

Application of Sentiment Analysis to Prevent Cyberattacks on Objects of Critical Information Infrastructure

**SVITLANA LEHOMINOVA, YURII SHCHAVINSKY, TETIANA MUZHANOVA,
 DMYTRO RABCHUN, MYKHAILO ZAPOROZHCHENKO**

State University of Information and Communication Technologies, Kyiv, Ukraine, (e-mail: yushchavinsky@ukr.net)

Corresponding author: Yurii Shchavinsky (e-mail: yushchavinsky@ukr.net).

ABSTRACT The article addresses the pressing issue of ensuring cyber security for critical information infrastructure, which is associated with the development of modern information technologies and the increased potential for cyber attacks from criminal groups and potential adversary state entities. An analysis of the scientific literature indicates the necessity of preventive measures and scientific research, which involve monitoring the cyberspace. The application of sentiment analysis is proposed to detect the emotional sentiment towards critical information infrastructure objects. Following a defined algorithm, a sentiment analysis model is constructed based on an artificial neural network using open-source Python programming language libraries. The model's distinguishing feature is the consideration of emoticons to determine the intensification of emotional attitudes towards conducting cyber attacks on critical information infrastructure objects. A dataset related to cyber attacks from social media platforms such as Twitter and Instagram is collected to train the neural network. The results of training and testing the neural network provide grounds to assert that the network's accuracy of 0.7852 is relatively high, enabling its application by cyber reconnaissance units for early detection of cyber threats to critical infrastructure objects in combination with other tools.

KEYWORDS cyber security; information security; sentiment analysis; neural networks; artificial intelligence; machine learning; critical infrastructure, Python.

I. INTRODUCTION

PROTECTION of critical infrastructure objects (CIOs), the malfunction of which can harm vital national interests, is one of the most important tasks of any state today. CIOs include energy networks, transport systems, banking systems, communication networks, water supply and purification systems, healthcare systems, information systems of state institutions, and others. Compromising these systems can disrupt their continuity and stability, create real or potential threats to the population, society, socio-economic status, national security and defense of Ukraine, threaten people's lives and health, and can lead to economic and social disaster [1].

In modern times, as the world becomes increasingly digital, the information component of critical infrastructure – the critical information infrastructure (CII) – is the most vulnerable part of the overall critical infrastructure (CI) due to the growing number of cyber attacks and cybercrime. CII is considered a central component of the critical infrastructure of various countries. CII objects consist of a combination of information systems, communication networks, databases, management

systems, power systems, transportation networks, and other components that are essential to ensure the continuity of government management, economic development, national security, and defense capability of the country. Malfunctioning of CII objects can result in significant material losses, interruptions in the functioning of vital systems, leakage of confidential information, threats to public safety, and damage to the entire critical infrastructure as a whole.

As CII objects are important for the functioning of society and the state, they are becoming the primary target of cyber attacks today, and protecting them from cyber threats is an extremely important task for every country. Cyber threats can come from both criminal groups and state structures, which significantly increases the risk of threats and importance of addressing cybersecurity issues. Therefore, the relevance of protecting CII objects continues to grow, requiring scientific research, development of new technologies and strategies for effective protection against cyber attacks.

II. METHODS OF CYBER PROTECTION OF CRITICAL INFRASTRUCTURE OBJECTS

Organizing research in the field of cyber protection of critical infrastructure objects is an important task as it enables the development and improvement of effective methods and tools for preventing cyber attacks, which helps to preserve national security and economic stability of the country.

Research on cyber protection of critical infrastructure objects is typically carried out by scientific institutions and specialized research centers that work in the field of cybersecurity and have dedicated laboratories for conducting research and testing cyber protection measures. In addition, other interested parties such as companies providing cybersecurity services and government organizations responsible for national security may also participate in research. They can provide their researchers with access to real data and critical infrastructure systems to conduct research and test cyber protection methods.

Research in this field is also conducted by universities that have specialized faculties in information security and cybersecurity. Within such research, new methods and tools are developed to prevent cyber attacks on CII. The results of their research are highlighted in many scientific papers available to the scientific community.

In work [2], a qualitative study of cyber attacks by extremists and ideologically motivated actors on digital infrastructure and the Internet in the UK and Canada from 2000 to 2015 was conducted, identifying cybersecurity problems of CII objects and the need for preventive measures to ensure their cyber protection.

In the face of complex threats, studies [3-5] have been conducted on the application of cyber defense methods for critical infrastructure based on knowledge of physical processes in the infrastructure. This approach enables the detection of traditional computer attacks that alter the behavior of the primary physical process in the infrastructure, based on the knowledge of the physical process in the cycle of infrastructure management. According to the results of these studies, in works [6-9] stands and industrial firewalls are proposed for blocking commands that lead to a critical state of automated control systems of CIOs, thereby ensuring their stability.

