Ministry of Education and Science of Ukraine
Black Sea Universities Network

ODESA NATIONAL UNIVERSITY OF TECHNOLOGY

International Competition of Student Scientific Works

BLACK SEA SCIENCE 2022

PROCEEDINGS

ODESA, ONUT 2022

Ministry of Education and Science of Ukraine

Black Sea Universities Network

Odesa National University of Technology

International Competition of Student Scientific Works

BLACK SEA SCIENCE 2022

Proceedings

Odesa, ONUT 2022

UDC 001.8(063)

Black Sea Science 2022: Proceedings of the International Competition of Student Scientific Works / Odesa National University of Technology; B. Iegorov, M. Mardar (editors-in-chief) [*et al.*]. – Odesa: ONUT, 2022. – 749 p.

Proceedings of International Competition of Student Scientific Works «Black Sea Science 2022» contain the works of winners of the competition.

The author of the work is responsible for the accuracy of the information.

Organizing committee:

Prof. Bogdan Iegorov, D.Sc., Rector of Odesa National University of Technology, Head of the Committee

Prof. Maryna Mardar, D.Sc., Vice-Rector for Scientific and Pedagogical Work and International Relations of Odesa National University of Technology, Deputy Head of the Committee

Prof. Baurzhan Nurakhmetov, D.Sc., First Vice-Rector of Almaty Technological University (Kazakhstan)

Prof. Michael Zinigrad, D.Sc., Rector of Ariel University (Israel)

Prof. Plamen Kangalov, Ph.D., Vice-Rector for Academic Affairs of "Angel Kanchev" University of Ruse (Bulgaria)

Prof. Heinz Leuenberger, Ph.D., Professor of the Institute of Ecopreneurship of University of Applied Sciences and Arts (Switzerland)

Prof. Edward Pospiech, Dr. habil., Professor of the Institute of Meat Technology of Poznan University of Life Sciences (Poland)

Prof. Lali Elanidze, Ph.D., Professor of the Faculty of Agrarian Sciences of Iakob Gogebashvili Telavi State University (Georgia)

Dr. Dan-Marius Voicilas, Ph.D., Associate Professor of the Institute of Agrarian Economics of Romanian Academy (Romania)

Prof. Stefan Dragoev, D.Sc., Vice-Rector for Scientific Work and Business Partnerships of University of Food Technologies (Bulgaria)

Prof. Jacek Wrobel, Dr. habil., Rector of West Pomeranian University of Technology (Poland)

Dr. Mei Lehe, Ph.D., Vice-President of Ningbo Institute of Technology, Zhejiang University (China)

Dr. V. Kozhevnikova, Ph.D., Associate Professor of the Department of Hotel and Catering Business of Odesa National University of Technology, Secretary of the Committee

INTRODUCTION

International Competition of Student Scientific Works “Black Sea Science” has been held annually since 2018 at the initiative of Odesa National University of Technology (formerly Odesa National Academy of Food Technologies) with the support of the Ministry of Education and Science of Ukraine. It has been supported by Black Sea Universities Network (the Association of 110 higher education institutions from 12 countries of the Black Sea Region) since 2019, and by Iseki-FOOD Association (European Integrating Food Science and Engineering Knowledge into the Food Chain Association) since 2020.

The goal of the competition is to expand international relations and attract students to research activities. It is held in the following fields:

- Food science and technologies
- Economics and administration
- Information technologies, automation and robotics
- Power engineering and energy efficiency
- Ecology and environmental protection

The jury includes both Ukrainian and foreign scientists. In the 4 years that the competition has been held, the jury included scientists from universities of 24 countries: Angola, Azerbaijan, Benin, Bulgaria, China, Czech Republic, France, Georgia, Germany, Greece, Israel, Italy, Kazakhstan, Latvia, Lithuania, Moldova, Pakistan, Poland, Romania, Serbia, Slovakia, Switzerland, Turkey, USA.

At the same time, every year the geography has expanded and the number of foreign jury members has increased: from 46 jury members representing 25 universities from 12 countries in 2018, to 73 jury members of the 46 universities from 19 countries in 2022.

More than a thousand student research papers have been submitted to the competition from both Ukrainian and foreign institutions from 25 countries: China, Poland, Mexico, USA, France, Greece, Germany, Canada, Costa Rica, Brazil, India, Pakistan, Israel, Macedonia, Lithuania, Latvia, Slovakia, Romania, Kyrgyzstan, Kazakhstan, Bulgaria, Moldova, Georgia, Turkey, Serbia.

The interest of foreign students in the competition grew every year. In 2018, the students representing 15 institutions from 7 countries have submitted 33 works. In 2021 the number of submitted works increased to 73, authored by the students of 40 institutions from 18 countries.

The competition is held in two stages. In the first stage, student research papers are reviewed by members of the jury who are experts in the relevant fields. In the second stage of the competition, the winners of the first stage have the opportunity to present their work to a wide audience in person or online.

All participants of the competition and their scientific supervisors are awarded appropriate certificates, and the scientific works of the winners are included in the electronic proceedings of the competition. Every year the competition receives a large number of positive responses from Ukrainian and foreign colleagues with the desire to participate in the coming years.

3. INFORMATION TECHNOLOGIES, AUTOMATION AND ROBOTICS

RESEARCH APPLICATION OF THE SPAM FILTERING AND SPAMMER DETECTION ALGORITHMS ON SOCIAL MEDIA

Author: Vasyl Oliinyk
Advisors: Andrii Podorozhniak,
Nataliia Liubchenko
National Technical University «Kharkiv Polytechnic Institute» (Ukraine)

Abstract: *There are a bunch of different social networks and messengers today, which in times of pandemic corona-virus have take a really big part of our entire live, especially in our work activities. Besides that, the problem with the spam and spammers is the most relevant than ever, the count of spam in the work text stream is continuously increased.*

Under spam we understand the text content that is not necessary in the particular text stream, in case of spammer it is meant the person that is sending the spam messages in his or her own purposes.

The project was design to solve the scientific and applied problem of detecting spammers and identifying spam messages in the text context of any social network or messenger using various spam detection algorithms and spammer detection approaches. We have implemented 4 algorithms: an algorithm using naive Bayesian classifier, Support-vector machine, multilayer perceptron neural network and convolution neural network.

The project was developed in purpose of implementing a spam detection algorithm that is easy to integrate in a messenger (in our case we used Telegram as an example). Design algorithm recognizes spam based on the context of a particular text stream, deletes the spam message and blocks the spammer until one of the application managers unblock the spammer-user. Since the spam detection task is essentially the task of sorting messages into two classes, the usage of the design application is not limited to dealing with spam.

Keywords: *spam, social network, naive Bayesian classifier, Support-vector machine, multilayer perceptron neural network, convolution neural network, spammers detection.*

I. INTRODUCTION

Thanks to various anti-spam and spammer algorithms, the share of spam in global email traffic in 2020 was down by 6.14 p.p. when compared to the previous reporting period, averaging 50.37% [1] (Fig. 1.1).

