КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2(18), 2022
ISSN 2663 - 4023
DOI: 10.28925/2663-4023.2022.18.8698
УДК 004.056

Voitovych Olesia
PhD in engineering, assoc. professor
Vinnytsia National Technical University, Vinnytsia, Ukraine
ORCID ID: 0000-0001-8964-7000
voytovych.olesya@vntu.edu.ua

Kupershtein Leonid
PhD in engineering, assoc. professor
Vinnytsia National Technical University, Vinnytsia, Ukraine
ORCID ID: 0000-0001-6737-7134
kupershtein.lm@gmail.com

Holovenko Vitalii
Master in cybersecurity
Vinnytsia National Technical University, Vinnytsia, Ukraine
torvald124@gmail.com

DETECTION OF FAKE ACCOUNTS IN SOCIAL MEDIA

Abstract. Social media is becoming increasingly used as a source of information, including events during warfare. The fake accounts of the social media are often used for a variety of cyber-attacks, information-psychological operations, and social opinion manipulating during warfare. The analysis of online social media research methods are carried out, the main metrics and attributes of fake accounts in Facebook are investigated. Each metric is assigned to the appropriate categories for the convenience of their analysis and gets a certain number of points depending on conditions from 0 to 3, which indicate how much every of the metrics influenced on conclusion about the fakeness of the account. The levels of influence have the following meanings: 0 – no influence, 1 – weak influence, 2 – significant influence, 3 – critical influence. For example, if the histogram feature reaches level 3, this means that the parameter characterizing this feature has a critical impact on account fakeness. Otherwise, if the column is at 0 or 1 level, this means that the parameter is inherent in the real account. Thus, based on the level of each of the parameters, we conclude on the fakeness or reality of a certain account. The following metrics are analyzed: likes, friends, posts and statuses, personal information about the user and the photos, considering their possible parameters and influence on the status of the account. Each metric is assigned to the appropriate categories for the convenience of their analysis. A decision-making system based on a supported vector machine is developed and has 9 inputs and single output. A series of experimental research was conducted where account analyzing as well as parameters extracting and selection are realized on Facebook. The classifier accuracy of the fake accounts detection is 97% with the special prepared dataset of the real and fake account parameters.

Keywords: social media, information warfare, social media metrics, neural networks, support vector machine

INTRODUCTION

Social media has become widespread in recent times, primarily as a tool for communication, exchange of ideas, and information obtaining.

Currently, with the continuous improvement of information and communication technologies, any conflict is reflected on the Internet. Very often, such a reflection affects the outcome of the confrontation of the competing parties. Active involvement by a multimillion audience allows one to manipulate public opinion and significantly influence the processes of

the opposing sides [1]. Moreover, social media becomes a field for different attacks such as social engineering.

Famous among social medias are Facebook, Twitter, LinkedIn, Pinterest, Google+, Tumblr, Instagram, Telegram, Flickr, MySpace, etc. [2]. The largest social media is Facebook, with more than 2 billion users. Such number of users allows conducting research on the social opinion of people on certain events, tracking user preferences and even conducting information wars [3].

Understanding the importance of the Internet and social media makes advanced nations invest heavily in social media that has become not only a means of communication but also an effective political weapon.

Social medias are a specific arena for conducting special information operations, in particular information-psychological operations directed to society [4]. Billions of people all over the world are already actively using social media for communication, news coverage, etc. However, a large number of agents use social media as a tool for manipulating individual and social consciousness. To do this, they use fake accounts that contain copied or false information about the user. Regardless of the specific goals of those who create fake accounts, their use tends to change public opinion in one form or another. The lack of censorship and all kinds of obstacles creates a favorable basis for successful actions in the virtual space. All this indicates that social media is turning into an arena of information confrontation.

There are a lot of researching works about fake account detection in recent years. Different parameters are suggested in [5-9] to fake account detection (fig. 1).