Other studies by researchers [10-11] have shown the effectiveness of data clustering methods in timely detecting anomalies in the functioning of critical infrastructure.

The most popular new topics in the field of critical infrastructure security are developed in work [12], where the computational aspects of critical infrastructure security models are studied for describing information and economic processes. The importance of developing encryption algorithms with consideration of known attack analysis problems, symmetric cipher issues, and the great practical and commercial importance of security are determined.

In works [13, 14], the authors explored the use of machine learning for detecting cyber threats and identifying cyber criminals based on the analysis of sentiment and other aspects of user behavior in social networks. Their work demonstrates that sentiment analysis can help detect cyber attacks faster and with greater accuracy compared to traditional methods of network activity monitoring.

Paper [15] describes the effectiveness of sentiment analysis in cybersecurity, particularly the use of sentiment analysis in

social media to detect extremism. Additional feature extraction methods are discussed to improve performance, with practical results presented. The *Multinomial Naïve Bayes* and *Linear Support Vector Classifier* algorithms are used for classification purposes. A brief description of complex neural network sentiment classifiers with intelligent analytics is provided.

The vast majority of researchers emphasize the necessity of automated methods for detecting cyber threats to CII objects in cyberspace, based on artificial intelligence technologies. Manual heuristic analysis of malware is no longer considered effective and productive compared to the high prevalence of malware. In this regard, to assist cybersecurity experts, Microsoft announced the development of a new tool, *Security Copilot*, which can simplify their job of managing multiple tools and huge volumes of data from multiple sources to mitigate CII security threats using an easy-to-use AI assistant [16]. The new tool leverages the advantages of the latest technology based on *GPT-4 OpenAI LP* to allow cybersecurity experts to ask questions and get answers about current security issues affecting their environment. Using Microsoft's own global threat intelligence, *Security Copilot* can predict and identify potential threats that professionals may miss. This will enable tracking anomalies and identifying potential issues in CII objects. However, Microsoft warned of the need to verify the accuracy of the provided answers and suggestions, as this tool requires additional training.

Ukrainian scientists consider modern objects of CII as the basis for ensuring continuous and stable functioning of CII. In works [17, 18], methodological approaches were developed to ensure cybersecurity of critical information infrastructure objects, which are crucial for the defense capabilities of the state, its economic and social development. The principles and ways of improving the cyber protection of objects have been determined.

In work [19], a process model for managing the cybersecurity of critical infrastructure using an integrated system for managing the national cybersecurity sector in Ukraine was developed and presented. The functional components of the CII cybersecurity system were described, and the practical value of the integrated cybersecurity management system for these objects was justified.

Most scientists identify several key problem areas in organizing cybersecurity for critical information infrastructure objects CIIs:

- lack of adequate security standards, which can lead to the use of different security methods that may be incompatible with each other and reduce the effectiveness of protection;
- outdated technology in many protection systems developed decades ago does not meet modern security requirements, making them more vulnerable to new threats;
- lack of a monitoring and early incident detection system can result in an attack being detected too late, when it has already caused significant damage.

These problems can be addressed through scientific developments and technologies such as machine learning, artificial intelligence, quantum technologies, blockchain, and others. It is important to improve protection technologies and adapt them to new threats to ensure effective protection of CIIs.

III. ALGORITHM FOR CREATING A SENTIMENT ANALYSIS MODE

One of the preventive methods for ensuring cyber security of critical information infrastructure (CII) is the use of sentiment analysis by cybersecurity experts to detect threats early based on monitoring of social media.

Sentiment analysis is a method of analyzing texts that allows for the automatic determination and classification of the emotional tone of statements (positive, negative, or neutral) contained in textual documents, product or service reviews, social media messages, news, etc.

Sentiment analysis can be a useful tool for ensuring cyber security, as it enables the determination of the emotional state and intentions of users, which can indicate possible threats to CII. Sentiment analysis can help track user feedback and comments on social media and forums, which can help identify potential threats to the organization. For example, users may discuss attacks on a particular organization or use terms related to cybersecurity, such as "virus," "fraud," or "data breach".