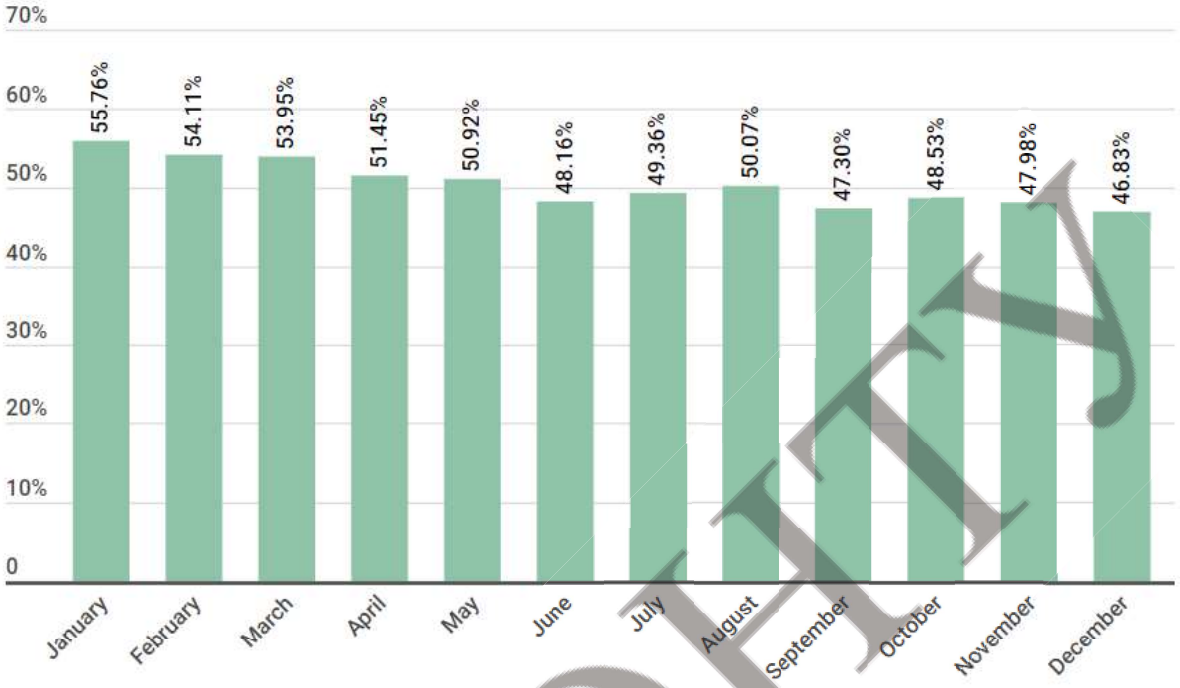

Fig 1.1. Percentage of spam in email traffic in 2020

Most probably only inboxes have built-in the anti-spam algorithms, the others chat rooms do not have such functionality. It can be the reason why the spam percentage in the mail-boxes and others message is mostly the same. For instance, the malicious link injected to the message and sent to the company employ can be a big danger for the whole company. Therefore, our today's world has an issue of monitoring the incoming text stream in social networks and messengers. Is also necessary to identify and ban spammers, this facilitates the work of algorithms and complicates the life of spammers, and the most important is that it reduce the share of the spam as we see from Fig. 1.1.

The ability to filter spam messages, identify and ban spammers in messengers and social networks can save a bunch of humanity time and prevent loss of information and money.

To solve the problem we used algorithms using a naive Bayesian classifier, support vector method, multilayer perceptron neural network and convolution neural network. We also developed a simple algorithm that identifies and blocks the user that was recognized as a spammer. An approach with integrated application of the investigated algorithms can begin to solve the problem of spam in social networks and messengers.

II. LITERATURE ANALYSIS

2.1. Characterization of spam. Ways to deal with spam

Let's start and firstly discuss what is the spam actually. Spam is a mass mailing of correspondence of an advertisement to people who have not expressed a desire to receive it [2].

Here is the different types of spam: advertisements; phishing; Nigerian emails; mass mailings of letters with religious content; mass mailings to put the mail system out of service (causing the system crush); mass mailings of letters containing computer viruses (for their initial spread); mass mailings on behalf of another person in order to cause a negative attitude towards that person;

The most popular spam spreading methods are the following [2, 3]: e-mail; usernet; messengers; substitution of Internet traffic; SMS messages; phone calls, etc.

The receiver of the spam usually has to pay the Internet provider for the time used to receive the spam, in the same time for sender of the spam messages it costs almost nothing. Th load traffic is also messed up because of the mass spread of spam, it also complicates the operation of information systems and resources. Due to mass mailings the user has to spend unnecessary time filtering the messages. To avoid this, we use anti-spam filters to save our time. But spam filters can also accidentally erase an important message by recognizing it as spam.

The surest way to deal with spam is to prevent spammers from getting your email address.

Auto-Spam Detection Software is called Anti-Spam Filters. They can be applied by end-users or on servers. This software has two main approaches [4]:

1) the content of the message is analyzed and based on the algorithm decides whether it is spam or not. If a message is classified as spam, it can be marked, moved to another folder, or even deleted. Such software can run both on the server and on the client computer. With this approach you don't see the spam filtered, but you continue to pay the full cost for receiving it, because the anti-spam software receives each spam message anyway (wasting your money) and only then decides whether to show it or not;

2) it classifies the sender as a spammer without looking at the text of the message. This software can only work on the server which directly receives the messages. With this approach it's possible to reduce the cost - money is only spent on communicating with spam mailers (i.e. refusing to accept the messages) and on contacting other servers for verification. The gain, however, is not as great as you might expect. If the recipient refuses to accept the message, the spammer program tries to bypass the protection and send it another way. Every such attempt has to be handled separately, which adds to the overhead on the server.

This project discusses a statistical Bayesian spam filtering method using a support vector method and a multilayer perceptron neural network.

2.2. Analysis of spam detection algorithms. Naive Bayesian classifier

A naive Bayesian classifier is a probabilistic classifier that uses Bayes theorem to determine the probability of an observation (sample element) belonging to one of

the classes under the assumption of (naive) independence of the variables [5]. Here are the examples of the method usage: recognizing spam, analyzing emotional coloring of texts, detecting racism in text voters, any information processing systems and the like.

Classification on new examples is performed with Bayes' rule by selecting the class that is most likely to have generated the example [6].

The naive Bayes classifier is the simplest of these models, in that it assumes that all attributes of the examples are independent of each other given the context of the class. This is the so-called "naive Bayes assumption" [7].

While this assumption is clearly false in most real-world tasks, naive Bayes often performs classification very well.

Mathematically Bayes' theorem is [8]:

$$P(A \mid B) = \frac{P(B \mid A)\, P(A)}{P(B)} \quad (2.1)$$

where A and B are events:

– P (A) and P (B) are the probabilities of A and B without relation to each other;

– P (A | B) is the probability of observing event A if B is true;

– P (B | A) is the probability of observing event B if A is true.

2.3. Analysis of spam recognition algorithms. Support-vector machine

A support vector machine (SVM) is a supervised machine learning algorithm that can be used for both classification and regression tasks. In SVM, we plot data points as points in an n-dimensional space (n being the number of features you have) with the value of each feature being the value of a particular coordinate. The classification into respective categories is done by finding the optimal hyperplane that differentiates the two classes in the best possible manner [9, 10].

Hyperplanes can be considered decision boundaries that classify data points into their respective classes in a multi-dimensional space. Data points falling on either side of the hyperplane can be attributed to different classes.

