Original Article
ISSN (Online): 3048-894X

Journal of Digital Security and Forensics
January-June 2025 2(1), 1–5

INTERACTIVE MODULE "MARITIME SECURITY" OF MARITIME ENGLISH ONLINE COURSE ON MOODLE PLATFORM FOR MARINE ENGINEERS

Alona Yuriivna Yurzhenko [1], Olena Yuriivna Kononova [2], Olena Serhiivna Diahyleva [1]

[1] Associate Professor of English Language, Department for Maritime Officers (Abridged Programme), Kherson State Maritime Academy, Odesa, Ukraine
[2] Teacher of Subject Committee for the English Language of the Ship Engineering and Electrical Engineering Departments, Maritime Applied College of Kherson State Maritime Academy, Odesa, Ukraine

Received 09 March 2025
Accepted 11 April 2025
Published 03 May 2025

Corresponding Author

Alona Yuriivna Yurzhenko,
mz@ksma.ks.ua

DOI
10.29121/DigiSecForensics.v2.i1.2025.39

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Copyright: © 2025 The Author(s). This work is licensed under a Creative Commons Attribution 4.0 International License.

With the license CC-BY, authors retain the copyright, allowing anyone to download, reuse, re-print, modify, distribute, and/or copy their contribution. The work must be properly attributed to its author.

OPEN ACCESS

ABSTRACT

The issue of maritime security teaching while e-learning for future marine engineers was explored in the article. The research also presents interactive module created on MOODLE platform in the area of digital security. The module is shown in the context of Maritime English teaching. LMS MOODLE online course is described, particularly the module devoted to security on the ship. Key studies and concepts are analyzed in the research. The results prove that the basics of cyber security are vital during shipboard practice and furthering the career of seafarers.

Keywords: Digital Security, Digitalization, Maritime Professionals, E-Learning

1. INTRODUCTION

Navigation safety is a multifaceted phenomenon combining various organizational, legal, technical, and other measures. According to the definition provided in the current legislation, navigation safety is a state of preservation (protection) of the health and life of people, environment, and property at sea; the absence of unacceptable risk associated with death or injury of people, damage to

How to cite this article (APA): Yurzhenko, A. Y., Kononova, O. Y. and Diahyleva, O. S. (2025). Interactive Module "Maritime Security" of Maritime English Online Course on Moodle Platform for Marine Engineers. *Journal of Digital Security and Forensics, 2*(1), 1-5. doi: 10.29121/DigiSecForensics.v2.i1.2025.39

the environment or material losses Ministry of Transport of Ukraine (2003). Therefore, it is necessary to implement and maintain measures to prevent accidents and minimize risks to the crew. Seafarers must know the basics of safety on board to ensure the safety of both them and other crew members. They must be aware of and follow maritime rules and procedures, use equipment, be able to handle equipment, and learn how to act in an emergency. This will help to avoid collisions, accidents, and other problems on board the vessel. Digital/cyber security has also become integral to modern maritime security. As modern ships, ports, and navigation systems actively use digital technologies, maintaining their integrity and reliability is crucial to prevent accidents and protect the crew's lives. Training at a maritime educational institution involves theoretical training and the development of students' linguistic competence in marine safety. This module, "Maritime Safety," part of the Maritime English course, aims to enable students to communicate effectively in critical situations using unique terminology and expressions, contributing to better coordination of actions between crew members and rescue services.

2. OBJECTIVE

This research shows online module in the area of digital security on LMS MOODLE online course for future marine engineers.