Sentiment analysis can help detect phishing attacks because attackers try to use users' emotions and beliefs to gain access to their accounts or computers. Hackers during phishing attacks usually use manipulative language and emotional appeals – techniques or methods of speech influence that aim to elicit an emotional reaction from the reader or listener in order to convince or influence them. These techniques are used in communication, advertising, political campaigns, media materials, etc. Emotional appeals can be positive (for example, using positive emotions such as joy, laughter, love, etc.) or negative (for example, using negative emotions such as fear, anger, horror, shame, etc.). Emotional appeals can include the use of emotionally charged words, phrases, stories, metaphors, images, symbols, etc. The main goal of using emotional appeals is to draw attention to the problem and achieve the desired effect.

Sentiment analysis is typically performed using machine learning and statistical natural language processing methods. The algorithm for creating and applying a sentiment analysis model based on a neural network for monitoring social networks to detect CII threats is shown in Fig. 1.

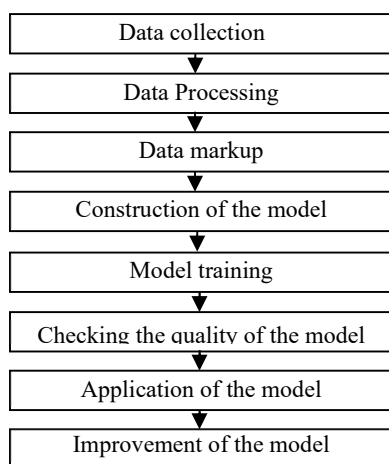


Figure 1. Scheme of the algorithm for the use of sentiment analysis in cyber security

To create the model, a sufficient amount of data reflecting the interaction of users with the system, as well as feedback,

comments, messages, and other information containing sentiment nuances, is required. To collect data for sentiment analysis aimed at preventing cyber attacks on critical infrastructure objects, various sources can be used.

The main sources for collecting data for monitoring threats to CII objects can be:

- social media (Twitter, Facebook, LinkedIn, Reddit, Instagram, etc.), which contain a large amount of information about criminal activity, criminal intentions, their plans, attack methods, etc.;
- specialized forums and blogs, where issues of cybersecurity and criminal activity are often discussed;
- websites related to cybersecurity, such as Stack Exchange, Cybersecurity Forum, Dark Reading, etc., which may contain user feedback, comments, advice, and news about cybersecurity and critical infrastructure;
- news portals, where news about cyber attacks on CII and similar events may appear;
- open sources, databases with public information about cyber attacks on CII objects;
- monitoring systems that track cyber attacks on critical infrastructure objects and similar events;
- documents and reports related to cybersecurity, such as reports on data breaches, may contain important data for model creation;
- other data sources may include datasets that have already been created and published for use in machine learning.

Automated data collection from social media websites can be achieved using web scraping tools. They can be useful for automating the collection of large amounts of data from user reviews posted on the internet.

The main process of web scraping involves the following steps:

- identifying the data source from which information is required;
- establishing a connection with the website and receiving a response from the server;
- analyzing the response and extracting the necessary data using web scraping tools;
- storing the data in a file or database.

There are several approaches to web scraping, but the most common one is to use the Python programming language and web scraping libraries such as BeautifulSoup, Scrapy, Selenium, etc.

To scrape data from Twitter using Python, the Tweepy library is used, which provides access to the Twitter API.

To scrape data from Facebook using Python, the PyFacebook library is used, which provides access to the Facebook Graph API. To use the Facebook Graph API, it is necessary to have a Facebook developer account and create own application to obtain an access key.

However, it is important to remember that web scraping may violate website usage rules, so it is necessary to carefully research the laws and rules of using a particular website before starting the web scraping process. Incorrect use of web scraping can lead to legal issues and access to the website being blocked.

The collected data must be verified and ensured to be of high quality and representative, meaning that they reflect real feedback and sentiments of users. Inaccurate data can lead to incorrect conclusions and erroneous decisions. To achieve this, the method of expert evaluation must be applied.

During data processing, they are transformed into a format understandable for the neural network by removing unnecessary characters, performing tokenization, lemmatization, and other methods that reduce the number of text variations and facilitate further processing.

Emotional expressions that may indicate preparation for a cyber attack on critical infrastructure objects may contain elements such as:

- the use of threatening words, such as "destroy," "hack," "kill," "cause harm," "break into," "seize," "destroy the system," "strike," "create chaos";
- the use of emotionally charged words or phrases such as "revenge," "hate," "anger," "outrage," "hostility," "tension," "disrespect," "despair," "anxiety," "fear," "panic";
- the use of technical terms related to cybersecurity and cyber attacks, such as "botnet," "DDoS attack," "virus," "spyware," "trojan," "criminal group," "exploit";
- the use of abbreviations or code words that may indicate a cyber attack, such as "APT" (Advanced Persistent Threat), "Zer0day" (use of an unknown vulnerability), "Bot" (malicious software controlled remotely), and others.

