Journal of Theoretical and Applied Information Technology
15th November 2022. Vol.100. No 21

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EVALUATION OF THE CONTEMPORARY STATE OF SOCIAL NETWORK SECURITY ISSUES: PUBLICATION CONTENT ANALYSIS

YE.MAKATOV [1], **Al.AKTAYEVA** [2], **R.NIYAZOVA** [3], **A.KONYRKHANOVA** [4], **A.BEISSEKOV** [5], **M.AITKENOVA** [6], **D.PLESKACHEV** [7], **M.ZHAMANKARIN** [8]

[1, 4] Department of Information Security , L.Gumilyov Eurasian National University, Kazakhstan
[2,5] Department of Information and Communication Technologies, Sh.Ualikhanov Kokshetau University, Kazakhstan
[3] Department of Artificial Intelligence Technologies, L.Gumilyov Eurasian National University, Kazakhstan
[6, 7, 8] Department of Information Systems and Informatics, A.Myrzakhmetov Kokshetau University, Kazakhstan

E-mail: [1]m.yerkhan@list.ru, [2]aakhtaewa@gmail.com, [3]rozamgul@list.ru, [4]ErkeshanK@mail.ru
[5]b.akilbek@mail.ru, [6]mahabat_89_is@mail.ru, [7]denispleskachev@mail.ru, [8]zhamankarin@yandex.kz

ABSTRACT

Among various social media platforms, the concept of all users' openness and accessibility of information is becoming even more lifelike. Social networks afford to receive the freshest news, communicate with various interesting people, regardless of their location and residence, contribute to changing the interaction between people, and so on. This article presents the standard principle of content analysis of the publications indexed in the Scopus and WoS databases and provides the analysis of 67 high-rating publications. The result of the analysis allows for the conclusion that most social network researchers use readily available methods for classifying the threats to information security violations, which cannot be considered specifically suitable for the analysis of social networks since they do not reflect the characteristic features of research in this area. This paper proposes a different approach to the clustering of implemented threats to the information security of social networks. An analysis of the currently existing threats and vulnerabilities in the information security of social networks indicates that the achievement of the goals and objectives of information protection, as well as ensuring the maximum level of security, requires the integrated use of available methods and means of protection.
Keywords: *Social networks, Ontology, Security privacy, Security methods, Content analysis.*

1. INTRODUCTION

At present, the globalization of information technologies has an increasing impact on most areas of modern society. At the same time, there is an active growth and variety of computer attacks and abuses planned and carried out by means of new technologies.

The study and analysis of the phenomenon of social networks in the modern world has a rich history. Social networking platforms developed gradually, and prototypes of modern solutions appeared in the 20th century. The term "social network" was first coined in 1954 by the sociologist James Barnes in his "*Classes and Gatherings in a Norwegian Island Parish*" [1].

The term "social network" has been widely used since the early 2000s with the development of global information and telecommunication spaces and technologies,
facilitating the creation of the first social networking platforms. From that moment on, the phenomenon of "social network" partially lost its historical roots as belonging exclusively to the field of sociology and acquired a commonly used status, shifting to the focus of the natural sciences and the humanities.

In a modern sense, a social network is a service (*Internet platform*) that allows users to publish personal or other data about themselves on their pages (personal account) and serves to simplify

Journal of Theoretical and Applied Information Technology
15th November 2022. Vol.100. No 21

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

communication and information exchange between network users (see Figure 1). For example, in 1995, R. Konrads developed the first prototype of a social network, named Classmates.com.

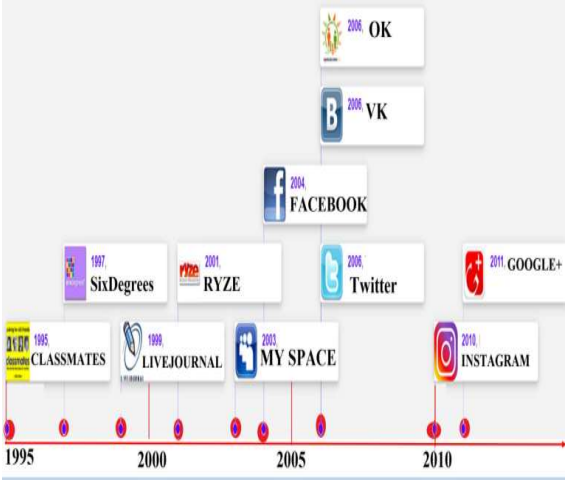

Figure 1: History of the development of social networks [2]

Initially, the Classmates.com website implied no personal user profile (personal account) and only opened up access to the lists of students studying at a particular university (see Figure 2).

The Classmates.com social network requires authorization and provides everyone with the opportunity to find their classmates, coursemates, and other options. The social network Classmates.com still exists and is popular among millions of users from North America and Europe [1,3].

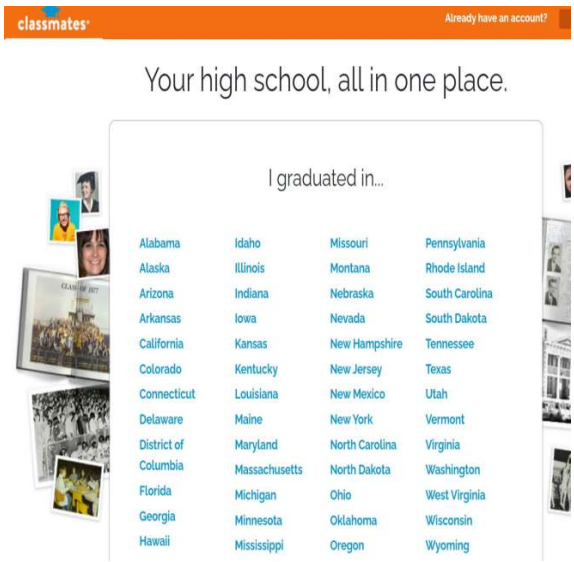

Figure 2: Homepage of the Classmates.com Social Networking Website [4]

Fig. 3 depicts that the exact number of existing social networks today is unknown, since every day, something new is being developed and another ceases to exist.