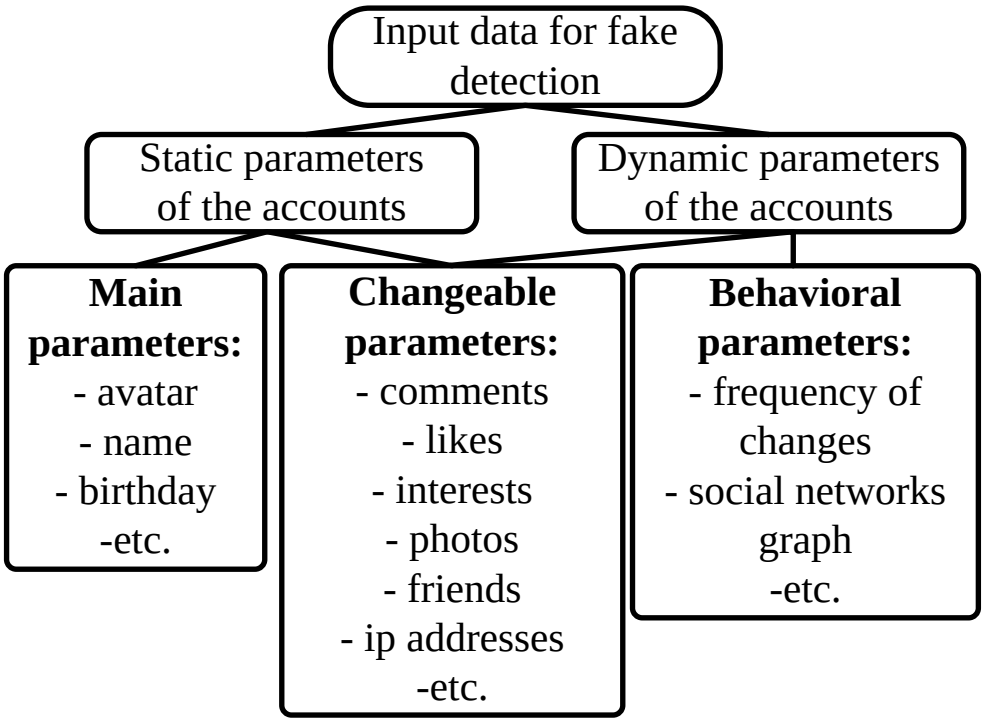

Fig. 1 The input parameters for fake detection

The static parameters are usually used for ad hoc analyzing e.g., profile picture (avatar), name, date of birth, number of friends, photos, likes, etc. Some of them are changeable e.g.

ISSN 2663 - 4023

number of friends and can be used for dynamic analyzing which their changes during time intervals. Some approaches include behavior parameters used for graph building of social media links or online analyzing of changes in the accounts.

According to the input parameters, the different methods for fake account detection are proposed based on [5-9]:

- Account parameters summary (rating);
- Account analysis for a time interval;
- Machine learning algorithms;
- Graph-based techniques;
- Dig data approaches.

The problem of the fake account detection stays of current interest, and the **goals** of this research are analyzing parameters of real and fake accounts on Facebook and identifying the key machine learning based classifier with high accuracy rate fake account detection.

METHODS AND MATERIALS

Social media is a social structure consisting of a plurality of agents (subjects - individuals, communities, groups of individuals or organizations) and a set of relations defined on it (a set of relationships between agents such as dating, friendship, communication, etc.) [10]. The social media is a graph G (N, E), where N = {1, 2, ... , n} is the finite set of vertices (agents) and E is the set of edges that reflects the interaction of agents.

Today, the number of users of the most popular social media in the world, Facebook, reaches several billion people, and the amount of information it stores is about 600 petabytes. Every day, Facebook users make more than 5 billion publications, which is a great base for researching the social status of any country's population. Therefore, one can conclude that social media is a great base for large numbers of fake accounts and their informational affects other users during warfare [11].

An account typically contains the information needed to identify the user when logged in, information for authorization and accounting. This is the user ID and password. A password or its counterpart, as a rule, is stored in encrypted or paged form for user security. However, no secret that Facebook stores on its servers a huge amount of account information that is not visible to the average user. Such information includes:

- User's geolocation data;
- Data about comments and user posts;
- Data about user marks in a photo by this or another user;
- Network signal strength;
- Operating system;
- Browser;
- Service provider / internet provider;
- Third party cookies (including searching and shopping);
- User-hidden posts;
- Account information removed from the account;
- «Like» marks;
- And much more information.

Thus, the general structure of an account in social media is represented as a schema (fig. 2), which displays both the visible content of the account that the user sees and the content not visible by the ordinary user that is stored on social media servers.

