методів реагування на кризові ситуації, дозволяють надійно забезпечувати безпеку в морському середовищі.

Отже, ефективне технічне забезпечення морської безпеки України є результатом комплексного підходу, що включає модернізацію флоту, розвиток інфраструктури, підготовку кадрів та активну міжнародну співпрацю. Це дозволяє гарантувати захист національних інтересів та безпеку на морі.

Література:

1. Мельник О. М., Актуальні проблеми морської безпеки та сучасні шляхи забезпечення охорони судна. Комунальне господарство міст, 6 (166), 204-210. Комунальне господарство міст 6.166. 2021. С. 204-210.
2. Кузніченко С.О. Деякі особливості національних стратегій морської безпеки. Maritime security of the baltic-black sea region: challenges and threat. 2022. С. 18.
3. Мельник О. М., Ю. В. Бичковський. Сучасна методика оцінки рівню безпеки судна та шляхи його підвищення. Розвиток транспорту 2.9. 2021. С. 37-46.

DOI https://doi.org/10.30525/978-9934-26-527-3-39

MODERN TRENDS IN ARTIFICIAL INTELLIGENCE AND MARITIME SECURITY: A FOREIGN VISION

СУЧАСНІ НАПРЯМИ ШТУЧНОГО ІНТЕЛЕКТУ І МОРСЬКА БЕЗПЕКА: ЗАРУБІЖНЕ БАЧЕННЯ

Piadyshev Volodymyr Heorhiyovych
Doctor of Law, Professor,
Professor of the Department
of Criminal Analysis and Information
Technologies,
Odesa State University
of Internal Affairs
Odesa, Ukraine

Пядишев Володимир Георгійович
доктор юридичних наук, професор,
професор кафедри кримінального аналізу
та інформаційних технологій,
Одеський державний університет
внутрішніх справ
м. Одеса, Україна

Today, the maritime industry transports more than 90% of the world's cargo. It is therefore an important component of the global economy. This important sector is rapidly digitizing today. Digital technologies improve the operational capabilities of vessels. They are mainly used in logistics,

navigation and communications. They contribute to increased energy efficiency and reduced emissions [1, p.1]..

But at the same time, systems are developing that can harm maritime security. The threat from cybercriminals and aggressor states is extremely high. Shipping is therefore becoming an attractive target for cyberattacks. The operational (OT) and information technology (IT) components of vessels are now closely linked. Therefore, attacks on them can be extremely dangerous [2, c. 1].

The above problems in Ukraine are extremely acute today due to the full-scale, all-round aggression of the russian federation.

The place of cybersecurity in maritime security

Maritime security is a crucial component of global trade and transportation. Working at sea is associated with a number of dangers: capsizing, fires, bad weather, equipment failure, etc. Other security problems are smuggling, piracy, cyber threats.

In several regions of the world, in particular, in the vicinity of Africa, in the Middle East, in Southeast Asia, there is an aggravation of the political situation, which necessitates the strengthening of security systems at sea. Moreover, conventional security systems are not able to cope with new threats. More and more money is being spent on security. Thus in 2029, the market for maritime security systems will amount to up to $50 billion. That is, maritime cybersecurity is becoming a problem. The answer to this problem can only be a comprehensive approach to risk management. Time-tested areas of cybersecurity management include the following [3, p. 1]:

• improving awareness of seafarers, shore personnel and all stakeholders;
• assessing and implementing countermeasures;
• monitoring the reliability and improving barriers.

Artificial Intelligence in Maritime Security

The integration of artificial intelligence (AI) into maritime security has become a turning point in the organization of maritime operations protection. There are key trends in the implementation of AI in maritime security [4, p. 2]:

• *Machine learning algorithms*: detect illegal activities by detecting patterns and anomalies;

• *Autonomous drones and robots*: AI-powered UAVs and autonomous underwater vehicles increase the effectiveness of maritime surveillance;

• *Analytics and data fusion* from different sources offer a more holistic view of threats.

Ways to redefine maritime security with AI:

• *Proactive threat detection:* detecting threats before they occur,

• *Global collaboration* : sharing experiences internationally with AI.

AI is transforming the maritime industry. AI systems collect data and look for patterns. Machine learning automates functions. AI systems suggest changes to improve efficiency and sustainability of processes.

AI plays an important role in navigation. It makes transportation safer and more efficient. Possible routes are automatically reviewed, and numerous factors (weather forecasts, piracy situation) are checked and the best route is selected. AI systems improve navigation through problematic ports. AI systems use past information about port navigation together with current information and plot a safer route [5, p. 2].