According to reports from IT companies, in January 2022, social networking services were used by 4.62 billion people, which is 58.4% of the total population of the world [6].

The architecture of modern social networking platforms is based on the principles of *nonlinearity, interdependence, interchangeability,* and *multicentricity*. The system of hyperlinks destroys the dichotomy of "*semiperiphery*" and points to such a specific resource feature when every network element correlates with all through numerous reciprocal links. Such conventionality constitutes a threat of violation of the information security of the social network as an object of the critical cyberspace infrastructure.

An assessment of the current state of social networks shows that software and hardware progress is substantially more rapid than the process of creating technologies and information security tools.

The high priority and most relevant the tasks are identifying, analysing and classifying existing mechanisms for implementing information security threats that could lead to unauthorized data access or disruption of the normal functioning of the system; assessment of possible damage; determination of the main measures to counteract threats and vulnerabilities; development of security criteria and protection mechanisms; and an appropriate legal and regulatory framework in the field of social networks.

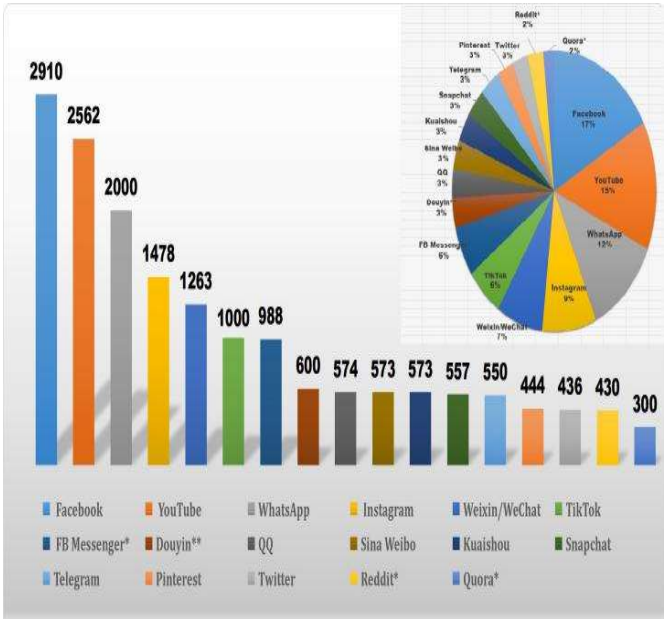

Figure 3: Popular social networks: monthly active users, in millions, Jan. 2022 [5]

Analysis and research of scientific works and publications in the field of ensuring the security of confidential information in social networks over the past decade have shown that with a general increased attention to the virtualization of society, specific sociological problems, such as the structure, features and main methods of stratification of social networks, are understudied.

Information about these processes and phenomena requires clarification and systematization based on current scientific methodological approaches.

2. SOCIAL NETWORKS SECURITY ANALYSIS

A social network is a virtual environment in which a person establishes, expands and deepens social ties, forming a specific structure of relations, and socializes, self-realizes, generates and consumes any information of interest through various communication channels in certain forms. Social networks are basically characterized by the following:

1. Virtuality.
2. Media exposure.
3. Interactivity [7].

Social networks are favourable for the formation of a new culture, i.e., the culture of virtual reality. An shows how the social characteristics of virtual reality affect the socialization of the individual.

A social network is a collection of people or groups of people who have certain connections and interactions between them. This structure gives rise to many social problems of virtual communities in social networks, including in the field of information security, which involve the trends in their development, influence on social processes and external internet phenomena as well as some features of the interactions of actors (malicious users) within communities [7,8].

The urgency of the problems and assessment of the degree of user data security in social networks (*security/vulnerability of users and confidential documents*) is emphasized by incidents that become known from numerous media reports.

For example, on January 27, 2020, computer security company Hudson Rock published a report stating that the phone numbers of 533 million Facebook users are being sold online. On April 20, 2020, Cyble analysts announced the purchase of 267 million Facebook accounts on the dark web, which were purchased from hackers for 0.0002 cents to $540. The dark web database server *contains all* of the sensitive information about users (*name, phone number, unique Facebook identification number and timestamp*) [9].

Since social networks are web services, security standards are defined based on the security measurements of web services and client and server applications that interact over the global Internet.

Table 1 demonstrates that the main objectives of social media data security are the same as those of cyberspace security and are based on the key properties of information security, namely, *privacy, integrity and availability.*

Table 1: Key Goals of Social Media Data Security [10]

No.	Key security properties	Definition of security properties
I.	Privacy	Ensuring that unauthorized users and/or nonauthorized persons cannot gain access to personal data or confidential information of users. Various encryption and access control methods are used to ensure privacy. Currently, Secure Socket Layers/Transport Layer Security protocols are used to ensure privacy.
II.	Integrity	Ensuring the accuracy and originality of data, the process of preventing intentional or unintentional changes to data by third parties. To check the integrity, it is necessary to use hashing, methods and models of cryptography and to message authentication.
III.	Availability	Ensuring that confidential information is available only to those users who have been authorized, identified, or specified as trusted persons.