Usually, textual data is converted into numerical vectors using vectorization algorithms. For automatic conversion, the ready-made Word2Vec model of the Gensim library is used, which must be installed in Python. An example of vectorization of the Word2Vec text "I plan to conduct vulnerability testing on critical infrastructure servers to find weak points and break their system" using the model in Fig. 2.

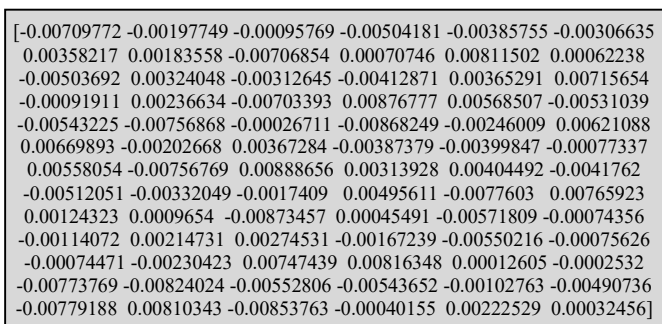


Figure 2. The result of text vectorization

Marking data from the point of view of sentiment when building a sentiment analysis model is carried out by assigning to each text the appropriate tag: positive, negative or neutral. The determination of the intensity of the emotional color of the text in social networks, which characterizes the relationship to a cyberattack on the objects of the KII, is given in Table 1.

Table 1. Intensity scale




Criterion	Indicator
very strong negative intensity of emotions	-5
strong negative intensity of emotions	-4
moderate negative intensity of emotions	-3
slight negative intensity of emotions	-2
weak negative intensity of emotions	-1
unexpressed emotional relationships	0
weak positive intensity of emotions	+1
slight positive intensity of emotions	+2
moderate positive intensity of emotions	+3
strong positive intensity of emotions	+4
very strong positive intensity of emotions	+5

Using the scale indicated in Table 1, the evaluation of the text "I believe that a cyber attack on critical infrastructure is a terrible and unacceptable thing. I am very concerned about the security of our country and think that everything possible should be done to prevent such attacks. If our systems are subjected to attacks, this could have serious consequences and even threaten national security" results in the vector (-4,1,0), which characterizes a strong negative attitude towards cyber threats to critical infrastructure. In the case of detecting a moderate or strong positive attitude towards cyber attacks on critical infrastructure, immediate decisions will need to be made to strengthen the cybersecurity of these objects.

When determining the emotional coloring of a text in sentiment analysis, a comprehensive approach is needed. As a valuable guide for mood analysis in [20], combining text with images is suggested.

Emoticons (a combination of the words "emotion" and "icon"), which are used by the majority of social media users in their comments, serve to strengthen the emotional coloring. Several examples of smileys and emoticons that can enhance the coefficients of negative and positive intensity shown in Table 1 above are shown in Table 2.

Table 2. The meaning of emoticons

image	graphic image	content	Indicator
=) :)		positive attitude towards the message	1
(:-E :E :-t]:->		negative attitude towards the message	-1
:- _. :-e		indifference	0

It is necessary to take into account the language in which the text is written and the social network in which there are specific features of emotional expression through emoticons. In addition, the method of analyzing profanity, which was proposed by the author in [21], can be used to determine the reinforcement of emotional attitudes towards the text.

As experts pointed out in [22, 23], determining emotional attitudes usually involves three stages, although some tasks may require more steps:

- firstly, the input text is divided into parts, such as sentences, and each segment is checked for tonality – whether the sentence is subjective or objective;
- secondly, subjective sentences are analyzed for tonality;
- thirdly, which is crucial for identifying potential cyber attacks on CII objects, an object may be identified regarding which an opinion is expressed.

The next step is building the neural network itself. Typically, for sentiment analysis, models with one or multiple layers of LSTM (Long Short-Term Memory) or GRU (Gated Recurrent Unit) are used, which are well-suited for working with sequential data such as text.

After constructing the network, it is necessary to train the model on the collected and labeled data using the chosen

algorithm, and evaluate the model's quality on test data that were not used during training. Various metrics are used to determine the training quality, depending on the objective, such as Accuracy, Precision, Recall, F1-Score, Mean Squared Error, Mean Absolute Error, and others.

After verifying the model's quality, it can be applied to analyze real-world data, such as user's messages, forum comments, and so on.

A crucial part of the model development process is its continuous improvement, as real data constantly changes and machine learning algorithms and technologies evolve. It is necessary to periodically update the model, incorporate new data, improve algorithms, and rectify errors.