Security management still largely depends on human decisions and is carried out according to the following logic: collecting and processing information (learning) → manipulating information (establishing causes) → considering the results of these actions (understanding). At the same time, from 75% to 96% of accidents at sea are still caused by human errors. ***And what can AI do?***

Recognition, as well as prediction of behavior, involves the use of powerful AI – artificial general intelligence (AGI) [6, p. 1-3]. Despite the funds invested in its development, many applications with general AI still remain a fantasy. Most AI programs are reactive, that is, they react to an event, but do not predict it (based on weak AI). An example is autonomous driving. At the same time, when determining the parameters of learning algorithms, AI depends on a human solution.

The maritime industry is well suited for machine learning. It produces significant amounts of data on cargo inspection, etc. daily. However, today, instead of full automation, partial assistance focused on individual solutions can give a better return on investment.

So, today, AI-based technologies offer the following: *real-time threat identification; predictive analytics; improved awareness of the maritime environment; cybersecurity.*

Generative Artificial Intelligence and Maritime Security

In addressing this question, it is important to recall two definitions. ***Artificial intelligence (AI)*** is a field of research in computer science that develops and studies methods and software that allow machines to perceive their environment and use learning and intelligence to perform actions that maximize their chances of achieving specified goals. ***Generative AI (GenAI, or GAI)*** is a subset of AI that uses generative models to generate text, images, video, or other forms of data. These models learn the underlying patterns and structures of their training data and use them to generate new data based on input, often in the form of natural language prompts.

The UK's National Cyber Security Centre warns that AI will increase the volume and impact of cyberattacks because it lowers the barrier to entry for novice hackers to access effective ransomware; it multiplies the toolkit for

AI-powered attacks; increases the ability of threat actors to find valuable targets [7, pp. 1 2].

Phishing and malware, as before, remain the main ways of cyberattacks. Through phishing in May 2024, an employee of the British firm ARUP in Hong Kong was tricked into transferring $25 million from his company to the criminals' account. He started believing the criminals during a Zoom conference, as if with a partner. Deepfake AI technology was used to imitate the voice and appearance of high-level company executives.

As for malware, in 2022, the famous port of Lisbon was hit by the AI-based LockBit program. The loss amounted to $ 1.4 million.

Today, generative AI is used even by poorly educated hackers to create complex programs containing polymorphic malware. Moreover, criminal attacks are carried out both on individual crew members and on entire vessels and fleets.

Adversarial AI This is a new type of malware for manipulating AI models – to bypass the limitations built into AI models, to overcome AI in cybersecurity systems. The main areas of application are as follows.

Poisoning attacks are the introduction of malicious software that feeds malicious data into a machine learning model at both the training and execution stages.

Evasion attacks are aimed at tricking the AI model that is supposed to make decisions.

Conclusions

So, we see that the latest information technologies, in particular AI, not only work to improve the situation with maritime security, but also vice versa – criminals (even states) spare no expense in achieving criminal goals by violating maritime security. While AI has become an accelerator of cyber threats to maritime security, the acquisition, study and use of AI tools, in particular generative AI, also serves to combat these new threats. The latter should be promoted in every possible way.

References:

1. Enhancing Maritime Security with Artificial Intelligence. *Linkedin. July 29 2024*. Site. URL: https://www.linkedin.com/pulse/enhancing-maritime-security-artificial-intelligence-soshianest-sw0be

2. Maritime cyber security. *DNV Group. 2024.* Site. URL: https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/

3. Maritime cyber security services and solutions. *DNV Group. 2024.* Site. URL: https://www.dnv.com/services/maritime-cyber-security-services-and-solutions-73927/

4. The Future of Maritime Security with AI. *SEAGULL Surveillance. Jul 31, 2024*. Site. URL : https://www.seagullsurveillance.com/never-blink-an-eye-enhanced-maritime-security/the-future-of-maritime-security-with-ai

5. Artificial Intelligence and Other Technologies Improve Maritime Safety. *Maritime Injury Center. July 11, 2024*. Site. URL: https://www.maritimeinjurycenter.com/2024/07/11/artificial-intelligence-and-other-technologies-improve-maritime-safety/

6. Artificial intelligence in maritime safety management. *KAIKO Systems. 2024*. Site. URL: https://www.kaikosystems.com/blog/artificial-intelligence-maritime-safety

7. How AI is Transforming Maritime Cybersecurity: Navigating the Storm Ahead. *CYDOME. 2024*. Site. URL: https://cydome.io/how-generative-ai-impacts-maritime-cybersecurity/