Cybercrime has cost the global economy more than $1 trillion, which is just over 1% of the global GDP, according to the McAfee *Hidden Costs of Cybercrime* 2020 report, produced in collaboration with the Center for Strategic and International Studies.

Compared to the 2018 data, this figure has grown by more than 50%. In 2018, it was approximately 600 billion US dollars [11]. There is growing concern among IT professionals about the security of using social networking resources as the primary means of service communication.

The information security of social networks presumes three categories of confidential data protection:

1. Protection of user data (*software and technical protection and protection of users from social engineering attacks*).
2. Information protection.
3. Classification of potential threats in social networks.

The first and third categories of information protection cover the research in the field of protecting confidential data of social network users from threats and vulnerabilities.

Presently, the main part of the research is dedicated to the improvement of software and hardware, i.e., the *technical control of information security threats in social networks*.

According to research by Kaspersky Lab, the most common information security incidents are related to the actions of users in social networks [12].

The analysis of scientific works and the publications of researchers proves that given general increased attention to the topic of personality virtualization, such specific, restricted, and precise problems of information security, such as the structure, features and main ways of stratification of social network threats, remain underestimated.

Information about the processes and phenomena of the information security of social networks requires clarification and systematization based on current general scientific methodological approaches.

3. RESEARCH DESIGN

The methodology of the presented study employs the models "*confidential information - social network - user - malicious user*", the formalization of which makes it possible to study the considered systems using the methods of probability theory, synthesis, analysis, search and comparison of information.

The approaches used in this study include methods for searching, comparing and analysing information extracted from social networks that characterize the intensity of communication between users and providing for assessing the severity of certain features of their personality as the basis for further building a profile of user vulnerabilities and assessing their security.

This study involves the methodology of secondary analysis and the synthesis of publications in the indexed databases of Scopus, Elsevier, SciVal, WoS, and more. [13].

4. EMPIRICAL RESEARCH BASIS AND METHODS

The theoretical and methodological basis of this study is represented by several dimensions. Currently, the scientific and innovative activity of scientists is characterized by more than 20 parameters, including *publications in scientific journals, collections of articles and abstracts of reports, patents and certificates for an intellectual product, dissertations, and so on* (see Figure 4).

This article presents methods, models, algorithms and implementations of automatized retrieval and data collection - the results of content analysis of the publication activity of researchers. To establish the scientific problem and determine its limits, employing a critical analysis of the status of the issue considered and the related open sources, the object of study is to be selected and described. Examples are the following:

1. A typical social network: the basics of the terminological apparatus used in the article are introduced;
2. The features of the current state of ensuring the security of information resources of a social network in the context of the existence of threats to information security violations in cyberspace, for which the evolution of security tools is traced from 2010 to the present.

The results of such a classification enable us to perform a more accurate search in certain areas, specifying, in addition to the keywords, the field of science under consideration.

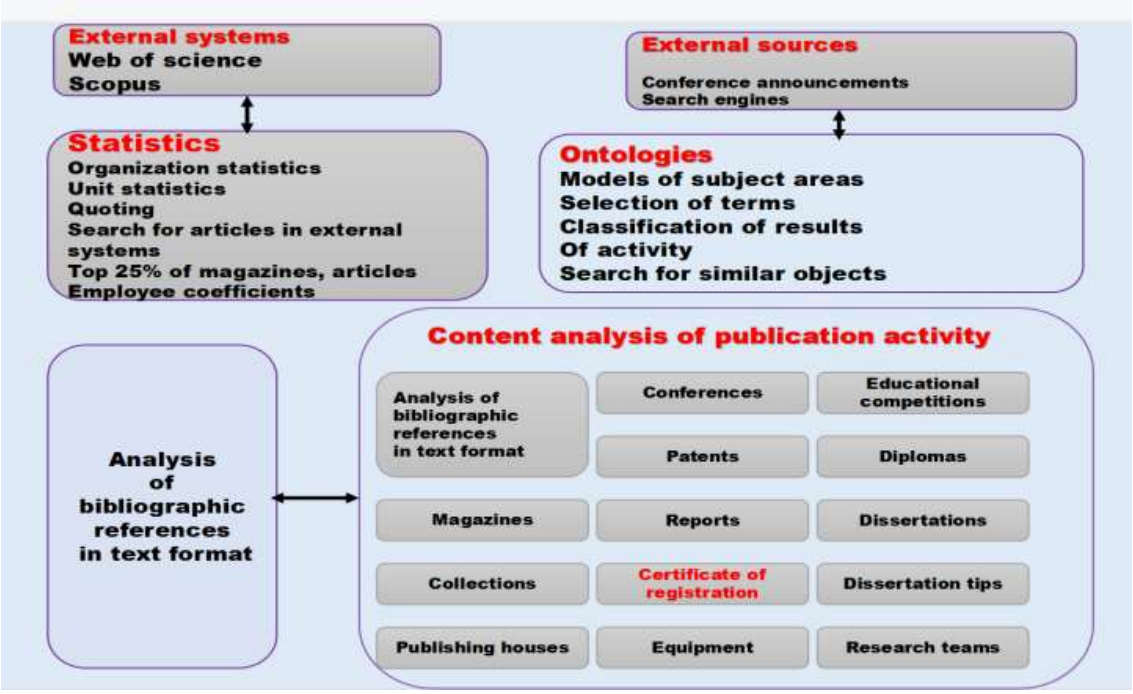

Figure 4: Technologies for the implementation of automatized retrieval and data collection [14]

According to the results of the critical appraisal of the state of affairs on the issue under study and the relevant sources, the conceptual statement of the research problem in general can be formulated as follows:

1. Publications devoted to threats to information security and methods of protecting social networks.
2. Classification of threats to information security and the means of protecting social networks.
3. Structure and classification of social networks.
4. Review of implementations of software and hardware for protecting social networking resources.