IV. CREATION AND TRAINING OF THE MODEL

To implement the neural network, the object-oriented programming language Python is chosen. The dynamic typing and extensive functionality of built-in libraries, as well as additional modules and packages specifically designed for neural network development and machine learning, provide added convenience during the development process. Furthermore, Python is cross-platform, allowing it to run on different operating systems and hardware platforms, eliminating the need for software adaptation and reducing development costs.

The architecture of the neural network is implemented based on the TensorFlow library, which is used for building neural networks. The open-source Keras library, integrated with TensorFlow, is employed for rapid experimentation with neural networks (Fig. 3).

```
import pandas as pd
import numpy as np
import cv2
import tensorflow as tf
from tensorflow import keras
from tensorflow.keras.preprocessing.text import Tokenizer
from tensorflow.keras.preprocessing.sequence import pad_sequences
from tensorflow.keras.layers import Embedding, Bidirectional, LSTM, Dense
from tensorflow.keras.models import Sequential
import csv
#from tensorflow.keras.callbacks import TensorBoard
import matplotlib
```

Figure 3. Using standard Python libraries

The dataset for training the neural network was collected using web scraping with the BeautifulSoup library from social media platforms, including 2458 posts on Twitter and Instagram related to cyber attacks on critical infrastructure objects, taking into account emoticons. The dataset was evaluated by experts, considering Table 1, and divided into training and test sets in an 80:20 ratio. To assess the sentiment of emoticon images, they were processed using functions from the cv2 library and converted into numerical indicator values (Table 2) to refine the intensity of emotional coloring in the text (Table 1). Thus, the data set before starting the training of the neural network is submitted to the first layer already taking emoticons into account.

To regenerate response using the connected libraries (Fig. 3), an artificial neural network (ANN) is constructed, which includes the following layers:

- an embedding input layer for encoding words into fixed-length vectors, allowing text input to the model. It takes the vocabulary size (`vocab_size`), vector size

(`embedding_dim`), and maximum length of the input sequence (`max_length`) as parameters;

- bidirectional LSTM layers, each being a bidirectional LSTM. LSTM is a type of recurrent neural network capable of retaining and retrieving information about previous states. The first two LSTM layers return sequences at each time step, while the last LSTM layer returns the final output state;
- dense (fully connected) layers, each having different numbers of neurons and activation functions. The last dense layer contains a single neuron with the `relu` activation function, used for sentiment prediction.

Due to the fact that the application of ANNs in sentiment analysis has not yet been studied, various variants of the number of layers and neurons in them, various variants of activation functions and loss functions were used during the research, and the optimal version of the model was determined experimentally (Table 3).

Table 3. Variants of the model structure

Number of epochs	layer and number of neurons	Activation function	The amount of losses	Learning accuracy
20	Bidirectional1 (64)	tanh	0.6740	0.276543
	Bidirectional2 (32)	tanh		
	Bidirectional3 (16)	tanh		
	Dense1 (32)	sigmoid		
	Dense2 (16)	sigmoid		
20	Bidirectional1 (64)	sigmoid	0.9844	0.355687
	Bidirectional2 (32)	sigmoid		
	Bidirectional3 (16)	sigmoid		
	Dense1 (32)	sigmoid		
	Dense2 (16)	sigmoid		
...
10	Bidirectional1 (64)	tanh	0.8854	0.328721
	Bidirectional2 (32)	tanh		
	Bidirectional3 (16)	tanh		
	Dense1 (32)	sigmoid		
	Dense2 (16)	sigmoid		
10	Bidirectional2 (32)	tanh	0.3917	0.785234
	Bidirectional3 (16)	tanh		
	Dense1 (32)	relu		
	Dense2 (16)	relu		
	Dense3 (1)	relu		

The final version of the model with characteristics that gave the best result during the experiment is shown in Fig. 4.

```
model = Sequential([
    Embedding(vocab_size, embedding_dim, input_length=max_length),
    Bidirectional(LSTM(32, return_sequences=True)),
    Bidirectional(LSTM(16)),
    #Dense(32, activation='relu'),
    Dense(16, activation='relu'),
    Dense(1, activation='relu')
])
model.compile(loss='binary_crossentropy', optimizer='adam',
metrics=['accuracy'])
model.summary()
num_epochs = 10
history = model.fit(train_padded, train_data['label'], epochs=num_epochs,
validation_data=(test_padded, test_data['label']))
```

Figure 4. Characteristics of the created model

V. ANALYSIS OF THE RESULTS OF ANN CREATION AND TRAINING

The created model is a hybrid sequential recurrent-fully connected neural network, consisting of five layers with varying numbers of neurons and activation functions as indicated in Fig. 4. During the experiment and training process, it was observed that increasing the number of layers and neurons leads to overfitting of the model and inaccurate results. Increasing the number of epochs results in higher losses (Fig. 5), which is not aligned with the model's objective and reduces the accuracy of the target value.