For a given set of training samples, each marked as appropriate to one or the other of two categories, the SVM training algorithm builds a model that assigns new samples to one or the other category, making it a probabilistic binary linear classifier. (Fig. 2.1).

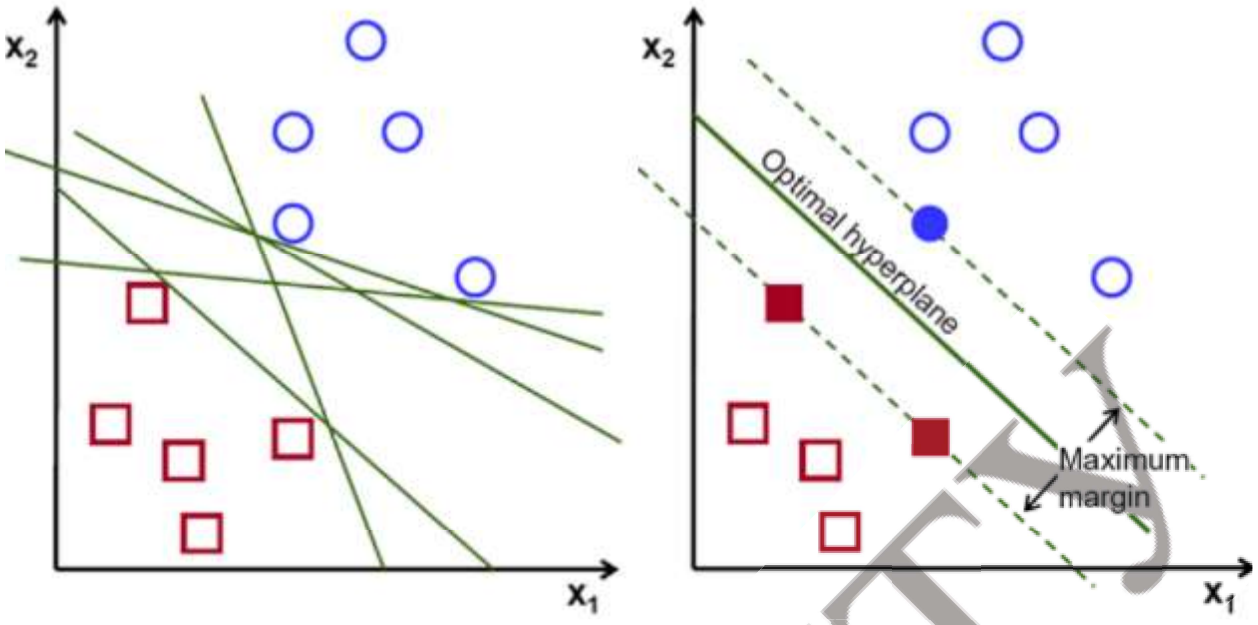

Fig. 2.1. SVM deals with linearly separate data

There are a bunch of cases when the data are not linearly separable. For this reason, it has been proposed to map the primary finite-dimensional space into a space with more dimensions, presumably making splitting easier in this space (Fig. 2.2).

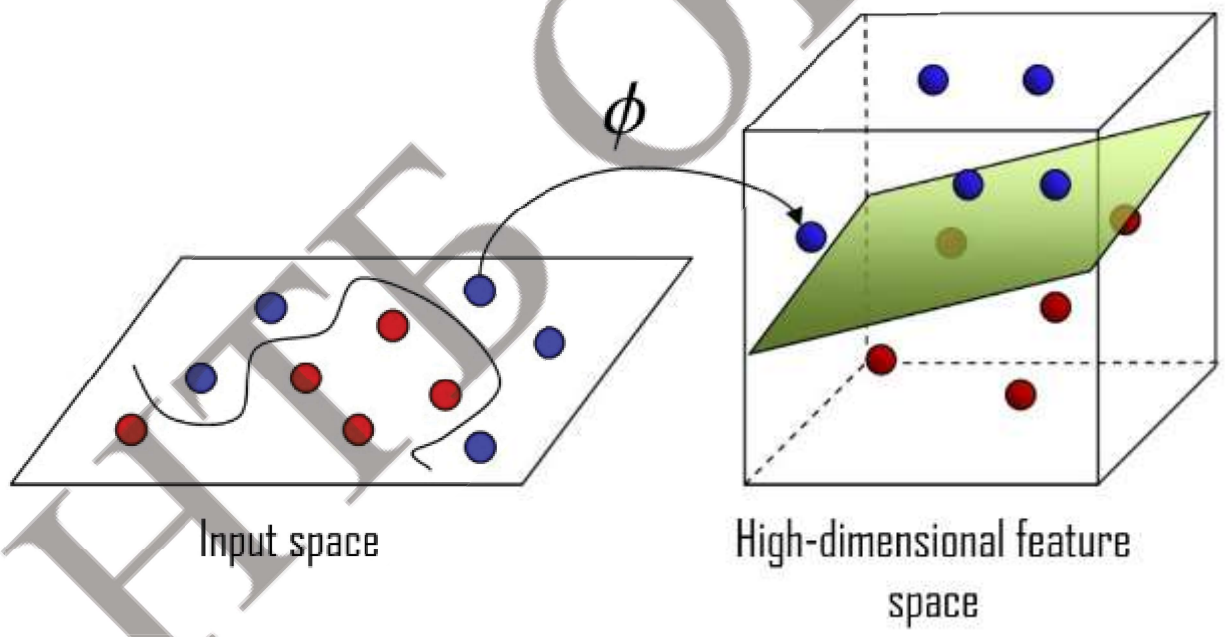

Fig. 2.2. Linearly inseparable data

2.4. Analysis of spam recognition algorithms. Perceptron

A Perceptron is an algorithm used for supervised learning of binary classifiers. Binary classifiers decide whether an input, usually represented by a series of vectors, belongs to a specific class. In short, a perceptron is a single-layer neural network. They consist of four main parts including input values, weights and bias, net sum, and an activation function [11, 12].

The process begins by taking all the input values and multiplying them by their weights. Then, all of these multiplied values are added together to create the weighted sum. The weighted sum is then applied to the activation function, producing the perceptron's output. The activation function plays the integral role of ensuring the output is mapped between required values such as (0,1) or (-1,1). It is important to note that the weight of an input is indicative of the strength of a node. Similarly, an input's bias value gives the ability to shift the activation function curve up or down [13].

Fig. 2.4 shows a model of the basic perceptron.