Currently, subject heading lists are used as a source of information about research topics in retrievals, and the topic of the publication is determined by the fixed topic of the journal in which the article is published.

The use of ontologies instead of subject heading lists might facilitate a more accurate determination of the thematic focus of the publication, since it is assumed that the ontology contains a larger number of concepts and relationships compared to the subject heading lists, and each individual publication, rather than the journal as a whole, is linked to the concept from the ontology.

The ontology classifier model is an interpretable method that offers straightforward and human-interpretable decision rules.

The Keyword Ontology Model was used to perform a more in-depth thematic data analysis on the issues of solving social network platform security problems in retrievals, as described and summarized in Fig. 5.

The constructed ontologies might be useful, among other things, for query refinement and expansion when performing full-text searches.

The essence of the approach is that the researcher sets research-specific keywords, after which they are automatically supplemented with terms from the ontology that correspond to his needs.

Algorithm of publication search according to a given model of subject fields. For the full implementation of automated search and data collection, the means, the results of content analysis of the publication activity of researchers in a given period, and the methods of computational linguistics were used.

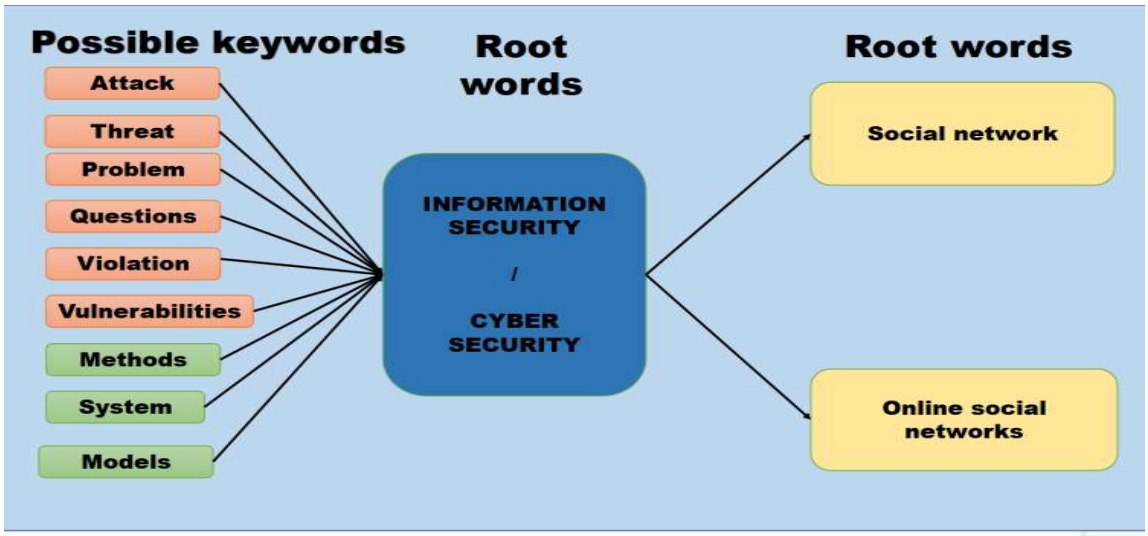

Figure 5: Keyword Ontology Model

For example, seven terms were used to implement automatized retrieval and data collection on threats, and three terms each were applied for protection and social networks.

Accordingly, a total of thirty requests for automatized retrieval were made, and the data collected corresponded to the results of a content analysis of the publication activity of researchers in a given period.

Inclusion and exclusion criteria. Automatized retrieval and data collection covering the results of a keyword content analysis of the publication activity of researchers in a given period produced 1860 original articles and conference proceedings. After exclusion, according to the proposed study criteria, 67 articles were excluded. Fig. 6 shows the flow chart of the proposed work.

