Analysis of modern mechanisms of influence on the mass consciousness in cyberspace and ways to prevent the spreading of destructive information

Volodymyr Shypovskyi *[1 A]; Volodymyr Cherneha [2 A]

*Corresponding author: [1] Senior research officer of Research Section of the Educational and Research Center of Strategic Communications in the Sphere of National Security and Defense, e-mail: vladimir.shipovsky@gmail.com, ORCID: 0000-0003-3743-3064
[2] Ph.D in Technical Science, Docent of Department of Information Technology and Information Security Employment, e-mail: chevn1980@gmail.com, ORCID: 0000-0016-1903-3252

[A] National Defence University of Ukraine named Ivan Chernyiakhovskyi, 28 Povitroflotsky Ave., Kyiv, 03049, Ukraine

Received: May 17, 2021 | Revised: June 6, 2021 | Accepted: June 30, 2021

DOI: 10.5281/zenodo.4904603

Abstract

Information and destructive influence on Ukrainian society has become an effective element of the hybrid war, which has long been conducted by special units of the Russian Federation. Under the guise of imaginary intentions to help the Russian-speaking population, Russia is trying to seize economically profitable and strategically profitable territories of Ukraine, actively setting up special-purpose military units without sparing the country's financial resources. The information space (mass media and other Internet-sources) has acquired the status of a separate arena for the aggressive use of forces and means of the armed forces of the Russian Federation. The popularity of social media has opened a separate space for the application of informational influence on certain target audiences. To research the issue, it is necessary to identify the causes and mechanisms of the impact of media content on human consciousness. The development of social media has established a new level for mass communications, through the creation of numerous groups – Internet communities (virtual communities) with fundamentally new opportunities to influence traditional public and state structures. It is possible to define virtual communities as a type of communities that arise and function in the information space (primarily through the Internet) in order to help solve their professional, political problems, meet their needs in art, leisure and more (Porter, Constance Elise, 2004). Along with constructive virtual communities that seek to actively interact with society, with the aim of improving the lives of society as a whole and individual social groups and individuals, social media are increasingly used to create destructive virtual communities. However, destructive virtual communities, in contrast to constructive ones, try to fight this community in various, not always legal, ways. The object of aggression of destructive virtual communities can be a society or supporters of certain social groups, usually hostile to this destructive virtual community (Carley K., Lee J., Krackhardt D., 2002). That is why virtual communities are increasingly used in the interests of information and psychological influence by Russian military specialists in social engineering. They provide wide spectrum of opportunities in terms of influencing the formation of world public opinion, political, economic and military decisions, influencing the information resources of the enemy and the dissemination of specially prepared information (misinformation) (Hrynenko I., Prokofieva-Yanchylenko D., 2012).

Key words: bot farms, bots, cyberspace, social media, destructive influence, cyberprotection, destructive information.

Introduction

Facebook owner Mark Zuckerberg said during the 56th Munich Security Conference that millions of fake accounts are deleted from the network every day. He noted that most fake

accounts are detected within couple minutes after registration. Zuckerberg added that Facebook spends billions of dollars annually on post analysis and content security. He did not give exact figures, but said it was more than the company's revenue when it went public in 2012. The head of Facebook expressed the opinion that there is no need for special regulations for "harmful content" (Zuckerberg told). In their official blog, the company's representatives reported that in 2020, more than a hundred anti-Ukrainian accounts maintained by Russia's intelligence services were removed from Instagram and Facebook. Social network administrators deleted 78 Facebook accounts, as well as 29 groups, 11 pages and 4 Instagram accounts. They were engaged in misinformation about Ukraine and neighboring countries, the report said. It is noted that the authors of the accounts pretended to be locals and tried to influence public opinion within the country. Some of them introduced themselves as local journalists and tried to establish contact with politicians, journalists and other public figures in the regions. Content on the pages was published in Russian, English and Ukrainian. The news concerned politics, wrote there about public figures in Ukraine, the military activities of the Russian Federation in Syria. Also – about the downed plane of Malaysian airlines in Ukraine in 2014. Processes in social media are of great interest in science, but the pace of research lags far behind the development of social media. In research related to combating the destructive information and psychological influence of security and defense scientists are interested in the following areas:

research of problems of creation of systems of monitoring of content of social resources of the Internet for the purpose of reconnaissance and information confrontation by means of OSINT;

ways to automatically detect fake pages through which destructive content is distributed;

development of methods and algorithms for conducting information operations in open (closed) resources of the Internet.

