platforms, adaptive pathways commonly reduce time-to-mastery for discrete grammar and vocabulary items by measurable margins, and classroom implementations often observe that students reach required performance bands after fewer iterations when practice is spaced and targeted rather than uniformly assigned. Scientifically, this reflects established principles of mastery learning and spaced repetition, where adaptive scheduling optimizes memory consolidation and reduces cognitive overload, particularly important for Cybersecurity students whose curricula are already heavy with technical content.

Another key role of AI is supporting domain-specific vocabulary and collocation learning through corpus-informed instruction, defined as using large collections of authentic cybersecurity texts to model how terms co-occur and how meaning changes by context. The mechanism is that AI can extract frequent n-grams and collocations, cluster terms by semantic similarity, and generate contextualized examples that show phraseology typical for standards and advisories. A concrete example is teaching the phrase "attack surface reduction" together with its common verb partners "implement," "enforce," and "evaluate," and contrasting it with "reduce exposure" in policy texts, which prevents students from producing unnatural combinations. A practical indicator is that when students learn vocabulary through collocations rather than isolated word lists, their reading speed and summarization accuracy often increase because they recognize chunks as single processing units, and chunk-based processing can reduce working-memory load during comprehension. Scientifically, this corresponds to usage-based linguistics and formulaic language research, suggesting that fluent professional communication depends heavily on stored multiword sequences rather than purely rule-generated output. AI also enables simulation-based speaking and listening practice, defined as interactive dialogues in which learners negotiate meaning under realistic constraints, such as time pressure and professional roles. The mechanism combines speech recognition, dialogue management, and error-focused feedback that can be aligned with communicative functions like clarifying, escalating, and de-escalating incidents. An example relevant to Cybersecurity is a simulated Security Operations Center call where a student must ask for log details, confirm scope, and summarize next steps using polite directives and precise temporal markers, while the AI adjusts difficulty by adding noise, accents, or unexpected turns. In many tertiary contexts, learners receive far fewer minutes of individual speaking time than required for automaticity, and AI-mediated practice can expand speaking exposure substantially beyond classroom limits, which is especially valuable when cohorts are large and contact hours are constrained. Scientifically, interactionist theories predict that negotiated interaction and pushed

output promote development, because learners notice gaps in their interlanguage and attempt repairs, and AI can provide that interaction repeatedly without exhausting instructor resources.

Writing for cybersecurity is a specialized competence, defined as the ability to produce structured, evidential, and audience-appropriate documents such as incident reports, vulnerability assessments, and security policies. The mechanism by which AI improves this competence lies in automated formative feedback on cohesion, register, hedging, and terminological consistency, as well as templates that teach genre moves rather than only grammar. For example, an AI writing assistant can guide students to include the essential elements of an incident report: detection, timeline, impacted assets, root cause hypothesis, containment actions, and recommendations, and it can flag vague phrases like “a lot of traffic” by suggesting quantification and log-based phrasing. In instructional pilots, rubric-based analytics often show that students improve most on organization and clarity when feedback is immediate and revision cycles are short, and these improvements tend to be visible in higher task completion rates and fewer instructor interventions per draft. Scientifically, process-writing pedagogy emphasizes revision and feedback loops, and AI can operationalize that pedagogy by making iterative drafting feasible within limited semester time.

Conclusion. The role of AI in teaching English as a second language for Cybersecurity students is best understood as an enabling infrastructure that amplifies deliberate practice, supports domain-specific vocabulary and genres, and extends interaction opportunities beyond classroom constraints while preserving teacher-led curricular intent. When AI is integrated through corpus-informed materials, simulation-based speaking tasks, and iterative writing feedback aligned with incident response documentation, students develop communicative precision that directly maps onto professional cybersecurity workflows. The effectiveness of this integration depends on secure and ethical use, assessment designs that maintain validity, and a hybrid pedagogy in which AI automates routine feedback while instructors cultivate critical reasoning, evidence-based rhetoric, and professional responsibility.

Adabiyotlar, References, Литературы:

1. Hutchinson T., Waters A. English for Specific Purposes: A Learning-Centred Approach. Cambridge: Cambridge University Press, 1987. 183 p.
2. Chapelle C. A. Computer Applications in Second Language Acquisition: Foundations for Teaching, Testing and Research. Cambridge: Cambridge University Press, 2001. 246 p.
3. Dudeney G., Hockly N., Pegrum M. Digital Literacies. Harlow: Pearson Education, 2013. 384 p.
4. Гальскова Н. Д., Гез Н. И. Теория обучения иностранным языкам. Лингводидактика и методика. Москва: Академия, 2006. 336 с.
5. Азимов Э. Г., Щукин А. Н. Новый словарь методических терминов и понятий (теория и практика обучения языкам). Москва: ИКАР, 2009. 448 с.
6. Jalolov J. J. Chet til o‘qitish metodikasi. Toshkent: O‘qituvchi, 2012. 336 b.