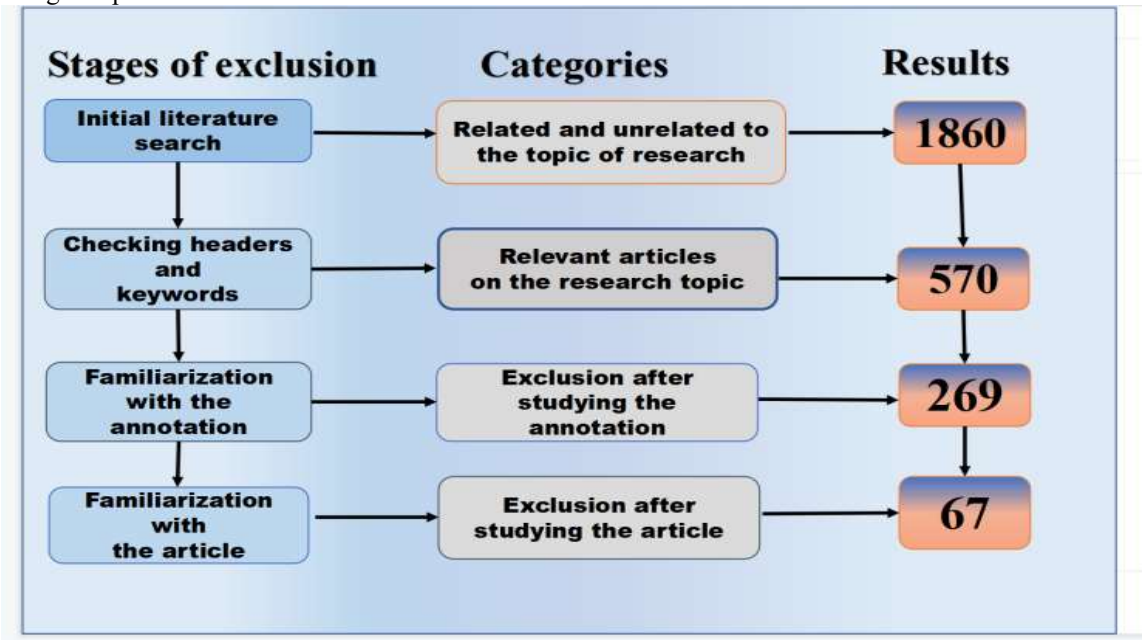

Figure 6: Stages of publication exclusion

Finally, the use of an ontology allowed the addition of features such as displaying a list of studies similar to a given study, a list of scientists working on similar topics, a list of similar journals, and other topic queries.

Evaluation of the quality of the publication for a given model of subject fields. To obtain references, the last stage involved the evaluation of 67 articles. At this stage, the researchers' publications were analysed for compliance with the subject-specific search of the procedure for assessing the reliability of the data presented therein.

To add such a publication to the list of references, the material should address the solution of information security problems, namely, the types of threats/attacks and the methods and models for protecting social network resources. The results *of assessing the quality of publications according to a given model of subject fields* were divided into three groups:

1. "Complete response received" - 2.
2. "Partial response received" - 1.
3. "Does not answer the question" - 0.

4. RESULTS OF THE RESEARCH: CLASSIFICATION OF THREATS TO INFORMATION SECURITY

The key elements of ensuring the information security of social network resources include the definition, analysis and classification of security threats and vulnerabilities. The analysis of risks and the formulation of requirements for systems for protecting social network resources are based on a *list of existing threats and vulnerabilities, an assessment of the likelihood of threats, and a malicious user model*. According to the results of the study, four groups of problems associated with threats of information security violations of social networking resources were identified:

1. Direct attacks - targeted attacks.
2. Privacy issues related to the leakage of personal information;
3. Vulnerabilities, means, weaknesses or loopholes in a system that open up the information security of the system to an attack.
4. Indirect attacks, means, listening to the network or sniffing. Here, two types are distinguished, namely, intersegment and intrasegment.

Generally, an overview of the problems associated with threats to the information security of social networking resources can be presented in the form of a summary, as in Table 2.

Based on the study, five main areas of threats/attacks and proposed recommendations for solving the problems of ensuring the information security of social networking resources are considered:

Spam is the distribution of many messages in instant messengers and social networks without the consent of the user. Spammers encourage users to click on malicious (viral) links or redirect to malicious websites with viral links or documents, lottery winning information, and fake bank statements. Basically, spamming is done for personal gain, for example, to access the recipient's funds or personal data.

Furthermore, Sahoo S.R. et al. [15] proposed exploratory developments in spam detection techniques based on data collected over the past decade . This paper proposes methods for protecting unique user accounts and provides a comparative analysis of various methodologies for detecting spammers.

Table 2: Major security issues/attacks and their impact

Attacks / security issues	Basic Security Goals in Web Services		
	Privacy	Integrity	Availability
Bonet	1	1	1
XSS attack with content tracking	1	0	0
Click hacking	1	0	0
Interdomain attack	1	0	0
Creation of a fake profile	0	1	0
Attack "Friend in the middle"	1	1	1
Attack on Cloning Personal Data	1	0	0
Identity theft attack	1	1	1
Malware scanner	1	0	0
Malicious Web Content / Malicious	1	1	0
Social Campaigns	1	1	0
Distribution of Malware	1	0	1

Phishing	1	0	0
Privacy Conflicts	1	0	0
Session capture	1	1	0
Social engineering	1	1	0
Spamming	1	0	1
SQL injection	1	1	0
Sibyl Attack	1	1	1
Third Party Application	1	0	0

In Ref. [16], Al-Zoubi A.M. et al. also proposed five classification algorithms in the spam detection domain, namely, k-nearest neighbours (k-NN), random

forest (RF), naive Bayes (NB), decision tree (DT) classifiers (J48) and multilayer perceptron (MLP).

There are five filter-based feature selection methods, namely, informative*, chi-square, bump, correlation, and significance*.

Profile clone attack. There are no strict rules on the uniqueness of content in social networks (*personal data: full name, date of birth, photo, etc.)*, which allows the attackers to implement cloning one more virtual user profile. Attackers use this approach for various purposes, but the most common purpose is obtaining funds.

Ref. [17] proposed a model of hierarchical fuzzy methods. An analysis of existing methods for detecting malicious accounts showed that most of them are based on clustering models.

In Ref. [18, 19], Meleshko Y. et al. and Abulais M. et al. proposed a method for detecting a bot network in a recommender system based on graph clustering and analysing user actions. The authors demonstrated the capabilities of socialbots and malicious accounts.

This approach distinguishes three categories of the goals of socialbots: *active, reactive and inactive users*. These malicious accounts can influence people's opinions.