ISSN 2663 - 4023

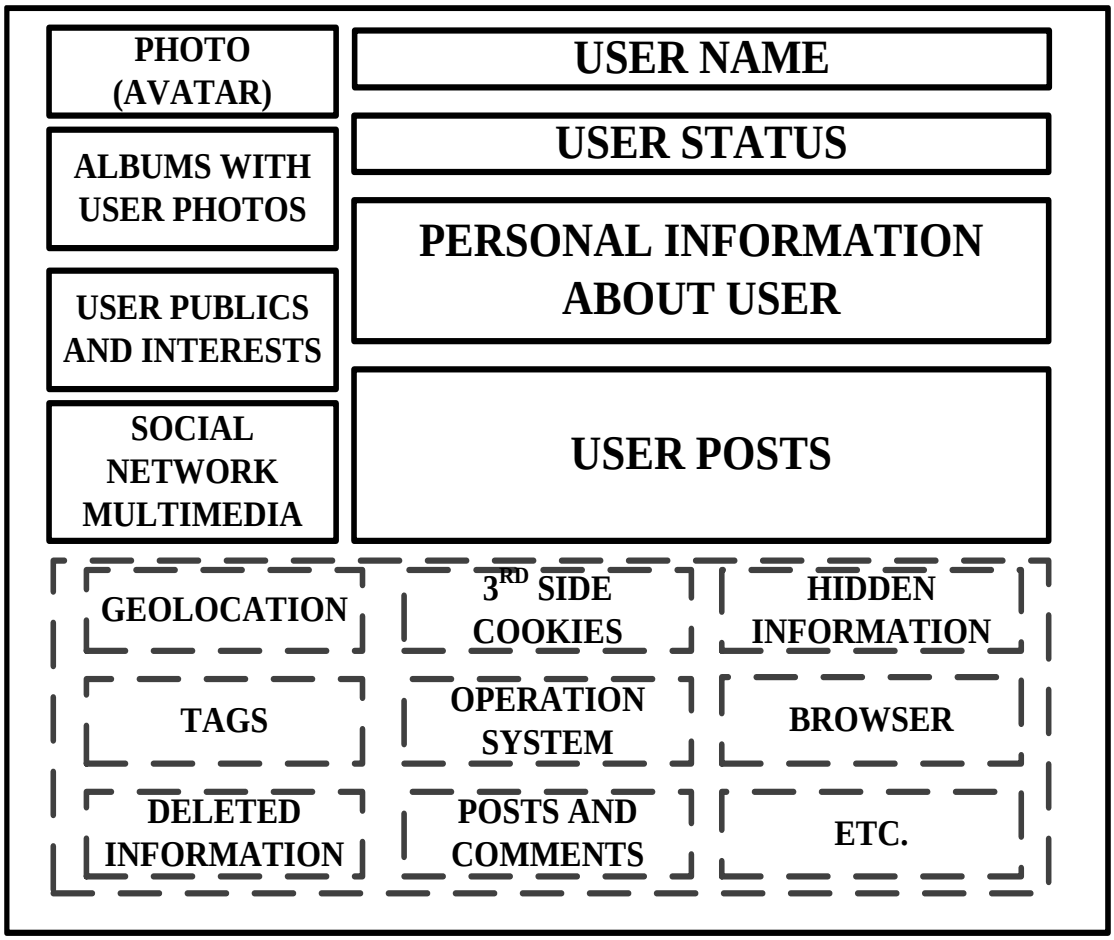

Fig. 2. The general structure of the account data in social media

Significantly, not all account information is visible, as modern social media have the ability to hide information from third-party users.

Mark Zuckerberg, founder of Facebook, said that about half of the accounts (and it is more than 1 billion accounts) are fake. Therefore, the detection of fake accounts in social media is currently an issue.

The formation of metrics for data analysis in social media, you can use information about likes, comments, reposts on publications, user identification data (gender, age, city of residence, place of work/training, address, etc.), information about the user's friends, their community, statistics of the user's stay in the social media, connections between users, etc. [12-14].

Like by signs is divided into number of likes and who left them on the user page. In turn, both friends and strangers receive likes. The number of likes is also important for defining the profile. If there is a number of likes on a certain post greater than the number of user's friends, which may indicate that the user received these likes in an unusual way. The absence of a nickname on the page indicates the «isolation» of the user, which may also indicate its fakeness.

Personal information on a user's page indicates a lot about the profile or authenticity of the profile. For further analysis, personal information is divided into user names, amount of data, contradictory information and private information.

Date of birth has signs that may indicate the validity of the page. Often, users of fake accounts do not pay attention when creating the account leave the default birthday (usually

January 1). It is also possible that the age of the user is questionable or does not coincide with other dates on the page. For example, the user is 15 years old, but other information on the page indicates that he graduated from the university 10 years ago.

User name is difficult to research because there are many people with the same name and last name. However, it is worth checking the name for its coincidence with the name of the famous people. You should pay attention to whether the username belongs to the default names of this user's country.

The lack of personal information in the profile and insignificant information about interests and user groups indicates that the user does not want to be identified by other users, and therefore this is a sign of fakeness.

The contradictory information on the page is one of the most reliable indicators of fakeness; however, it requires complex analysis. For example, information in the posts of the user does not match the information specified in the profile, or the user is in groups that do not meet his stated interests [8].

Personal information includes e-mail and mobile phone number. Users rarely disclose such information to public access, unlike fake accounts and specially created promotional profiles.

Status and posts on a user's page as a single entity since they differ only in profile placement are analyzed based on the following features: on the frequency of editing/adding and on the commenting. Status and posts are sometimes used as advertising.

The frequency of editing/adding posts and statuses indicates the activity of the user. If posts/statuses are added rarely or very often - this is one of the hallmarks of fakeness. If a user has long ago added a post/status and does not update it for a long time, it's likely that this account is a fake.

Number of comments also indicates the activity of the profile itself. Their absence or excessive number is most often the case. Both user's friends and strangers can post to Comments.

User's friends play a significant role in fake defining, since they indicate both the activity of the profile in the social media and the range of the user's interests. The fakeness depends on the number of user's friends and is difficult to analyze, because in order to draw a conclusion, it is necessary to analyze the friends themselves. E.g. if there is a fake in the user's list of friends, it is likely that the user himself is a fake. If the user does not have friends, there is a high probability that his profile is used not for communication but for other purposes. Gaining a large number of friends in a short period after creating a profile also causes suspicion, therefore, most likely, such a profile is a fake.

User photos analysis plays an important and, at the same time, the most difficult role in the study of the fakeness of the account. First, the lack of photos on both the avatar and the albums already shows that this account is a fake. Secondly, presented on the page photos need to be analyzed for coincidence with other images on the Internet or with photos of other profiles, since the user could download and use photos of celebrities, animals, or other objects. The number of photos is also an important indicator, since excessive or small amounts of photos indicate their fakeness or inactivity of the user, respectively.

Of course, these criteria alone cannot point to the «fakeness» of the account, since merely analyzing their association may call into question the authenticity of the account. For a more precise definition of account status, you need to use an analysis using as many criteria as possible.

ISSN 2663 - 4023

EXPERIMENTS RESULTS

The generalized structure of fake detection system is shown in the fig. 3.