Material and methods

The purpose of the article is to analyze the factors influencing the movement of information messages and to determine the factors influencing the distribution of information content in numerous groups of social media as subjects of information security of the state; classification of categories and types of virtual communities, according to the methods of information and psychological influence on users of social media; to consider modern methods of manipulation in the Internet space (bot farms), methods and means of detecting and assessing information threats of virtual communities in the Internet environment of social media and to determine recommendations for detecting, preventing and rapid neutralization destructive information content.

Analysis of recent research and publications. Monitoring of the information space today is in the list of tasks of all structures of the security and defense sector of Ukraine, research of social media is set out in the scientific works of D. Lande, O. Dodonov, G. Pocheptsov; research and models of informational influence in social media are also offered by D. Gubanov, E. Smith. Representatives of business and other areas of civil society, using the monitoring of the information space, analyzing the information obtained and as an effective targeting tool, have already achieved high results. Various issues concerning the formation and development of a virtual society are considered in the works of the following scientists: M. Castells, D. Bell, A. Touraine, A. Toffler, J. Galbraith, R. Ingelgart. The scientific works of a number of researchers are devoted to the basic principles and principles of using social media and predicting the further development of this form of human interaction in the Internet, such as J. Walter, D. Westerman, B. Van Der Hyde, C. Tong, L. Langwell, J. Kim, J. Anthony. The possibilities of the Internet and social media have not yet been fully explored, but the available research shows

their huge impact on the formation of human consciousness, behavior, values, lifestyle, choice of goals and ways to achieve it. It should also be noted that in the modern literature there are few works devoted to the issue of positive and negative aspects of the use of social media by modern youth. Thus, despite the large number of publications on this issue, it remains actual.

Results and discussion

The development of any information content always carries a message for a certain category of users, so the strategy of such influences includes the formation of a clear idea of the target audience, which may consist of potential consumers; real consumers who make decisions about actions or influence decision-making; individuals; interest groups; social groups or society as a whole. The characteristics of the target audience greatly influence the decision of a social engineering specialist about when, where, how and to whom he will address and what his message will be. The key to the success of the promotion of the narrative in its formation is the correct definition of the segments of consumers of information content, and then the target audience of the message. However, no information source is able to influence all audiences at once, while satisfying the demands of all consumers of information, on the contrary, it will prosper only if it clearly identifies its potential consumer and will influence him. The target audience is homogeneous with special parameters (socio-economic, geographical, demographic, behavioral). company or information transaction. For the rapid dissemination of information messages (messages) it will be rational to influence the category of recipients who have access to a certain group of users, so the following categories will be relevant for the implementation of mass communications:

1. Media Relations:
owners and correspondents of news agencies;
TV crews and column editors;
radio journalists;
online media journalists;
journalists of periodicals;
editors of specialized sections.
2. Distributors of goods and services:
existing and potential;
satisfied and dissatisfied (loyal, disloyal);
3. Influencers (Influence Relations) – agents of influence:
bloggers;
thought leaders, stars, famous people.
4. Partners, dealers and sales representatives:
customers, contractors, subcontractors;
5. Employees of companies.
6. Residents of a particular region: district, city, region, country, several countries, the world.
7. Tourists, guests of the region, emigrants, refugees.
8. Representatives of the diaspora, national minorities.
9. People united by common beliefs, denominations, etc.