2.1. ANALYSIS OF RECENT RESEARCH AND PUBLICATIONS

Oruc, A., Chowdhury, N. & Gkioulos, V. A in their study addresses the increasing cyber vulnerabilities in the rapidly digitalizing maritime industry—primarily due to human error—and presents a solution in the form of a modular, role-based cybersecurity training program called Maritime Cyber Security (MarCy). The Critical Events Model was created and evaluated by 19 experts through the Delphi technique, the program offers eleven elective modules for office staff to know more about cybersecurity. It is designed for implementation by education institutions, crewing companies, and government bodies Oruc et al. (2024). Shapo, V. and Levinskyi, M. highlight that a significant shift in maritime technology is underway in integrating Industry 4.0, IIoT, and Shipping 4.0, enabling unmanned, autonomous, and remote-controlled ships. While these advancements open up new engineering possibilities, they expose systems to cyber threats. Consequently, maritime education must deepen its focus on areas like IIoT, data transfer technologies, satellite systems, big data, AI, VR/AR, remote control, and cybersecurity Shapo and Levinskyi (2021). The global maritime industry's rapid digitization increases vulnerability to cyber threats, mainly due to human error. Therefore, the authors Aybars Oruk, Nabin Chowdhury, and Vasileios Gkiulos propose to address this gap in cybersecurity training at sea, a modular program called Maritime Cybersecurity (MarCy) using the Critical Event Model (CEM) was developed. This program was evaluated by 19 experts using the Delphi technique. MarCy offers eleven optional modules aimed at improving the cybersecurity skills of both seafarers and office staff and is designed for implementation by education institutions, crewing companies and related organizations Oruc et al. (2021). Maritime Cyber Range training is presented in this research, showing the core components of such an environment. The presented Cyber Range environment includes navigational, information, and telecommunications systems, networks, and SCADA systems. It supports maritime vulnerability, penetration and exploitation scenarios, traffic eavesdropping, GNSS/AIS spoofing, navigation takeover, signal intelligence scenarios, etc. Potamos et al. (2021). Specific gaps were discovered by us in the issue of maritime security teaching while e-learning for future ship engineers.

3. RESEARCH METHODS

This study presents an innovative interactive module that combines modern pedagogical technologies with advanced teaching methods and aims to develop critical digital security skills among future seafarers. Implementing this module in the Maritime English course on the LMS MOODLE platform addresses the challenges associated with the growth of cyber threats due to the digitalization of the industry. It creates a unique environment where students receive language knowledge and specialized cybersecurity information necessary for working in a digital maritime environment. The module consists of 3 subtopics and is designed for 10 lessons. Each topic corresponds to the curriculum and STCW. In addition, cadets from the ship engineering and navigation departments participated in our study to increase their awareness of modern cyber threats and methods for their prevention. Their participation allowed us to assess the initial level of future specialist's knowledge and demonstrate the effectiveness of the implemented training module Diahyleva et al. (2021), Behforouzi et al. (2022).

4. RESULTS

Training and education are key components of safety at sea. They serve to prepare seafarers for their duties and ensure the safety of the crew, the ship, and the environment. Modern ships are equipped with various safety systems that help prevent accidents and ensure the crew's safety in emergencies. They contain several components, including safety procedures, equipment and technology, and safety management systems. Students should master the basic terms and expressions related to maritime safety, including terms related to navigation, evacuation, emergencies, rescue services, and other aspects of safety Sørensen (2023), Senarak (2021), Scanlan et al. (2023).

The module aims to improve speaking, listening, reading, and writing skills in English in a safe context. This includes practical exercises, role-playing, emergency simulations, and group discussions. Also, the module contains interactive exercises, video materials, and case studies, which help students feel more confident when communicating with international partners and in emergencies Baum-Talmor and Kitada (2022). Students learn the primary international safety standards, protocols, and procedures used in the maritime industry. Thanks to the integration with MOODLE, students have convenient access to educational materials, can participate in group discussions, perform practical tasks, and independently research digital security issues. This contributes to a better understanding of global requirements and allows them to respond correctly in emergencies Pavlinović et al. (2022), Pseftelis and Chondrokoukis (2021).

In addition, the module contributes to the development of professional communication in English, which is extremely important for working in an international maritime environment. This approach allows future marine engineers to comprehensively understand digital security and apply the acquired knowledge in practice, significantly increasing their competitiveness in the labor market Amanuel (2023).

Digital/cyber security is an essential complement to traditional maritime security measures. It helps protect critical information systems, ensuring the smooth functioning of shipping and saving human lives Karahalios (2025), Björnlund and Faqiri (2023), Kechagias et al. (2022). A comprehensive approach that combines technological innovation, personnel training, and international cooperation will contribute to increasing the overall resilience of maritime infrastructure to modern cybersecurity challenges Kononova and Yurzhenko (2020).