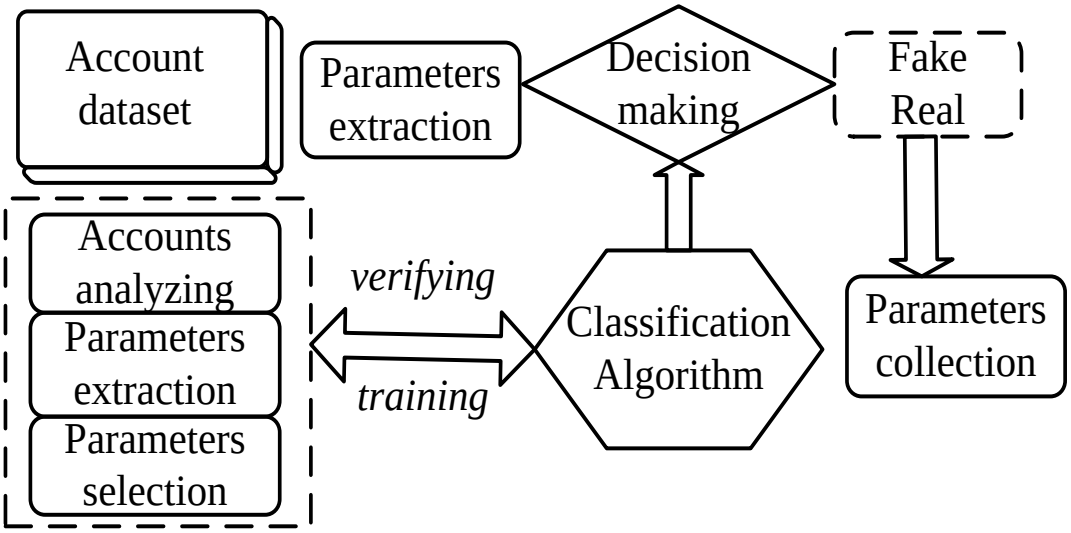

Fig. 3. The structure of the fake detection system

The parameters analyzing, extraction and selection module is used for training and verifying dataset collection for classification module. The decision-making system uses learned classifier for fake account detection and forming parameters collection for subsequent analyzing and learning.

There are a lot of methods for analyzing information in social media that solve the tasks of classification [8, 9, 15, 16]:

- Bayesian classifier (a method of closest neighbors, linear Fisher discriminant);
- Neural network (perceptron);
- Linear delimiter (logistic regression, linear Fisher discriminant);
- Induction (decision tree, test algorithm);
- Reduction of dimension (principal component method, independent component method);
- Choice of model (minimization of empirical risk, genetic algorithm, self-organization of models).

For further research and analysis of data from Facebook, a neural network based on supported vector machine (SVM) method is used [17-19]. The main task of the SVM is finding the most correct line or hyperplane, which divides the data into two classes. SVM is an algorithm that receives input data and returns the corresponding partitioning line classes.

The SVM algorithm is arranged in such a way that it is looking for plane points that are located closest to the separation line. These points are called reference vectors. Then, the algorithm calculates the distance between the reference vectors and the dividing plane. This distance is called the interval. The main purpose of the algorithm is to maximize the gap distance. A hyperplane is considered a hyperplane, for which this gap is maximal. Hyperplane is a (n-1) dimensional subspace in an n-dimensional Euclidean space, which divides the space into two separate parts.

For a two-dimensional data set, the dividing line is a hyperplane. Simply put, for n-dimensional space there exists (n-1) dimension hyperplane, dividing this space into two parts.

The neural network consists of an n number of neurons that retain certain values of coefficients and weights. In general, it is a mathematical computational model for inputting data

ISSN 2663 - 4023

into the input layer of neurons, processing them in hidden layers and obtaining the output layer. The key feature of the system is self-learning, not explicitly programmed.

Neurons, as the simplest computing units, perform simple calculations of the received information and transmit it further, thus each neuron has two basic parameters of an input signal and an output signal, thus transmitting the initial data. In the case of classifying problem, the number of neurons in the output layer depends on the number of classes to which the results of the calculation of the model need to be attributed. In this case, there are two classes: the account may be fake or true, and the output signal takes value of «0» or «1».

The input vector is provided to the input layer, each element of which, multiplied by certain weights of the neuron, is transmitted to the next layer in accordance with the relations established between the neurons.

In this case, the classifier has 9 inputs (x1, x2, x3, ..., x9) that are responsible for each of the checked account parameters and one output Y, which takes the value of «Real» or «Fake». On the next layer, before the sum S of input values and the constant, a certain activation function F() is applied that returns the normalized signal and passes it further over the network.

There is scheme of the SVM-classifier in fig. 4.