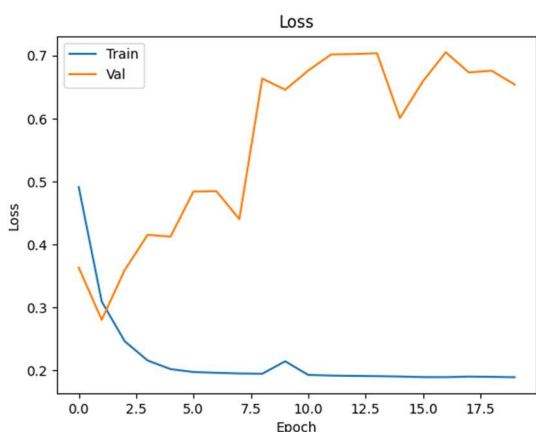


Figure 5. The number of losses for 20 epochs

Therefore, the optimal number of learning epochs is no more than 10, as can be seen on the graphs of model accuracy and losses during epochs (Fig. 6, 7).

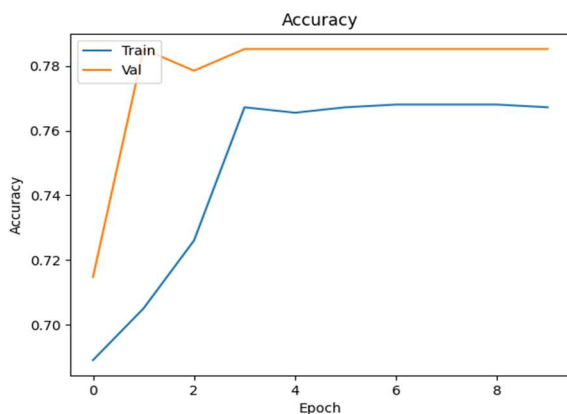


Figure 6. Increasing the accuracy of the model during training

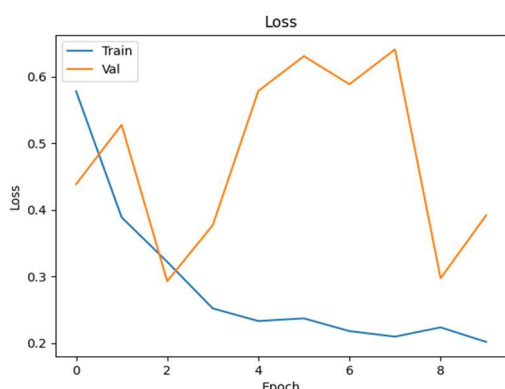


Figure 7. Reduction of model losses during training

After completing 10 epochs, the model's final accuracy (Test Accuracy) on the test dataset is 0.7852 (78.52%), with an optimal loss value of 0.3917. The output of the final testing of the model with floating-point summary shows that the model has successfully learned from the training data and possesses a certain level of universality and capability in assessing the sentiment towards cyber attacks on critical information infrastructure when evaluating the emotional intensity of messages on unseen data.

When evaluating the model on the control data, such as "destroy the bank's management system, 🌪️", "hack the defense ministry's website, 😊", and "take control of the workstation" the model assessed the sentiment towards cyber attacks, considering the emotional tone of the text, as "[[3.64187]]", which corresponds to reality. The value determined by the model on the scale (Table 1) corresponds to a strong emotional intensity in relation to carrying out cyber attacks and requires a response to such a level of threat (identifying the source of negative interest).

VI. CONCLUSIONS

The protection of critical information infrastructure has become one of the primary tasks of government agencies due to the development of information and communication technologies. One effective preventive measure in addressing these tasks is the detection of hidden attempts in social media to launch cyber attacks on critical infrastructure objects. An important tool for identifying hidden intentions is the application of sentiment analysis on message texts and online discussions. To monitor a large volume of information in cyberspace and assess the emotional sentiment towards cyber attacks, a sequential recurrent-fully connected artificial neural network has been developed using standard Python programming language libraries. The neural network takes into account the presence of emoticons during the evaluation process.

The training of the network over ten epochs and the evaluation of its performance on the test dataset showed a classification accuracy of 78.52% (or 0.7852) in identifying the emotional component of the text related to cyber attacks on critical infrastructure objects. Considering these results, it can be concluded that the network achieved relatively high accuracy on this test dataset. The confirmed effectiveness of the sentiment analysis model provides a basis for its potential application by cyber reconnaissance units for early detection of cyber attack capabilities. The advantages of the proposed approach in the created model of sentiment analysis are the consideration of graphic images of emoticons, which allows us to significantly expand the scope of determining the emotional relationship to objects of critical information infrastructure.

