Кустовський О. В.,
здобувач вищої освіти,
Національна академія Служби безпеки України
(м. Київ, Україна)

Кононова Д.В.,
кандидат філологічних наук, доцент,
доцент кафедри романо-германських мов,
Національна академія Служби безпеки України
(м. Київ, Україна)

LINGUISTIC ANALYSIS AS A TOOL FOR INFORMATION SECURITY

The modern digital space is characterized by unprecedented dynamics and complexity of cyber threats. While at the dawn of the computer age the main risks were associated with technical vulnerabilities in software and hardware, today the threat landscape has undergone a fundamental transformation. There has been a significant shift from attacks targeting only machine systems to hybrid campaigns that exploit the weakest link in the security chain - the human factor. Modern cyber threats, such as spear-phishing, Business Email Compromise (BEC), social engineering, disinformation, and insider threats, are becoming increasingly sophisticated and psychologically manipulative. Their effectiveness is not based on "zero-day vulnerabilities," i.e., unknown vulnerabilities that software developers actually had 0 days to address, as these are only discovered at the moment of attack, but on the ability of attackers to manipulate human emotions, cognitive biases, and social norms using natural language [1].

Today's linguistic analysis, implemented using natural language processing (NLP) and machine learning (ML) methods, has evolved from an auxiliary tool to a key component of a modern active information security strategy. The use of NLP allows for the automation of human language analysis on a scale unattainable by human analysts, transforming chaotic streams of unstructured text into structured, actionable intelligence and evidence. This technological transformation makes it possible not only to respond to incidents that have already occurred, but also to detect threats at an early stage ( ), predict attack vectors, determine responsibility for cybercrimes, and create adaptive defense systems capable of countering language-oriented threats. The integration of linguistic analysis into Security Operations Centers (SOCs) is no longer an option but a requirement for ensuring resilience in the current threat environment, which requires not only network engineers but also data processing specialists, computer linguists, and philologists [4].

With the development of machine learning, more sophisticated methods have emerged. Models that learn with a "teacher," such as Support Vector Machines (SVM),

are trained on large arrays of texts that have been pre-labeled for tone. They are capable of detecting more complex patterns than simple lexicons. A further breakthrough came with the advent of deep learning models, in particular recurrent neural networks (RNN) and long short-term memory (LSTM) networks, which can analyze word sequences and better capture dependencies in a sentence. Modern models based on the Transformer architecture, such as BERT (Bidirectional Encoder Representations from Transformers), provide the highest accuracy thanks to attention mechanisms that allow weighing the importance of different words in a sentence and understanding the context at a deep level [2].

Thus, sentiment analysis becomes a kind of data collection system. Abnormal changes in public sentiment can predict not only cyberattacks, but also events in the physical world, such as civil unrest or protests. The threat detection process may look like this: first, the online space is filled with messages that form a certain narrative and evoke an emotional response (e.g., anger about government actions). NLP-based monitoring systems record this abnormal surge associated with certain keywords and user groups. By correlating this data, analytics centers can generate high-confidence alerts about potential threats, transforming social media monitoring from a reactive brand management tool into a proactive intelligence tool [1].

It is also worth noting the emergence of large language models (LLMs), such as the GPT (Generative Pre-trained Transformer) family of models, which represent the next stage in this evolution. These models, trained on large amounts of text data from across the Internet, demonstrate not only the ability to classify, but also to deeply understand, generalize, reason, and generate human language. Their integration into cybersecurity systems opens up radically new possibilities. The use of LLMs fundamentally changes the nature of security analyst work. Instead of spending hours manually analyzing raw data such as system logs or vulnerability reports, analysts receive ready-made, structured conclusions from LLMs. The role of humans is shifting from data processing to validating conclusions made by artificial intelligence and making strategic decisions. This significantly increases efficiency, but at the same time creates a new dependence on technology whose decision-making processes can be opaque. If an LLM misinterprets a particular nuance or falls victim to manipulation, it can mislead an analyst who has not seen the raw data. This creates an urgent need to develop and implement Explainable AI (XAI) methods in cybersecurity that would allow analysts to understand why a model has reached a particular conclusion and to verify its logic [3].

Thus, linguistic analysis, enhanced by natural language processing and machine learning methods, has become an integral and transformative technology in the arsenal of modern information security. It has changed the approach to protection: previously, the system responded to problems that had already occurred, but now it works proactively, analyzing data to prevent attacks in advance.

References:

1. Arora A., Arora A., McIntyre J. Developing chatbots for cyber security: assessing threats through sentiment analysis on social media. Sustainability. 2023. Vol. 15, no. 17. P. 13178. URL: https://doi.org/10.3390/su151713178

2. Mabel E., Enoch O., Idowu M. Sentiment analysis in social media: detecting misinformation and cyber threats. URL: https://www.researchgate.net/publication/389055739_Sentiment_Analysis_in_Social_Media_Detecting_Misinformation_and_Cyber_Threats

3. Niveen O. Jaffal, Mohammed Alkhanafseh, David Mohaisen. Large language models in cybersecurity: applications, vulnerabilities, and defense techniques. URL: https://arxiv.org/abs/2507.13629.

4. Oye E., Owen J. The role of natural language processing in cybersecurity. Natural language processing. URL: https://www.researchgate.net/publication/387252722_The_Role_of_Natural_Language_Processing_in_Cybersecurity