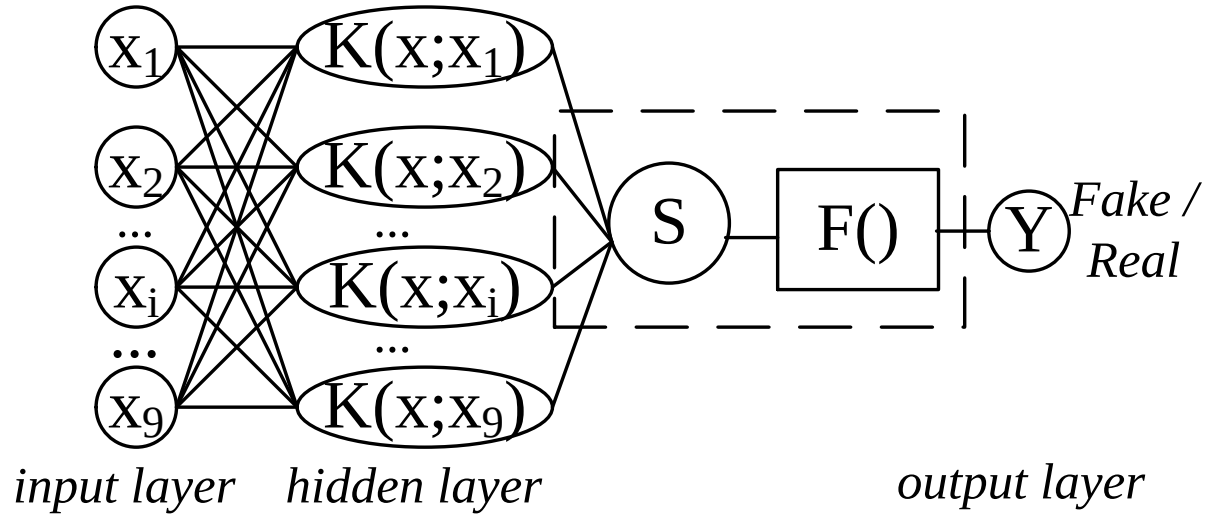

Fig. 4. The structure of the SVM classifier

The network learning to solve the problem of data classification is as follows: the classifier is learned on the «input - output» pairs, where the output is the correct class, which should belong to the object. Learning of the classifier ends at the time when neuronal weights are calibrated in such a way that the network gives the right answers when giving it any input value.

In the classifier, the input and output layers are selected. The neural network receives information, by the input receptors and then, passing this information through itself and converting it, generates output values. Nodes inside the neural network are called hidden, since they have no connections to the outside world, as nodes of the output and the input. They are called when the previous layers are activated only.

As indicator, the rating system is chosen. Each of metrics during the analysis gets certain number of points depending on conditions from 0 to 3 (table 1).

The resulting values for each parameter are formed in an array of data that is fed to the input of the classifier, which, in turn, analyzes them and issues the result. Depending on the

ISSN 2663 - 4023

situation, there is a necessity for additional research with the participation of experts and taking into account, the information contained in the histogram in order to accurately detects the status of the account.

For this purpose, the checking each of the columns and determining their influence level are obtained. In total there are four levels of influence (from 0 to 3), which indicate how much every of the metrics influenced on conclusion about the fakeness of the account. The levels of influence have the following meanings:

0 – No influence;
1 – Weak influence;
2 – Significant influence;
3 – Critical influence.

Table 1

Criteria of setting points due to metrics values

Parameter	0	1	2	3
Number of friends	30 < Number of friends < 500	500 < Number of friends < 2000	0 < Number of friends < 30 & Number of friends > 2000	Number of friends = 0
Photo on avatar	Photo exists	-	-	Photo doesn`t exist
Number of photos	100 < Number of photos < 500	Number of photos > 500	0 < Number of photos < 100	Number of photos = 0
Cover photo	Photo exists	-	Photo doesn`t exist	-
Number of posts	-	Posts exist	-	Posts don`t exist
Birthday	1932 < Birthday < 2009	2009 < Birthday	Birthday < 1932	Birthday isn`t shown
Personal information	5 fields filled	3-4 fields filled	1-2 fields filled	0 fields filled
Updates	Updates < 14 days	14 days < Updates < 1 month	1 month < Updates < 1 year	Updates > 1 year
User name	User name matches typical names of user country	-	User name doesn`t match typical names of user country	-

For example, if the histogram column reaches level 3, this means that the parameter characterizing this column has a critical impact on account fakeness. Otherwise, if the column is at 0 or 1 level, this means that the parameter is inherent in the real account. Thus, based on the level of each of the parameters, we conclude on the fakeness or reality of a certain account.

To train the classifier fit(X, y) method (X – table-like input 2D dataset, y – vector-like targets) from the “sklearn” library is used. To do this, a set of data is prepared in advance, consisting of training and a validation set distributed in the ratio of 60:40 (fig. 5).

ISSN 2663 - 4023

	A	B	C	D	E	F	G	H	I	J
1	STATUS	P1	P2	P3	P4	P5	P6	P7	P8	P9
2	Real	1	3	3	3	0	2	0	3	0
3	Fake	3	3	1	0	2	2	2	3	0
4	Fake	3	3	3	3	0	2	3	3	0
5	Real	0	0	0	0	2	2	0	2	0
6	Real	2	0	2	0	2	2	0	0	0
7	Real	2	0	0	0	2	2	3	0	0
8	Fake	3	3	0	3	3	0	3	3	1
9	Real	2	0	3	3	0	2	1	3	0
10	Real	0	0	3	0	1	2	2	2	0

Fig. 5. The structure of the Dataset.csv file

The dataset consists of numeric information about real accounts in Facebook (columns from P1 to P9), as well as the statuses corresponding to these accounts (STATUS column). The dataset contains information about 100 existing accounts.

After model training, the parameter of accuracy is displayed, indicating the accuracy of the training and the reliability of the subsequent results.

The predict(X) method is responsible for processing information coming from Facebook using the weighted coefficients of the already trained model.

The system for detecting fake accounts in the social media «Facebook» is realized with Python programming language [20, 21] that has a convenient and clear graphical user interface and shows the parameter influence histogram of single account and its status (fig. 6).

The graphical user interface consists of such elements:

- Text field «User id» for entering user id in social media;
- «Status» label where a status of the checked account is shown;
- Histogram where social media`s metrics and their influence on the account status are shown.