In Ref. [20], Rao P.S. and et al. consider an optimal verification model (OMV) that detects fake accounts in a social network, the so-called OM-SS. The authors propose using a fuzzy decision model to distinguish fake accounts from real ones, which maximizes the reliability of online identification.

Social engineering attacks. Social engineering is a method of obtaining the required information, given the psychology of people, by manipulating people to take necessary actions or divulge confidential information. This type of social engineering attack is one of many steps in a more complex fraud scheme.

In Ref. [21], V.Oliseenko and T.V.Tulupyeva contains a recommended method of protection against social engineering. To achieve this goal, an analysis of text messages is carried out, followed by clustering depending on the psychological characteristics of the social network users. This clustering method is based on neural network technologies with long-term and short-term memory architectures.

Fuertes W. et al. [22] conducted a systematic review of the literature from 2011 to 2020. As a result, it was determined that frequent victims of social engineering are users with human behaviour, implying innocence, unconsciousness and lack of training or ability. As the analysis of this author's study showed, the main victims are newly hired employees, people with a certain lack of knowledge, celebrities, politicians, and top middle and top managers.

Leakage of confidential information. In Ref. [23], Gangarde R. et al. demonstrated a new method that effectively provides anonymity in a social network using clustering based on several graph properties. The purpose of the clustering method is to achieve confidentiality of the edge, node, and user attributes in the graph. The application of clustering methods to graphs describing the authorship of scientific publications enables the determination of stable subgraphs (author groups) and the roles (contribution) of individual authors.

The main idea of the authors Naomi J.F. et al. [24] is to conceal the user information in such a way that the original data are transformed by data anonymization in accordance with the rules of data security and privacy. As a result, using various entropy-based metrics, the system will quantify the leakage of sensitive information, providing effective privacy protection for individual users.

In contrast, Langari R.K. et al. [25] designed a combined anonymization algorithm based on K-member fuzzy clustering and the firefly algorithm (KFCFA) to protect an anonymized database from identity, attribute, link, and similarity attacks and to substantially minimize information loss. The proposed methodology can be used both for the structure of the network graph and for microdata.

In Ref. [26], Mao J. et al. proposed a framework for a systematic analysis of typical approaches to attribute inferencing to highlight existing approaches among them. Four algorithms have been proposed for testing in various preconfigured environments. As a result of the experiment, it was revealed that a dataset that includes behaviour and social relations can improve the accuracy of forecasting, and the marked proportion of users affects the tested algorithms in different ways.

Machine learning techniques for the classification of threats. In Ref. [27], M.H.Jabardi and A.S.Hadi proposed a new approach to detect and classify fake accounts on social networks using ontological engineering. An example is Twitter. The authors focused on inferring ontological levels that are used to detect and classify a fake account and its type depending on the existing relationship. This research focused on machine learning for detection and classification techniques, while this approach demonstrated the use of ontology engineering with semantic web rules. Finally, the main ideas have been modelled across the OWL language, SWRL rules, and the reasoner, using an ontological approach to knowledge representation.

In Ref.[28], Ç.B.Aslan, R.B.Saglam and S.Li proposed automatic detection of cybersecurity-related accounts on social networks on Twitter based on three different sets of features and three different machine learning methods. Maintaining a list of cybersecurity-related accounts manually requires domain-specific knowledge and takes human effort. This work automatically suggests maintaining such a list and using it for more complicated analysis of things such as cybersecurity-related events and human behaviours of cyber criminals and cybersecurity experts via the automated monitoring of accounts on the list.

In Ref. [29], F. Elmendili, N. Maqran, Y.B.el Idrissi and H. Chaoui presented the results of a novel social honeypot-based approach to detecting malicious profiles in published social networking communities. Their main research goal was to investigate techniques and to develop effective tools for automatically detecting and filtering malicious users who target social systems.

By focusing on the social networking community, the authors used a set of users' characteristics and honeypots deployed characteristics to create a malicious profile classifier based on a machine learning algorithm adapted for identifying malicious accounts with high precision and allowing the rate of false-positives. This ongoing work will be used on the analysis results to automatically identify malicious users on the social network.

In Ref.[30], A.Halimi and E.Ayday leveraged a novel message-passing-based framework to model profile matching risk on online social networks. The authors have shown efficient quantification of profile matching risk in social networks via simulations in which the proposed framework provides comparable accuracy, precision, and recall compared to the state-of-the-art, while it is significantly more efficient in terms of its computational complexity. On the other hand, A.Halimi and E.Ayday showed that by controlling the structure of the proposed BP algorithm, one can further decrease the complexity of the algorithm while increasing its accuracy.

In [31], the paper presents an efficient location-sharing protocol to protect privacy in mobile online social networks (mOSNs) for smart cities, which not only supports location sharing among friends and strangers but also protects users' privacy. To develop an efficient protocol, dummy identities have been introduced to protect users' identity privacy and to prevent the location server from inferring users' activity tracks by updating dummy identities in time. This research discovered a new location-sharing protocol that solves these two issues by using symmetric and asymmetric encryption properly.

The publication [32] presents a social bot that can cause social, political, and economic disruptions by spreading rumours. The authors claim that a centralized method to prevent social bots from spreading rumours can be biased and might not be trusted by the users. These studies were based on using Bitcoin as the blockchain platform to form offline channels to develop a high-scale decentralized social network (DSN) and have proven that the proposed method is secure and privacy-preserving and can significantly reduce the spread of rumours using simulations of social networks.