Further research will be focused on improving the model and refining the methodologies for its application by cyber divisions.

References

- [1] On critical infrastructure: Law of Ukraine dated November 16, 2021 No. 1882-IX. [Online]. Available at: <https://zakon.rada.gov.ua/laws/main/1882-20#Text> (date of application: 01.02.2023) (in Ukrainian).
- [2] T. J. Holt, M. Stonhouse, J. Freilich, S. M. Chermak, "Examining ideologically motivated cyberattacks performed by far-left groups," *Terrorism and Political Violence*, vol. 33, issue 3, pp. 527-548, 2021. <https://doi.org/10.1080/09546553.2018.1551213>.
- [3] M. Mundt, H. Baier, "Mapping cyber-physical threats for critical infrastructures," in: Hämmerli, B., Helmbrecht, U., Hommel, W., Kunczik, L., Pickl, S. (Eds.), *Critical Information Infrastructures Security, CRITIS, Lecture Notes in Computer Science*, vol. 13723.

Springer, Cham, 2022. https://doi.org/10.1007/978-3-031-35190-7_12.

[4] A. Marino, E. Zio, "A framework for the resilience analysis of complex natural gas pipeline networks from a cyber-physical system perspective," *Computers & Industrial Engineering*, vol. 162, 107727, 2021. <https://doi.org/10.1016/j.cie.2021.107727>.

[5] M. Domínguez, J. J. Fuertes, M. Prada, S. Alonso, A. Morán, D. Pérez, "Design of platforms for experimentation in industrial cybersecurity," *Appl. Sci.*, vol. 12, 6520, 2022. <https://doi.org/10.3390/app12136520>.

[6] A. Mottahedi, F. Sereshki, M. Ataei, A. N. Qarahasanlou, A. Barabadi, "The resilience of critical infrastructure systems: A systematic literature review," *Energies*, vol. 14, no. 6, 1571, 2021. <https://doi.org/10.3390/en14061571>.

[7] G. M. Makrakis, C. Koliás, G. Kambourakis, C. Rieger, J. Benjamin, "Industrial and critical infrastructure security: Technical analysis of real-life security incidents," *IEEE Access*, vol. 9, pp. 165295-165325, 2021. <https://doi.org/10.1109/ACCESS.2021.3133348>.

[8] Y. Geeta, P. Kolin, "Architecture and security of SCADA systems: A review," *International Journal of Critical Infrastructure Protection*, vol. 34, 100433, 2021. <https://doi.org/10.1016/j.ijcip.2021.100433>.

[9] M. Conti, D. Donadel, F. Turrin, "A survey on industrial control system testbeds and datasets for security research," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2248-2294, 2021. <https://doi.org/10.1109/COMST.2021.3094360>.

[10] M. Landauer, F. Skopik, M. Wurzenberger, A. Rauber, "System log clustering approaches for cyber security applications: A survey," *Computers & Security*, vol. 92, 101739, 2020. <https://doi.org/10.1016/j.cose.2020.101739>.

[11] V. Lakhno, B. Husiev, A. Blozva, D. Kasatkin, T. Osypova, "Clusterization of signs of network attacks in information security analysis problems," *Cyber Security: Education, Science, Technology*, vol. 1, issue 9, pp. 45-58, 2020. (in Ukrainian). <https://doi.org/10.28925/2663-4023.2020.9.4558>.

[12] A. Kuznetsov, V. Kalashnikov, R. Brumnyk, S. Kavun, "Editorial 'Computational aspects of critical infrastructures security', 'Security and post-quantum cryptography'", *International Journal of Computing*, vol. 19, issue 2, pp. 233-236, 2020. <https://doi.org/10.47839/ijc.19.2.1766>.

[13] K. Shaikat, S. Luo, S. Chen, D. Liu, "Cyber threat detection using machine learning techniques: A performance evaluation perspective," *Proceedings of the 2020 International Conference on Cyber Warfare and Security (ICWS)*, Islamabad, Pakistan, pp. 1-6, 2020. <https://doi.org/10.1109/ICWS48432.2020.9292388>.

[14] A. Gupta, P. Matta, B. Pant, "Identification of cybercriminals in social media using machine learning," *Proceedings of the 2022 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*, Bangalore, India, pp. 1-6, 2022. <https://doi.org/10.1109/SMARTGENCON56628.2022.10084119>.