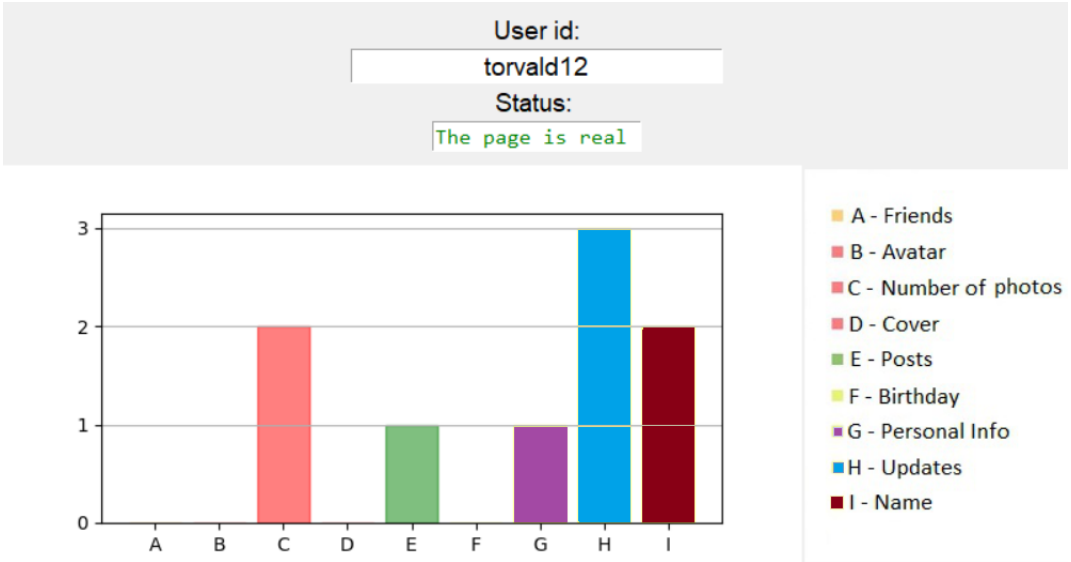

Fig. 6. The example of account analyzing

The software analyzes the following parameters: number of friends, number of friends, existing a photo on the avatar, a user`s photos, existing a cover photo, existing of posts, date of birth, personal information about the user, page update and user name. Thus, an analysis of

ISSN 2663 - 4023

these parameters allows concluding on statuses of accounts.

The effectiveness of the developed software tool is evaluated by the accuracy of fake accounts detection by the SVM. The software collected data from Facebook and then collection is prepared for experiment. The results of analyzing 10 of 100 total accounts are shown in the table 2.

Table 2

The result of users accounts analysis

User	Account status	Predicted status	User	Account status	Predicted status
Vitalii Holovenko	Real	Real	Den Ivanov	Fake	Fake
Oleksandr Topchii	Fake	Fake	Jenny Rahl	Real	Real
IvanVorobyov	Real	Real	Sergey Hubchakevych	Real	Real
Alex Rudyk	Fake	Fake	Dimon Anipchenko	Fake	Fake
Andrii Beatle	Real	Real	Jessica Dowling	Real	Real

After the analysis the accuracy checking is realized

$$\frac{n-t}{n}\cdot 100\% = \frac{100-3}{100}\cdot 100\% = 97\% \quad (1)$$

Where, t - the number of discrepancies between the account status and the result of the program; n - the number of the accounts checked.

Checking the accuracy of the fake accounts detecting system in Facebook showed that 3 of 100 accounts` statuses were detected wrong and 97 of 100 were detected correct.

CONCLUSIONS AND FUTURE WORKS

The structure of accounts in social media is analyzed and information about the user contained in them is highlighted. The main metrics of Facebook are considered and analyzed. Based on this metrics it is possible to define a fake account. The following metrics are analyzed: likes, friends, posts and statuses, personal information about the user and the photos, considering their possible parameters and influence on the status of the account. Each metric is assigned to the appropriate categories for the convenience of their analysis. The decision-making system based on a SVM is developed and has nine inputs and the single output. Accuracy is 97 % on the special prepared dataset.

Future works will be focused on more real and larger dataset analysis, which could change the accuracy, and identifying parameters (friend, comments, changing etc.) that have long-range impact on the fake accounts detection.

REFERENCES

1 *Information Warfare: The Role of Social Media in Conflict*. UNT Digital Library. https://digital.library.unt.edu/ark:/67531/metadc503647

2 *The 15 Biggest Social Media Sites and Apps [2022]*. Dreamgrow. https://www.dreamgrow.com/top-15-most-popular-social-networking-sites.

3 Dudatiev, A. V. (2017). *Complex information security of STS: models of influence and protection : monography*. VNTU.

4 Voitovych, O. P., Holovenko, V. O. (2016). Research of social networks as a source of information in warfare. In J. Rysiński (ed.), *Inżynier XXI wieku projectujemy przyszlosc* (p. 111–119).

5 Romanov, A., Semenov, A., Mazhelis, O., Veijalainen, J. (2017). Detection of Fake Profiles in Social Media - Literature Review. In *13th International Conference on Web Information Systems and Technologies*. SCITEPRESS - Science and Technology Publications. https://doi.org/10.5220/0006362103630369.

6 Voitovych, O. P., Dudatiev, A. V., Holovenko, V. O. (2018). The model and software for fake accounts detection in social networks. *Scientific notes of Taurida National V. I. Vernadsky University Series: Technical science*, *29*(68), 112–119.

7 Ramalingam, D., Chinnaiah, V. (2018). Fake profile detection techniques in large-scale online social networks: A comprehensive review. *Computers & Electrical Engineering*, *65*, 165–177. https://doi.org/10.1016/j.compeleceng.2017.05.020.