A characteristic common to most of the aforementioned approaches is that they rely on the training of classifiers to determine whether a user's pair is a match or not. Some of these analyses have their origins in primary sources. The time scale of the emergence of threats, as well as the main technologies and means of ensuring the information security of social networks, has been refined and significantly expanded compared to the existing approach, which allows for visual tracing of their

evolution and concludes that there have been no breakthrough technologies in recent years.

5. LIMITATIONS OF STUDY

This research has limitations as the data were collected from different publications belonging to different researchers, as each has its own aims that can be overcome in future studies.

First, the number of datasets in this research may be a little low because the standard principle of content analysis of the publications indexed in the Scopus and WoS databases were collected only in the different languages.

Second, we focus only on the result of the analysis, which allows for the conclusion that most social network researchers use readily available methods for classifying the threats to information security violations, which cannot be considered specifically suitable for the analysis of social networks since they do not reflect the characteristic features of research in this area.

An analysis of the current existing threats and vulnerabilities in the information security of social networks indicates that the achievement of the goals and objectives of information protection, as well as ensuring the maximum level of security, requires the integrated use of available methods and means of protection.

In the near future, we would like to study many improvements and a diversity of research methods to produce a high-quality result in detecting threats and vulnerabilities in information security that proposes a different approach to the clustering of implemented threats to the information security of social networks. One of the main ideas for future improvement in our work is to utilize clustering of implemented threats to the information security of social networks for hybridizing the classification models. Moreover, hybrid models based on these can improve the overall performance of the classification model.

6. CONCLUSIONS AND FUTURE WORK

In today's global information society, the environment for maintaining information security is very heterogeneous; it is complicated in terms of the number and variety of elements and their interrelations and interdependencies.

Therefore, the choice of methods and means of ensuring the information security of a social network requires an integrated approach for the identification of various protection boundaries and the use of legal, organizational, hardware, software, technical and other measures and means of ensuring information security.

The results of a study of a publication for the period 2010-2022 devoted to solving the problems of information security of social networks showed that the peak of the study falls on 2020-2021.

Many researchers most often refer to the data from social networks such as Facebook and Twitter.

Most of the scientific experiments were carried out in offline or online databases of social media users of a particular organization. Appropriate solutions to the problems of threats to information security violations were proposed, depending on the type and classification of social networks.

The complexity of determining the actual threats to data security for the social network under study is the processing of a large amount of data necessary to determine the list of actual threats to the security of confidential information.

The analysis of the study of social network service providers proves that different technologies are used to protect the resources of users' confidential data, depending on the vendor and the country. The main lack of security is the lack of awareness and the careless behaviour of social network users.

Despite the fact that new technology is in the focus of increased interest of representatives of various branches of scientific knowledge, explaining the nature, place and role of social networks in human life, as well as understanding the term "social network" itself, still remains a serious problem.

Moreover, developers need to develop the following for the purpose of prevention:

1. Methodologies for assessing the competencies of the relevant malicious user profile.

2. Models to represent and analyse the dynamics of user security.

It is advisable to continue further scientific research in the following areas using data science technologies:

a) Study of adaptive fuzzy neural systems, Takagi-Sugeno-Kang, Mamdani and Wang-Mendel fuzzy analysis algorithms.

b) Developing and improving the quality of known methods for determining actual vulnerabilities in user security in social networks.

c) Developing and improving the quality of known methods for identifying actual malicious users in social networks.

The established distinctive features of ensuring the information security of a social network require the development and future implementation of

proactive network security management using modern intellectual approaches.

Thus, in our forthcoming study, we will exploit the computer efficiency and the high security of the proposed research to enable the encryption of confidential data of users of social networks.

The proposed approach is a framework that can be used in the future by other researchers, data analysts, and scientists to build potential predictors using proposed models by making necessary changes in their respective approaches or methodology ensuring the safety of social networks.

REFERENCES:

[1] J.A.Barnes, Class and Committees in a Norvegian Island Parish, Human Relations, 7 (1954), 43-44.

[2] https://www.visualcapitalist.com/ranked-social-networks-worldwide-by-users

[3] Simeon O. Edosomwan, S.K.Prakasan, D.Kouame, J.Watson, T.Seymour The history of social media and its impact on business, Journal of Applied Management and Entrepreneurship, 16 (2011) 79-91.

[4] https://www.classmates.com

[5] https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users

[6] https://www.hootsuite.com/resources/digital-trends

[7] M.Castells, The Internet Galaxy: Reflections on the Internet, Business and Society, Yekaterinburg, U-Factoria, 2004

[8] E.M.Jin, M.Girvan and M.E.J.Newman, Structure of growing social networks, Physical Review E:Statistical, Nonlinear, and Soft Matter Physics, 4 (2001), https://doi.org/10.1103/ Phys RevE. 64. 046 13

[9] https://tadviser.com/index.php/Article:Social_networks

[10] V.Smirnov and P.Filippova, Providing information security to protect computer and network data, Journal StudNet, 5 (2021), https://elibrary.ru/item.asp?id=45760820

[11] J.A.Lewis, Zh.M.Smith, E.Lostri, Report by McAfee: The Hidden Costs of Cybercrime, https://www.csis.org/analysis/hidden-costs-cyber crime

[12] Business Information Security, Research on Current Trends in Business Information Security, Kaspersky Lab, 2014, https://press.kaspersky.com

[13] C.Okoli, A Guide to Conducting a Standalone Systematic Literature Review, Communications of the Association for Information Systems, 37 (2015), 879–910, https://doi.org/ 10.17705/ 1CAIS. 03743

[14] S.Afonin, V.Vasenin, A.Kozitsyn, D.Golomazov, A.Bakhtin, G.Gankin, Intelligent System of Theoretical Research of Scientific and Technical Information (ISTINA), Moscow, Moscow University Press, 2014.