5. CONCLUSIONS

It can be concluded that the research shows a significant increase in understanding of the cybersecurity's importance by future marine engineers, which will contribute to the formation of the necessary skills for a prompt response to cyber incidents in the maritime industry. Traditional maritime security measures should be added with basics of cyber security on the ship. The prospects of further research can be seen in the analysis of digital security learning of future navigators and electrical engineers.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Amanuel, A. (2023). How Digitalization is Affecting Maritime Safety and the Work Environment of the Crew : A Study of Technological Advances and Its Effect on End-Users Onboard an Lng Vessel.

Baum-Talmor, P., & Kitada, M. (2022). Industry 4.0 in Shipping : Implications to Seafarers' Skills and Training. Transportation Research Interdisciplinary Perspectives, 13, 100542. https://doi.org/10.1016/j.trip.2022.100542

Behforouzi, M., Dadwal, S. D. S., Hassan, K., Tugsan, A., Mostafa, E., Ghoneim, N. I., & Soltani, H. R. (2022). Implementing Digitalization and Authentication of Seafarer's Identification and Certification in the Sultanate of Oman. Journal of Maritime Research, 19(3), 68-76.

Björnlund, P., & Faqiri, F. (2023). Survey of Ongoing and Next-Generation Cybersecurity of Maritime Communication Systems.

Diahyleva, O. S., Gritsuk, I. V., Kononova, O. Y., & Yurzhenko, A. Y. (2021, March). Computerized Adaptive Testing in the Educational Electronic Environment of Maritime Higher Education Institutions. CTE Workshop Proceedings, 8, 411-422. https://doi.org/10.55056/cte.297

Karahalios, H. (2025). Cybersecurity Threats of Remote Autonomous Ships While Approaching Ports. Journal of Transportation Security, 18(1), 2. https://doi.org/10.1007/s12198-024-00289-1

Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital Transformation of the Maritime Industry: A Cybersecurity Systemic Approach. International Journal of Critical Infrastructure Protection, 37, 100526. https://doi.org/10.1016/j.ijcip.2022.100526

Kononova, O., & Yurzhenko, A. (2020). Engaging Future Ship Engineers in Distance Stem Education. Journal of Information Technologies in Education (ITE), (45), 22–31.

Ministry of Transport of Ukraine. (2003). Regulations on the Management System of Navigation Safety in Sea and River Transport (Order No. 904, November 20, 2003). Official Gazette of Ukraine, 52(2), 2844.

Oruc, A., Chowdhury, N., & Gkioulos, V. (2021). A Modular Cyber Security Training Programme for the Maritime Domain. International Journal of Information Security. https://doi.org/10.1007/s10207-023-00799-4

Oruc, A., Chowdhury, N., & Gkioulos, V. (2024). A Modular Cyber Security Training Programme for the Maritime Domain. International Journal of Information Security, 23, 1477-1512. https://doi.org/10.1007/s10207-023-00799-4

Pavlinović, M., Račić, M., & Karin, I. (2022). Cyber Risks in the Maritime Industry-Case Study of Croatian Seafarers. in Human Interaction, Emerging Technologies and Future Systems V (108-113). Springer International Publishing. https://doi.org/10.1007/978-3-030-85540-6_14

Potamos, G., Peratikou, A., & Stavrou, S. (2021). Towards A Maritime Cyber Range Training Environment. in 2021 IEEE International Conference on Cyber Security and Resilience (CSR) (180-185). IEEE. https://doi.org/10.1109/CSR51186.2021.9527904

Pseftelis, T., & Chondrokoukis, G. (2021). A Study About the Role of the Human Factor in Maritime Cybersecurity. SPOUDAI-Journal of Economics and Business, 71(1–2), 55–72.

Scanlan, J., Hopcraft, R., Cowburn, R., & Lützhöft, M. (2023). Maritime Education for A Digital Industry.

Senarak, C. (2021). Cybersecurity Knowledge and Skills for Port Facility Security Officers of International Seaports: Perspectives of it and Security Personnel. The Asian Journal of Shipping and Logistics, 37(4), 345-360. https://doi.org/10.1016/j.ajsl.2021.10.002

Shapo, V., & Levinskyi, M. (2021). Means of Cyber Security Aspects Studying in Maritime Specialists Education. in Auer, M. E., & Tsiatsos, T. (Eds.), Internet of Things, Infrastructures and Mobile Applications (389-400). Springer International Publishing. https://doi.org/10.1007/978-3-030-49932-7_38

Sørensen, R. (2023). How to Improve the Cyber Security Awareness in the Shipping Industry.