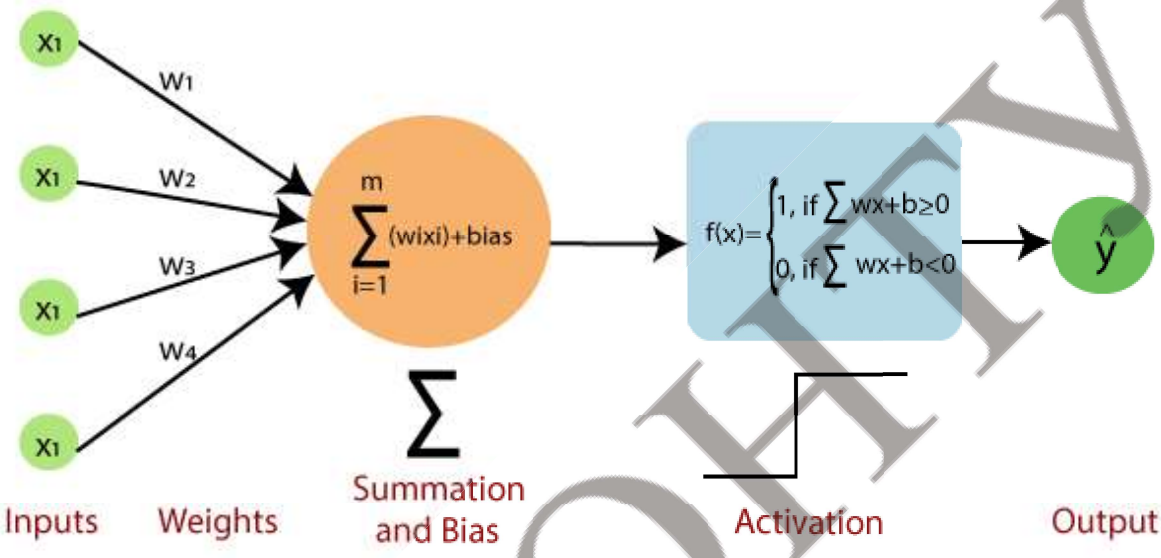

Fig. 2.4. Logic diagram of the basic perceptron

2.5. Analysis of spam recognition algorithms. CNN

Convolutional neural network, (CNN) – special architecture of artificial neural networks, proposed by Jan Lekun in 1988 [14] and aimed at effective pattern recognition, is part of Deep learning technologies. The structure of the network is unidirectional, without feedback, fundamentally multilayered.

CNN is designed to automatically and adaptively learn spatial hierarchies of features through backpropagation by using multiple building blocks, such as convolution layers, pooling layers, and fully connected layers [15].

The structure of the CNN we used is shown in Fig. 2.5.

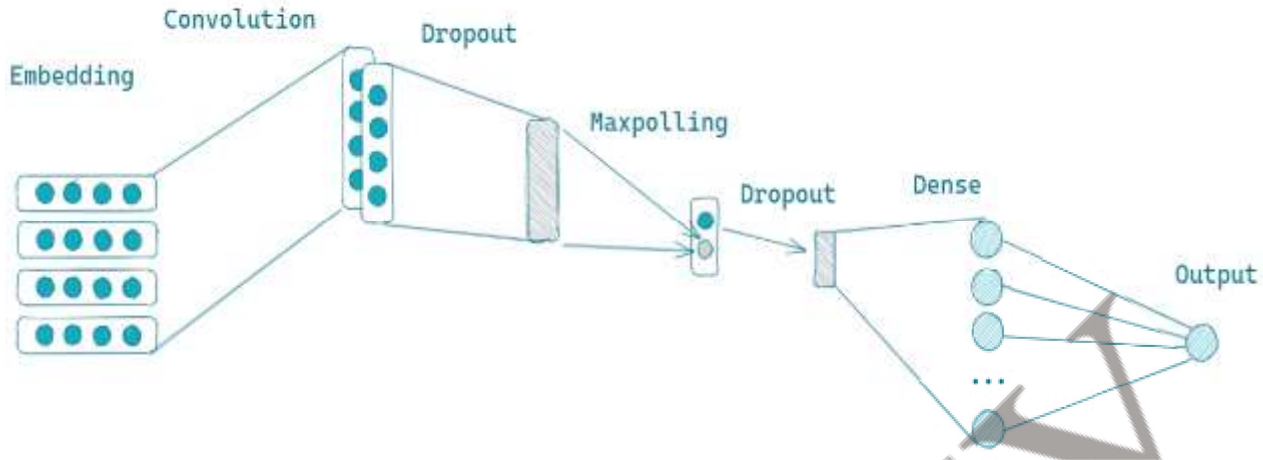

Fig. 2.5. The structure of the used CNN.

III. DETECTION AND BLOCKING OF SPAMMERS

3.1. Basic Spammer Detection Methods

Fake Content Based Spammer Detection [16]: “Gupta" performed an in-depth characterization of the components that are affected by the rapidly growing malicious content. It was observed that a large number of people with high social profiles were responsible for circulating fake news. To recognize the fake accounts, the authors selected the accounts that were built immediately after the Boston blast and were later banned by Twitter due to violation of terms and conditions. About 7.9 million distinctive tweets were collected by 3.7 million distinctive users. This dataset is known as the largest dataset of the Boston blast. The authors performed the fake content categorization through temporal analysis.

The aspects that were taken into account during spammer detection:

1) the average number of the verified accounts (spam / non-spam);

2) the number of followers of the account;

3) the fake content propagation metrics, such as: global engagement, topic engagement, likability and credibility.

Fake User Identification [16]: A categorization method is proposed by Erşahin to detect spam accounts on Twitter. The dataset used in the study was collected manually. The classification is performed by analyzing user-name, profile and background image, number of friends and followers, content of tweets, description of account, and number of tweets. The dataset comprised 501 fake and 499 real accounts, where 16 features from the information that were obtained from the Twitter APIs were identified. Two experiments were performed for classifying fake accounts. The first experiment uses the Naïve Bayes learning algorithm on the Twitter dataset including all aspects without discretization, whereas the second experiment uses the Naïve Bayes learning algorithm on the Twitter dataset after the discretization.

Detecting Spam In Trending Topic [16]. It is a method which is classified on the basis of two new aspects. The first one is the recognition of spam tweets without any

prior information about the users and the second one is the exploration of language for spam detection on Twitter trending topic at that time.

IV. OBJECT, SUBJECT AND METHODS OF RESEARCH

The aim of the work is to study the possibility of using different algorithms in the development of software for filtering spam in the textual content of social network messengers, quickly reacting to the spam message and identifying spammers.

The aim is to do the following tasks:

a) the analysis of the special possibilities of the recognition of spam messages;

b) the analysis of the existing methods of spam recognition;

c) the realization of the methods of combating spam based on the naive Bayesian Classifier, the method of reference vectors and multilayers perceptron neural network;
d) the analysis of the used algorithms;

e) the analysis of the basic existing spam detection algorithms;

f) the implementation of the spammer detection.

The object of the research is the process of identifying spam in the text context of SOCIAL networks messengers.

Subject of study – the process of filtering spam messengers in social networks using the base of methods for recognizing spam and spammer identifying and banning.

Research methods: classification theories, probabilistic classifiers, the theory of neural quantities, statistical methods of analysis of linguistic methods, spammer detection.

Scientific novelty – improved methods for the recognition of spam in the messenger using text messages of a particular text stream, identifying spammers and reacting to messages from spammers.

V. RESULTS

As a training dataset was chosen the dataset of spam messages from the kaggle SMS Spam Collection Dataset, but the dataset of messages from a particular company can also be used to train the algorithm [17]. To implement the spam filtering algorithms, we used the Python 3.6 programming language, the PyCharm. programming environment and the Keras, NumPy, Sklearn and Pandas libraries, MySQL DB for storing spammers and all users of the text stream [18, 19].