8 Mohammadrezaei, M., Shiri, M. E., Rahmani, A. M. (2018). Identifying Fake Accounts on Social Networks Based on Graph Analysis and Classification Algorithms. *Security and Communication Networks*, *2018*, 1–8. https://doi.org/10.1155/2018/5923156

9 Gupta, A., Kaushal, R. (2017). Towards detecting fake user accounts in facebook. У *2017 ISEA Asia Security and Privacy (ISEASP)*. IEEE. https://doi.org/10.1109/iseasp.2017.7976996

10 Can, U., Alatas, B. (2019). A new direction in social network analysis: Online social network analysis problems and applications. *Physica A: Statistical Mechanics and its Applications*, *535*, 122372. https://doi.org/10.1016/j.physa.2019.122372

11 Dudatiev, A. V., Voitovych, O. P. (2017). Information security of sociotechnic systems: Informational influence model. *Informational technologies and computer engineering*, (38), 16–21.

12 Voitovych, O. P., Dudatiev, A. V., Holovenko, V. O. (2018). Fake accounts detection in social network "Facebook". In *thesis of international scientific-practical conference "Informational technologies and computer modeling"* (pp. 190–193). http://itcm.comp-sc.if.ua/2018/zbirnyk.pdf

13 Toolkit of information wars: traditional and new tools. (2019). *Bulletin of the Book Chamber*, (1), 7–10. http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/vkp_2019_1_3.pdf.

14 *10 Metrics to Track for Social Media Success : Social Media Examiner*. (б. д.). Social Media Examiner. https://www.socialmediaexaminer.com/10-metrics-to-track-for-social-media-success.

15 Ulichev, O. S. (2018). Research of the models of information dissemination and information influences in social networks. *Control, navigation and communication systems. Collection of scientific papers*, *4*(50), 147–151. https://doi.org/10.26906/sunz.2018.4.147

16 Xiao, C., Freeman, D. M., Hwa, T. (2015). Detecting Clusters of Fake Accounts in Online Social Networks. У *CCS'15: The 22nd ACM Conference on Computer and Communications Security*. ACM. https://doi.org/10.1145/2808769.2808779

17 Bazzaz Abkenar, S., Haghi Kashani, M., Mahdipour, E., Jameii, S. M. (2020). Big data analytics meets social media: A systematic review of techniques, open issues, and future directions. *Telematics and Informatics*, 101517. https://doi.org/10.1016/j.tele.2020.101517

18 Kosinski, M., Matz, S. C., Gosling, S. D., Popov, V., Stillwell, D. (2015). Facebook as a research tool for the social sciences: Opportunities, challenges, ethical considerations, and practical guidelines. *American Psychologist*, *70*(6), 543–556. https://doi.org/10.1037/a0039210

19 *SVM-Light: Support Vector Machine*. Home | Department of Computer Science. https://www.cs.cornell.edu/people/tj/svm_light.

20 *Python 3.10.7 Documentation.* https://docs.python.org/3/.

21 *Selenium with Python — Selenium Python Bindings 2 documentation*. https://selenium-python.readthedocs.io.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (18), 2022
ISSN 2663 - 4023

Войтович Олеся Петрівна
Кандидат технічних наук, доцент, доцент кафедри захисту інформації
Вінницький національний технічний університет, факультет інформаційних технологій та комп'ютерної інженерії, Вінниця, Україна
ORCID ID: 0000-0001-8964-7000
voytovych.olesya@vntu.edu.ua

Куперштейн Леонід Михайлович
Кандидат технічних наук, доцент, доцент кафедри захисту інформації
Вінницький національний технічний університет, факультет інформаційних технологій та комп'ютерної інженерії, Вінниця, Україна
ORCID ID: 0000-0001-6737-7134
kupershtein.lm@gmail.com

Головенько Віталій Олександрович
Магістр з кібербезпеки
Вінницький національний технічний університет, факультет інформаційних технологій та комп'ютерної інженерії, Вінниця, Україна
torvald124@gmail.com

ВИЯВЛЕННЯ ФЕЙКОВИХ ОБЛІКОВИХ ЗАПИСІВ В СОЦІАЛЬНИХ МЕРЕЖАХ

Анотація. Соціальні мережі все частіше використовуються як джерело інформації, в тому числі про події під час війни. Фейкові акаунти в соціальних мережах часто використовуються для різноманітних кібератак, інформаційно-психологічних операцій та маніпулювання суспільною думкою під час війни. Проведено аналіз методів дослідження соціальних мереж, досліджено основні показники та ознаки фейкових акаунтів у мережі Facebook. Кожний показник ідентифікується певною кількість балів залежно від умов від 0 до 3, які вказують на те, наскільки кожен із них впливає на висновок про фейковість облікового запису. Рівні впливу мають такі значення: 0 – не впливає, 1 – слабкий вплив, 2 – значний вплив, 3 – критичний вплив. Наприклад, якщо у рівень впливу у деякого параметра визначений як 3 - це означає, що даний параметр суттєво вказує на фейковість облікового запису. В іншому випадку, якщо показник знаходиться на рівні 0 або 1 - це означає, що таке значення параметру більш властиве реальному обліковому запису. Таким чином, за рівнем кожного з параметрів ми робимо висновок про фейковість або реальність певного акаунта. Аналізуються такі параметри облікового запису: лайки, друзі, пости та статуси, особиста інформація про користувача та фотографії з урахуванням їх можливих параметрів та впливу на статус облікового запису. Кожна метрика віднесена до відповідних категорій для зручності їх аналізу. Розроблено систему підтримки прийняття рішень щодо фейковості облікового запису соціальної мережі Facebook на основі метода опорних векторів у якості класифікатора, який на вхід отримує 9 параметрів, що характеризують обліковий запис і на виході дає передбачення чи акаунт реального користувача чи ні. Було проведено серію експериментальних досліджень, у яких реалізовано аналіз акаунтів. Точність класифікатора виявлення фейкових акаунтів після навчання на тестових даних становить 97%.