[15] M. Asif, A. Ishtiaq, H. Ahmad, H. Aljuaid, "Sentiment analysis of extremism in social media from textual information," *Telematics and Informatics*, vol. 48, issue 3, 101345, 2020. <http://dx.doi.org/10.1016/j.tele.2020.101345>.

[16] K. Dotson, "Microsoft previews AI-powered security copilot to help cybersecurity staff," 2023 *SiliconANGLE Media Inc.* <https://siliconangle.com/2023/03/28/microsoft-previews-ai-powered-security-copilot-assist-cybersecurity-professionals/>.

[17] P. Rogov, B. Vorovych, V. Tkachenko, "Ways of ensuring the cyber security of objects of the state's critical information infrastructure in the military sphere," *Collection of scientific works of the Center for Military and Strategic Studies of the National Defense University of Ukraine named after Ivan Chernyakhovsky*, vol. 59, No. 1, 2017, pp. 64-72, (in Ukrainian). <https://doi.org/10.33099/2304-2745/2017-1-59/64-72>.

[18] S. Mazepa, L. Dostalek, O. Sharmar, S. Banach, "Cybercrime and vulnerability of critical information infrastructure of Ukraine," *Proceedings of the 2020 10th International Conference on Advanced Computer Information Technologies (ACIT)*, Deggendorf, Germany, pp. 783-786, 2020. <https://doi.org/10.1109/ACIT49673.2020.9208965>.

[19] L. Slipachuk, S. Tolyupa, V. Nakonechny, "Cybersecurity management process of critical infrastructure using an integrated management system of the national cyber security sector in Ukraine," *Proceedings of the 2019 3rd International Conference on Advanced Information and Communication Technologies (AICT)*, Lviv, Ukraine, 2019, pp. 451-454, <https://doi.org/10.1109/AIACT.2019.8847877>.

[20] D. Antonakaki, P. Fragopoulou, S. Ioannidis, "A survey of Twitter research: Data model, graph structure, sentiment analysis and attacks," *Expert Systems with Applications*, vol. 164, 114006, 2021. <https://doi.org/10.1016/j.eswa.2020.114006>.

[21] E. Pronoza, P. Panicheva, O. Koltsova, P. Rosso, "Detecting ethnicity-

targeted hate speech in Russian social media texts," *Information Processing and Management*, vol. 58, Issue 6, 102674, 2021. <https://doi.org/10.1016/j.ipm.2021.102674>.

[22] J.-H. Park, H.-Y. Kwon, "Cyberattack detection model using community detection and text analysis on social media," *ICT Express*, vol. 8, issue 4, pp. 499-506, 2022. <https://doi.org/10.1016/j.ict.2021.12.003>.

[23] J. Huang, Y. Meng, F. Guo, H. Ji, J. Han, "Weakly-supervised aspect-based sentiment analysis via joint aspect-sentiment topic embedding," *Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, pp. 6989-6999, 2020. <https://doi.org/2020.10.18653/v1/2020.emnlp-main.568>.



SVITLANA LEHOMINOVA, a Doctor of Economic Sciences, a Professor, Head of Department of Information and Cyber Security Management of the State University of Information and Communication Technologies. Scientific interests: economic security of the state, training of cyber security specialists, development of scientific methods of information and cyber

security management.



YURI SHCHAVINSKY, PhD, an Associate Professor of the Department of Information and Cyber Security Management of the State University of Information and Communication Technologies. Scientific interests: automated control systems, cyber security, information security, sentiment analysis, neural networks, artificial intelligence.

networks, artificial intelligence.



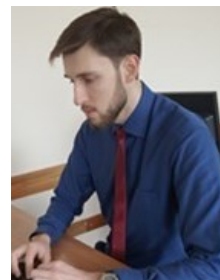
TETIANA MUZHANOVA, PhD, Associate Professor of the Department of Information and Cyber Security Management of the State University of Information and Communication Technologies. Scientific interests: application of scientific methods of managing information and cyber security of the state, training of cyber security specialists

management of the cyber security system of organizations.



DMYTRO RABCHUN, PhD, Associate Professor of the Department of Information and Cyber Security Management of the State University of Information and Communication Technologies. Scientific interests: technical systems of cyber security, management of cyber security of banks, application of monitoring systems in cyber security, improve-

ment of the cyber security system of organizations.



MYKHAILO ZAPOROZHCHENKO, an Assistant of the Department of Information and Cyber Security Management of the State University of Information and Communication Technologies. Scientific interests: cyber security management processes, methods of risk assessment in the field of information protection in organizations, formation of competence of cyber security specialists