The simulation was performed on a LifeBook E744 notebook with 8Gb RAM, an Intel Core i7 CPU (up to 3.2 GHz) and an Intel HD Graphics 4600 video processor.

The spam message analyzing process is shown in Figure 5.1.

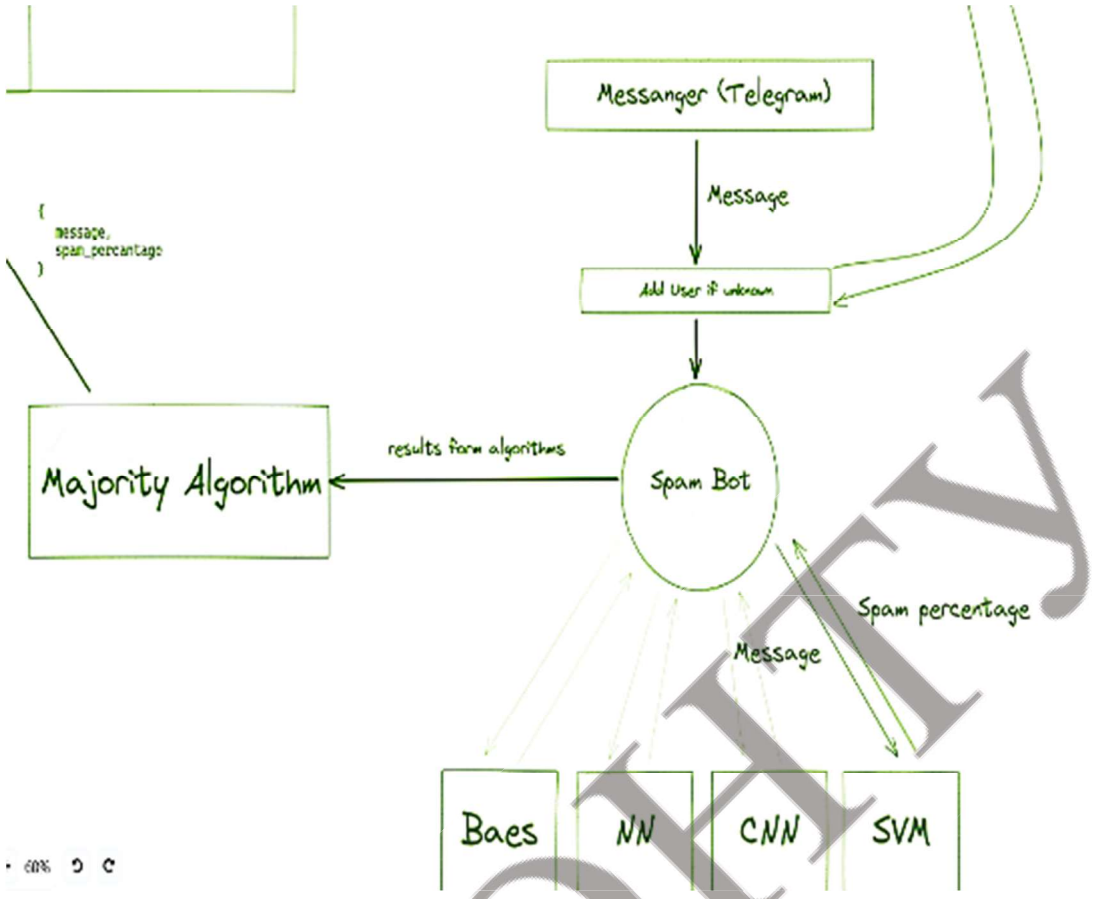

Fig. 5.1. The spam message analyzing process

We used 4 most popular spam recognition algorithms: Naïve Baes Classifier, Perceptron, Convolution Neural Network and Support Vector Machine.

We get the message from the user (in our case, form Telegram user) then if the user is unknown in our system, we add him to our database (DB) with all of the users of the application, after that we analyze the message using all of the existing algorithms, passing the results from all algorithms to the Majority algorithm we calculate the spam percentage of the message [20].

Then the result of the Majority Algorithm is passed to the Spam Analyzer, which decides if the user that sent the message is spammer or not based on the provided spam percentage of the message and two last predictions. So to identify the user as a spammer we analyze his 3 last messages and if the average spam percentage is bigger than specified edge, we recognize the user as a spammer and put his id to the DB with spammers.

The proposed complex majority algorithm shown in Figure 5.2 uses as inputs for the majority scheme the solutions of the Bayesian spam filtering method, Perceptron, Support vector method and Convolutional neural network algorithms. To match the outputs of the algorithmic blocks (0… 1) with the inputs of the majority scheme (0, 1), their binarization with a threshold of 0.95 is performed.

