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

Aminaxon Khushmamatova
"Cyber University" State University,
Senior teacher, Department of "Foreign Languages and Humanities"
aminaxon.xushmamatova@gmail.com
https://doi.org/10.5281/zenodo.20519967

Annotation

This thesis examines how artificial intelligence supports teaching English as a second language to Cybersecurity students by aligning language outcomes with professional threat-analysis communication. Using analytical review and instructional design logic, it proposes AI-enabled tasks for vocabulary, discourse, and incident-report writing. Novelty lies in integrating cybersecurity-specific corpora with adaptive feedback and ethics-oriented digital literacy to improve accuracy, fluency, and domain relevance.

Keywords*: artificial intelligence; ESL for cybersecurity; adaptive learning; domain-specific corpus; incident report writing; feedback analytics; academic integrity*

One of the main 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.

The cybersecurity context also requires attention to technical language artifacts, defined as semi-formal representations such as log lines, command outputs, and configuration fragments that appear within English texts and shape comprehension. The mechanism is that students must learn how natural language integrates with technical strings, including how to interpret and describe them accurately, and AI can generate controlled datasets and explanations that scaffold this integration. For example, a lesson can pair an English summary with a simplified log excerpt and ask students to transform the excerpt into a narrative timeline, explaining events using correct tense and causal connectors, while the AI checks whether the described sequence matches the evidence. In many training contexts, learners struggle when texts include embedded code-like elements, and comprehension errors often arise from misreading time stamps, IP addresses, or key-value pairs, which can lead to incorrect narratives even if general English is adequate. Scientifically, this supports multimodal literacy within ESP, where language competence includes interpreting specialized symbol systems, and AI can produce graded materials that progressively approximate real SOC documentation.

A concise comparative view clarifies why AI-supported ESL differs from traditional instruction in this niche, defined as the systematic comparison of inputs, processes, and outcomes between AI-mediated and instructor-only models. The mechanism of improvement is not that AI “teaches better,” but that it increases practice density, feedback speed, and domain authenticity, while the instructor retains responsibility for objectives, ethics, and higher-order discourse. For example, in a traditional model, a teacher may assign one incident report per unit with delayed feedback, while in an AI-supported model students can draft multiple micro-reports weekly, receive immediate guidance, and then bring the best draft to class for deeper rhetorical and critical discussion. Programs that adopt blended approaches often observe that teacher time shifts from correcting recurring grammar errors to evaluating argument quality, evidence sufficiency, and audience adaptation, which are higher-value outcomes for cybersecurity employability. Scientifically, this reflects a division of labor consistent with cognitive load theory: routine error detection can be automated, allowing instructors to focus on complex coaching that requires human judgment.

Aspect	Traditional Model	AI-Supported Model	Hybrid Governance Model
Definition	Instructor-centered delivery with limited individualized practice	Blended instruction with adaptive systems	Human-led curriculum with controlled AI integration
Mechanism	Scheduled classroom activities and periodic homework	Personalization via analytics and NLP feedback	Policy, secure tool selection, and integrity-centered assessment
Example	Weekly vocabulary lists and one report per module	Simulated SOC dialogues and iterative incident-report drafting	AI-assisted drafting with oral defense
Typical Indicator	Limited speaking time per student and delayed feedback cycles	Higher practice frequency and faster revision loops	Stable grade validity and reduced misconduct
Scientific Note	Constrained deliberate practice	Increased opportunities for noticing and output	Construct-aligned assessment design

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.