[15] S.R.Sahoo, B.B. Gupta, D Peraković, F.J.G. Peñalvo, I Cvitić, Spammer Detection Approaches in Online Social Network (OSNs), in book A Survey, Sustainable Management of Manufacturing Systems in Industry 4.0, Springer, Cham, 2022, pp.159-180

[16] A.M.Al-Zoubi, H.Faris, J.Alqatawna, M.Hassonah, Spam Profiles Detection on Social Networks Using Computational Intelligence Methods: The Effect of the Lingual Context, Journal of Information Science, 1 (2021) 58-81, https://doi.org/10.1177/01655515198 61599

[17] N.Pasieka, M.Kulynych, S.Chupakhina, Y.Romanyshyn, M.Pasieka Harmful Effects of Fake Social Media Accounts and Learning Platforms, in CEUR Workshop Proceedings, vol.2923, 2021, pp.258-271, http://ceur-ws.org/Vol-2923/paper28.pdf

[18] Y.Meleshko, M.Yakymenko, S.Semenov, A Method of Detecting Bot Networks Based on Graph Clustering in the Recommendation System of Social Network, in CEUR Workshop Proceedings, 2021, pp.1249-1261, http://ceur-ws.org/Vol-2870/paper92.pdf

[19] M.Abulaish, M.Fazil, A Machine Learning Approach for Socialbot Targets Detection on Twitter, Journal of Intelligent & Fuzzy Systems, 3 (2021) 4115 - 4133, https://doi.org/ 10.3233/JIFS-200682

[20] P.S.Rao, J.Gyani and G.Narsimha, OVM-OSN: An Optimal Validation Model Applied to Detection of Fake Accounts on Online Social Networks, International Journal of Internet Technology and Secured Transactions, 2 (2021) 109-130.

[21] V.Oliseenko and T.V.Tulupyeva Neural Network Approach in the Task of Multi-label Classification of User Posts in Online Social Networks, in Proceedings of XXIV International Conference on Soft Computing and Measurements (SCM) – IEEE, 2021, pp. 46-48.

[22] W.Fuertes, D.Arévalo, M.B.Ron Impact of Social Engineering Attacks: A Literature

Review, in book Developments and Advances in Defense and Security, 2022, pp. 25-35, https://doi.org/10.1007/978-981-16-4884-7_3

[23] R.Gangarde, A.Pawar, A.Sharma, R.Joshi, Privacy Preservation in Online Social Networks Using Multiple-Graph-Properties-Based Clustering to Ensure k-Anonymity, l-Diversity, and t-Closeness, Electronics, 22 (2021), http://dx.doi.org/ 10.3390 /electronics 10222877

[24] J.F.Naomi, A.Vasanthageethan, G.Roshini, G.Roshini, Data Privacy Preserving Recommendations for Social Media, in Proceedings of 7th International Conference on Advanced Computing and Communication Systems (ICACCS) - IEEE, vol.1, 2021, pp.1229-1232, https://doi.org/10.1109/ICACCS51430.2021. 9441870

[25] R.K.Langari, S.Sardar, S.A.Amin Mousavi and R.Radfar, Combined Fuzzy Clustering and Firefly Algorithm for Privacy Preserving in Social Networks, Expert Systems with Applications, 141 (2020), https://doi.org/10.1016/j.eswa. 2019.1129 68

[26] J.Mao, Y.Yang, T.Zhang, Empirical Analysis of Attribute Inference Techniques in Online Social Network, IEEE Transactions on Network Science and Engineering, 2 (2021) 881-893, https://doi.org/10.1109/TNSE.2020.3009864

[27] M.H.Jabardi and A.S.Hadi, Twitter Fake Account Detection and Classification using Ontological Engineering and Semantic Web Rule Language, Karbala International Journal of Modern Science, 4 (2020) 404-413, https://doi.org/ 10.33640/2405-609X.2285

[28] Ç.B.Aslan, R.B.Saglam, S.Li, Automatic detection of cyber security related accounts on online social networks: Twitter as an example, in Proceedings of the 9th International Conference on Social Media and Society, 2018, pp. 236-240, https://doi.org/ 10.1145/3217804. 3217919

[29] F.Elmendili, N.Maqran, Y.B.el Idrissi, H. Chaoui, A security approach based on honeypots: Protecting Online Social network from malicious profiles, Advances in Science Technology and Engineering Systems Journal, 3 (2017) 198-204, https://doi.org/ 10.25046 /aj020326

[30] A.Halimi and E.Ayday, Efficient Quantification of Profile Matching Risk in Social Networks Using Belief Propagation Computer Security – ESORICS 2020: in Proceedings 25th European Symposium on Research in Computer Security, 2020, p.110–130 https://doi.org/10.1007/978-3-030-58951-6_6

[31] Ou Ruan, Lixiao Zhang and Yuanyuan Zhang, Location-Sharing Protocol for Privacy Protection in Mobile Online Social Networks, EURASIP Journal on Wireless Communications and Networking, 1 (2021), https://doi.org/10.1186/ s13638-021-01999-z

[32] S.Thakur and J.G. Breslin Rumour prevention in social networks with layer 2 blockchains, Social Network Analysis and Mining, 1 (2021) 1-17, https://doi.org/10.1007/s13278-021-00819-y