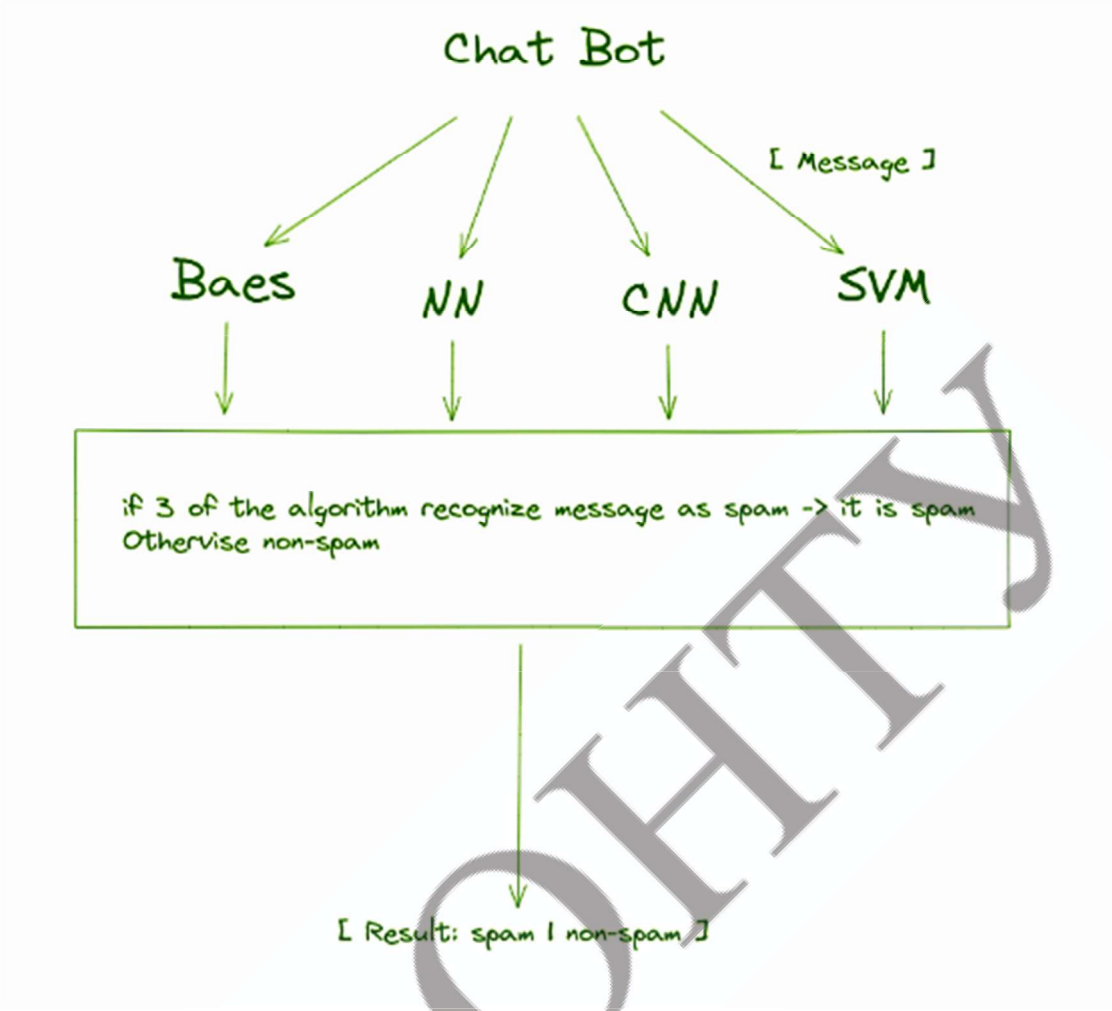

Fig. 5.2. The majority algorithm process

The results of the complex algorithm of antispam bot in the form of an estimate of the probabilistic of correct spam recognition for the test samples are shown in Figure 5.3.

```
mistake: 0.0317
acc: 99.9683
```

Fig. 5.3. The results of recognition of the complex algorithm of antispam bot

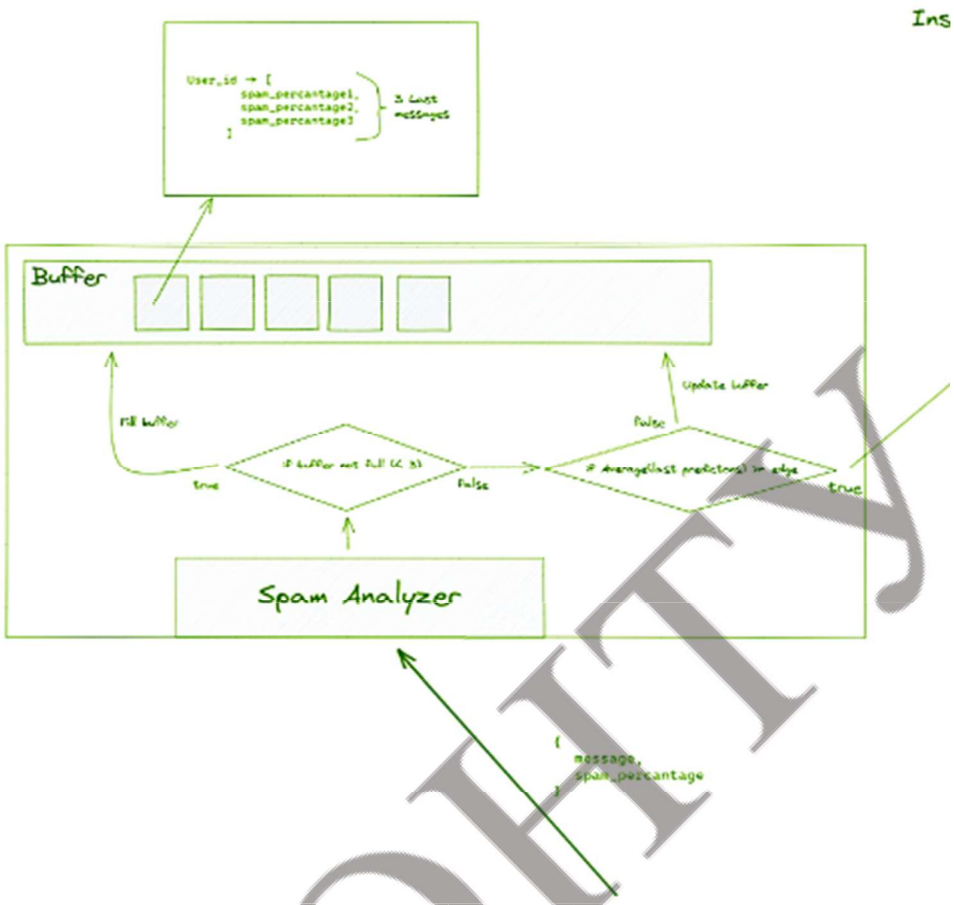

Fig. 5.4. The implementation of the spam analyzing, spammer analyzing.

If a user is in the spammers DB his messages are being deleted without even analyzing them. The user receives the message that he was blocked. Only the manager of the application is able to remove users from the spammers.

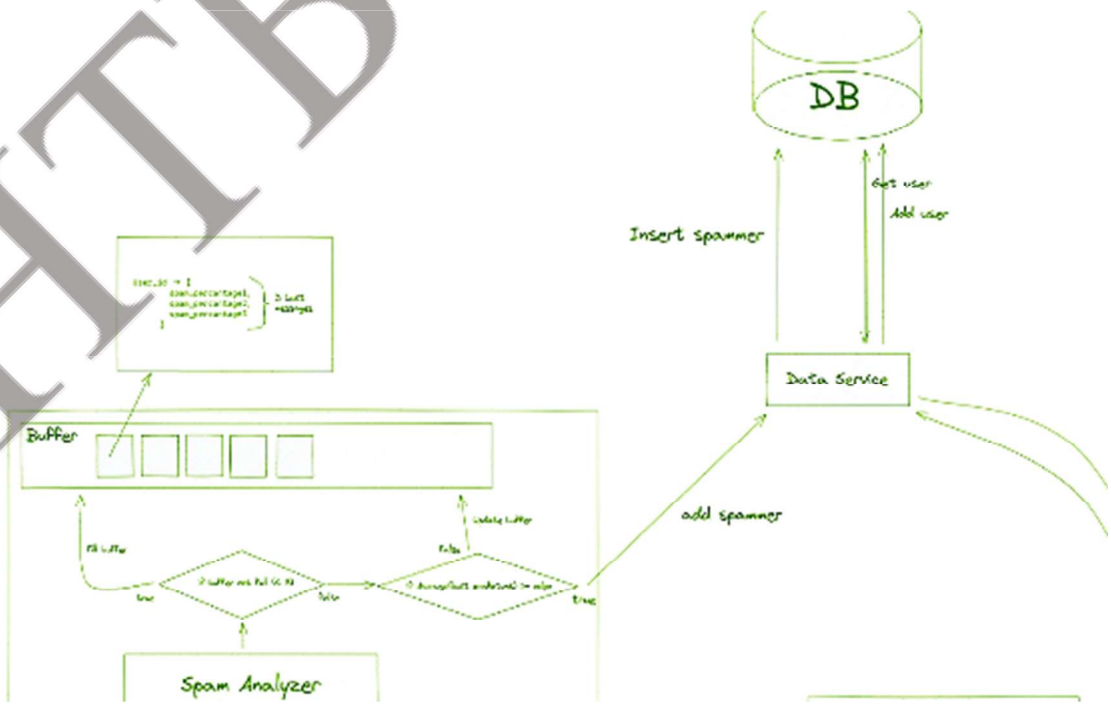

Fig. 5.5. The process of putting spammers to the DB. The communication of the spam analyzer and the DB.

The general scheme of execution of the developed software application is given in Fig 5.6 [21, 22].