Ключові слова: соціальна мережа , інформаційна війна, метрики соціальних мереж, нейронні мережі, метод опорних векторів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 *Information Warfare: The Role of Social Media in Conflict*. UNT Digital Library. https://digital.library.unt.edu/ark:/67531/metadc503647.
2 *The 15 Biggest Social Media Sites and Apps [2022]*. Dreamgrow. https://www.dreamgrow.com/top-15-most-popular-social-networking-sites.

3 Дудатьєв, А. В. (2017). *Комплексна інформаційна безпека соціотехнічних систем: моделі впливу та захисту*. ВНТУ. https://press.vntu.edu.ua/index.php/vntu/catalog/book/352.

4 Voitovych, O. P., Holovenko, V. O. (2016). Research of social networks as a source of information in warfare. In J. Rysiński (ed.), *Inżynier XXI wieku projectujemy przyszlosc* (p. 111–119).

5 Romanov, A., Semenov, A., Mazhelis, O., Veijalainen, J. (2017). Detection of Fake Profiles in Social Media - Literature Review. In *13th International Conference on Web Information Systems and Technologies*. SCITEPRESS - Science and Technology Publications. https://doi.org/10.5220/0006362103630369.

6 Войтович, О. П., Дудатьєв, А. В., Головенько, В. О. (2018). Модель та засіб для виявлення фейкових облікових записів у соціальних мережах. *Вчені записки таврійського національного університету ім. В.І. Вернадського. Серія: Технічні науки*, *29*(68), 112–119.

7 Ramalingam, D., Chinnaiah, V. (2018). Fake profile detection techniques in large-scale online social networks: A comprehensive review. *Computers & Electrical Engineering*, *65*, 165–177. https://doi.org/10.1016/j.compeleceng.2017.05.020.

8 Mohammadrezaei, M., Shiri, M. E., Rahmani, A. M. (2018). Identifying Fake Accounts on Social Networks Based on Graph Analysis and Classification Algorithms. *Security and Communication Networks*, *2018*, 1–8. https://doi.org/10.1155/2018/5923156.

9 Gupta, A., Kaushal, R. (2017). Towards detecting fake user accounts in facebook. У *2017 ISEA Asia Security and Privacy (ISEASP)*. IEEE. https://doi.org/10.1109/iseasp.2017.7976996

10 Can, U., Alatas, B. (2019). A new direction in social network analysis: Online social network analysis problems and applications. *Physica A: Statistical Mechanics and its Applications*, *535*, 122372. https://doi.org/10.1016/j.physa.2019.122372.

11 Дудатьєв, А. В., Войтович, О. П. (2017). Інформаційна безпека соціотехнічних систем: Модель інформаційного впливу. *Інформаційні технології та комп`ютерна інженерія*, *1*, 16–21. https://itce.vntu.edu.ua/index.php/itce/article/view/657/401.

12 Войтович, О. П., Дудатьєв, А. В., Головенько, В. О. (2018а). Виявлення фейкових облікових записів у соціальній мережі «Facebook». У *"Інформаційні технології та комп'ютерне моделювання"* (с. 190–193). п. Гоніней О.М. http://itcm.comp-sc.if.ua/2018/zbirnyk.pdf.

13 Toolkit of information wars: traditional and new tools. (2019). *Bulletin of the Book Chamber*, (1), 7–10. http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/vkp_2019_1_3.pdf.

14 *10 Metrics to Track for Social Media Success : Social Media Examiner*. Social Media Examiner. https://www.socialmediaexaminer.com/10-metrics-to-track-for-social-media-success.

15 Ulichev, O. S. (2018). Research of the models of information dissemination and information influences in social networks. *Control, navigation and communication systems. Collection of scientific papers*, *4*(50), 147–151. https://doi.org/10.26906/sunz.2018.4.147

16 Xiao, C., Freeman, D. M., Hwa, T. (2015). Detecting Clusters of Fake Accounts in Online Social Networks. У *CCS'15: The 22nd ACM Conference on Computer and Communications Security*. ACM. https://doi.org/10.1145/2808769.2808779

17 Bazzaz Abkenar, S., Haghi Kashani, M., Mahdipour, E., Jameii, S. M. (2020). Big data analytics meets social media: A systematic review of techniques, open issues, and future directions. *Telematics and Informatics*, 101517. https://doi.org/10.1016/j.tele.2020.101517

18 Kosinski, M., Matz, S. C., Gosling, S. D., Popov, V., Stillwell, D. (2015). Facebook as a research tool for the social sciences: Opportunities, challenges, ethical considerations, and practical guidelines. *American Psychologist*, *70*(6), 543–556. https://doi.org/10.1037/a0039210

19 *SVM-Light: Support Vector Machine*. Home | Department of Computer Science. https://www.cs.cornell.edu/people/tj/svm_light.

20 *Python 3.10.7 Documentation*. https://docs.python.org/3/.

21 *Selenium with Python — Selenium Python Bindings 2 documentation*. https://selenium-python.readthedocs.io.