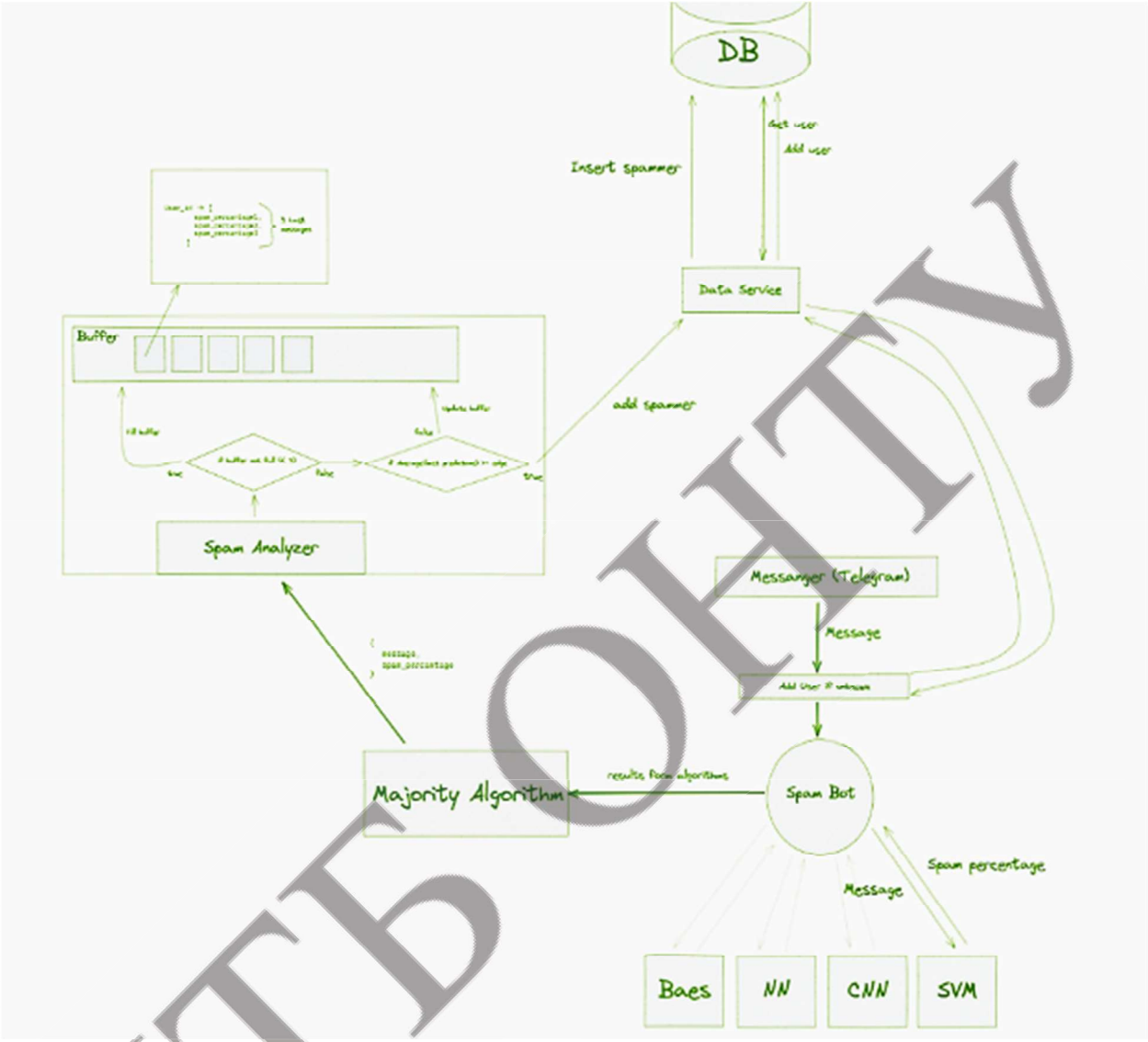

Fig. 5.6. The general scheme of execution of the developed software application

Algorithm of analyzing spam messages contains the following steps:

1) the user enters into the software application the initial text that should be analyzed;

2) software application parses the initial text into array of words, then each word is converted to the infinitive, then the resulting set of words is vectorized and transmitted to the input to the all of the used algorithms;

3) the algorithms analyze the received data and returns the result as the probability of belonging the received data to the class (each algorithm has two classes: spam and non-spam);

4) the received data passed through the Majority Algorithm to calculate the spam percentage;

5) the app decides if the user should be marked as spammer based on the last 3 spam prediction of his messages;

6) if the user was identified as a spammer he is blocked.

VI. TESTING AND COMPARISON

Also, in addition to the usual accuracy metric for evaluating selected algorithms, we used F1 score.

Accuracy is a ratio between the correctly classified samples to the total number of samples. Nowadays it is the most used metric of classification performance.

$$accuracy = \frac{TP + TN}{TP + FN + TN + FP} \quad (1)$$

where TP – (True Positive) correctly classified positive sample;

FN – (False Negative) the sample is positive but it is classified as negative;

TN – (True Negative) the sample is negative and it is classified as negative;

FP – (False Positive) the sample is negative but it is classified as positive.

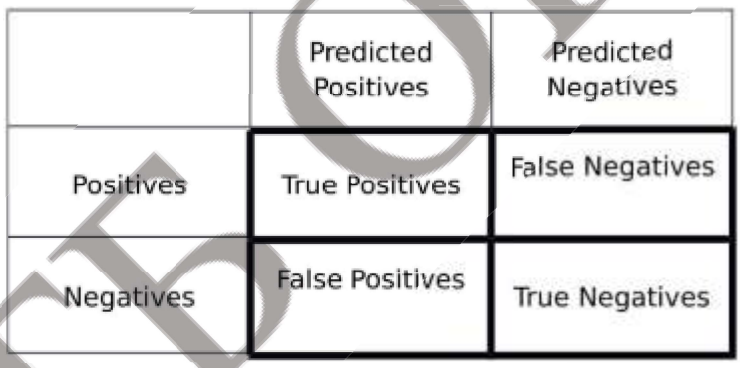

Fig. 6.1. The explanation of accuracy evaluation

The results of the tests using accuracy metric are shown at Table 6.1.

Table 6.1. The results of the testing algorithms on training and test samples

Algorithm	Training sample	Test sample
Bayes	0.988	0.982
SVM	0.998	0.989
NN	0.997	0.979
CNN	0.990	0.985
Majority	1.000	0.999

VII. CONCLUSIONS

As part of this research, the scientific and applied problem of determining spam in the textual context of social networking messengers was solved by the example of Kaggle SMS Spam Collection Dataset using chatbots in the popular messenger Telegram. Besides that, the basic spam detection algorithms were analyzed and the one was implemented in the application.

1. Considered the relevance of spam detection and possible problems due to spam intervention.

2. Consider the basic methods of spam recognition, namely naive Bayesian classifier, the method of support vectors, multilayer perceptron neural network and convolution neural network.

3. Consider the basic methods of spammer detection.

4. It was developed a program to filter spam and spammers detection in the messenger Telegram, that uses 4 implemented algorithms for spam recognition and proposed complex majority algorithm. All of the text traffic is also checked for the spammers.

VIII. REFERENCES

1. Kulikova, T., Shcherbakova, T., & Sidorina, T. (2021, February 15). Spam and phishing in 2020. https://securelist.ru/spam-and-phishing-in-2020/100408/.

2. Liu, B., Blasch, E., Chen, Y., Shen, D., & Chen, G. (2013). Scalable sentiment classification for Big Data analysis using Naïve Bayes Classifier. *Proceedings of the IEEE International Conference on Big Data*, USA, pp. 99-104. https://doi.org/10.1109/BigData.2013.6691740.

3. Chaudhry, S., Dhawan, S., & Tanwar, R. (2020). Spam Detection in Social Network Using Machine Learning Approach. In: U. Batra, N. Roy, & B. Panda (Eds.), *Data Science and Analytics. REDSET 2019. Communications in Computer and Information Science*. Vol. 1230, pp. 236-245. Springer. https://doi.org/10.1007/978-981-15-5830-6_20.

4. (2019, July 22). What is spam and how to fight it? https://www.ukraine.com.ua/uk/blog/marketing/chto-takoe-spam-i-kak-s-nim-borotsya.html.

5. Sarkar, S.D., Goswami, S., Agarwal, A., & Aktar, J. (2014). A Novel Feature Selection Technique for Text Classification Using Naive Bayes, International Scholarly Research Notices, 2014, Article 717092. https://doi.org/10.1155/2014/717092.

6. McCallum, A., & Nigam, K. (1998). A Comparison of Event Models for Naive Bayes Text Classification. *AAAI 1998: Learning for Text Categorization* (pp. 41-48). http://courses.washington.edu/ling572/papers/mccallum1998_AAAI.pdf.

7. Zhang, W., & Gao, F. (2013). Performance analysis and improvement of naïve Bayes in text classification application, *Proceedings of the IEEE Conference Anthology*, China, pp. 1-4. https://doi.org/10.1109/ANTHOLOGY.2013.6784818.

8. CFI. Formula for Bayes' Theorem. https://corporatefinanceinstitute.com/resources/knowledge/other/bayes-

theorem/#:~:text=Formula%20for%20Bayes'%20Theorem&text=P(A%7CB)%20%E2%80%93,the%20probability%20of%20event%20B.

9. Nguyen, L. (2017). Tutorial on Support Vector Machine. Applied and Computational Mathematics, 6(4), 1–15. https://doi.org/10.11648/j.acm.s.2017060401.11.

10. Sastry, P. S. (2003). An Introduction to Support Vector Machines. http://www2.cs.uh.edu/~ceick/DM/Sastry_svm_notes.pdf.

11. Toward data science. What is the Perceptron, https://towardsdatascience.com/what-the-hell-is-perceptron-626217814f53.

12. Chollet, F. (2018). *Deep learning with python.* Manning Publications. https://www.manning.com/books/deep-learning-with-python.

13. DeepAI, Perceptron, https://deepai.org/machine-learning-glossary-and-terms/perceptron.

14. LeCun, Y., Bottou, L., Bengio, Y., & Haffner P. (1998). Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, 86 (11), pp. 2278–2324. https://doi.org/10.1109/5.726791.

15. Yaloveha, V., Hlavcheva, D., & Podorozhniak, A. (2019). Usage of convolutional neural network for multispectral image processing applied to the problem of detecting fire hazardous forest areas. *Advanced Information Systems*, 3, 1, pp. 116-120. https://doi.org/10.20998/2522-9052.2019.1.19.

16. Masood, F., Ammad, G., Almogren, A., Abbas, A., & Zuair, M. (2019). Spammer Detection and Fake User Identification on Social Networks, *IEEE Access,* vol. 7, pp. 68140-68152. https://doi.org/10.1109/ACCESS.2019.2918196.

17. SMS Spam Collection Dataset [Data set]. https://www.kaggle.com/uciml/sms-spam-collection-dataset.

18. Python For Beginners. *Python Software Foundation*. https://www.python.org/about/gettingstarted/.

19. Applications for Python. *Python Software Foundation*. https://www.python.org/about/apps/.

20. Oliinyk V., Liubchenko N., & Podorozhniak A. (2021). Research of antispam bot algorithms for social networks. *CEUR Workshop Proceedings*. Vol. 2870, pp. 822-831. http://ceur-ws.org/Vol-2870/paper61.pdf.

21. Oliinyk, V., Podorozhniak, A., & Liubchenko, N. (2020). Method of comprehensive spam recognition in social networks. *Proceedings of the 8th international scientific and technical conference Problems of informatization*, Ukraine, *Vol. 2,* p. 39. http://repository.kpi.kharkov.ua/bitstream/KhPI-Press/52856/1/Oliinyk_Method_comprehensive_2020.pdf.

22. Oliinyk, V., Liubchenko, N., & Podorozhniak, A. (2021). Spam recognition and spammers detection. *Proceedings of the 9th international scientific and technical conference Problems of informatization*, Ukraine, Vol. 1, p. 46. http://repository.kpi.kharkov.ua/bitstream/KhPI-Press/54913/1/Conference_NTU_KhPI_2021_Problemy_informatyzatsii_Ch_1.pdf.

RESEARCH APPLICATION OF THE SPAM FILTERING AND SPAMMER DETECTION ALGORITHMS ON SOCIAL MEDIA
Author: Vasyl Oliinyk
Advisors: Andrii Podorozhniak, Nataliia Liubchenko
National Technical University «Kharkiv Polytechnic Institute» (Ukraine)…….. 480

SYNTHESIS OF THE CONTROL SYSTEM WITH NEUROCONTROLLER
Author: Sholopko Dmitry
Advisor: Gurskiy Alexander
Odessa National Technological University (Ukraine)…….. 495

4. POWER ENGINEERING AND ENERGY EFFICIENCY……508

INFLUENCE OF HEATING AND VENTILATION MODES ON THE ENERGY CONSUMPTION OF UNIVERSITY EDUCATIONAL BUILDINGS UNDER QUARANTINE CONDITIONS IN UKRAINE
Author: Tetiana Boiko
Advisors: Inna Bilous, Valerii Deshko
National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute»…… 509

ENERGY EFFICIENT CIRCUIT SOLUTIONS FOR LOW-TEMPERATURE REFRIGERATION MACHINES BASED ON ENVIRONMENTALLY FRIENDLY REFRIGERANTS
Author: Daniil Pylypenko
Advisors: Viktor Kozin
Sumy State University (Ukraine)…….. 526

ANALYTICAL STUDY OF THE THERMAL CONDUCTIVITY PROCESSES AT CERAMIC SINTERING
Author: Marina Grechanovskaya
Advisors: Heorhiiesh Kateryna, Natalya Volgusheva
Odessa State Academy of Civil Engineering and Architecture (Ukraine)……. 540

HELIUM PRODUCTION FROM NATURAL GAS AND MARKET ANALYSIS
Author: Juan Sebastian Serra Leal
Advisor: Jimena Incer Valverde
TU Berlin (Germany)……. 553

INCREASING THE ENVIRONMENTAL SAFETY OF THERMAL POWER PLANTS BY COAL FLY ASH UTILIZATION
Author: Marta Zegarek
Advisors: Hanna Koshlak
Kielce University of Technology (Poland)…… 571