Socio-psychological studies of mass audiences show that communication processes are most successful with small groups, with a clearly segmented audience by interests, expectations and preferences. Here are some more approaches to the classification of target audiences on the following grounds:

geographical segmentation – depending on the place of residence, for example: consumers living in the central or southern region, in a large or small city, in a rural area;

demographic segmentation – depending on such characteristics of consumers as age, sex, marital status, stage of the family life cycle, religion, nationality, ethnic group;

socio-economic segmentation – by income level, occupation, level of education;

psychographic segmentation – division into different groups depending on social class, lifestyle or personal characteristics of consumers;

behavioral segmentation – division depending on such characteristics of consumers as the level of awareness and knowledge, typical behavioral scenarios, the nature of product use or reaction to it (Types of market segmentation).

When considering these segmentation criteria, a “portrait” of a potential recipient of the message emerges, and information space is also segmented. The content producer, having

studied the target audiences and possible channels of information dissemination, dividing it into segments, allocates one or more of them for targeted influence for the implementation of personal goals. This is the definition of the target audience. The structure of the target audience is not strictly uniform.

The key information that a communications specialist should receive in the process of analyzing the target audience is the core target audience of the brand / product / service / product. It is necessary that in the next stages of creating and implementing an information strategy to choose such channels and tools that will be most effective. The core of the target audience can be understood as a kind of collective image or profile, a portrait of the consumer of information. As listed properties use any information that may in one way or another affect consumer behavior. Note that for any such profile it is easy to make an imaginary portrait of the content consumer and on its basis to draw certain conclusions about the choice of communication channels, related audiences, efficiency, etc.

Finding out how to determine the target audience for targeted (more targeted) influence, and defining social media as a communication channel – on the example of the most popular social network Facebook, consider such an effective tool of media manipulation as fake user groups of "bots". The purposes of manipulation with the use of "bot farms" are quite different – from the sale of household goods to information wars between countries. Numerous attempts to understand the reasons for Donald Trump's surprise victory in the 2016 US presidential election have shown the world how politicians and their teams use social media to achieve their goals. The attention of researchers in recent times requires the question of such a phenomenon as bot farms, which are an effective means of influencing the minds of users of social media. *Bots* (short for "robot") – a special program that performs automatically and / or according to a set schedule any actions through the same interfaces as a normal user. We will consider bots as a tool of manipulative influence for the user to obtain material benefits or coercion and encourage a certain action in favor of the customer. Consider the most common types of bots on Facebook, determine their purpose and features of their use:

Simple bots – awkwardly created accounts without a profile photo, with a small number of friends, empty or clogged with reposts tape. They are usually created automatically using scripts that can be found online. such bots perform a huge number of similar actions every day, thanks to which Facebook quickly finds and blocks them. Due to the fact that the task of such bots is to convey the message and disappear under the attack of moderators, the creators do not particularly try to make them look like real people. Depending on the activity, their life cycle is from one day to several months.

Ordinary bots – differ from simple by the presence of a cover picture and a profile photo with flowers, kittens, campaign pictures and almost never – with a person. Such accounts are created with more advanced versions of scripts, less often – manually. A better page fill allows such accounts to live a little longer than one day.

Foreign bots – accounts with exotic foreign names, bought cheaply at foreign "bot farms". The price varies depending on the country of origin. In general, this is a fairly common business in a number of third world countries, where accounts are produced on an industrial scale and are cheap. (For example, in Laos, the number of registered Facebook users is 3 times higher than the total number of Internet users among the country's population). In other respects, the external features of foreign bots are quite consistent with the classic works.

A bot with a character is a bot with behavior similar to the actions of a living person. Such accounts use different types of posts in the feed, under which there are lone likes or comments. The advantage of such pages is that they really resemble the pages of real people. Disadvantage – due to the dispersion of posts, the account may not have a clearly segmented audience.

Smart-bots – accounts that are created by a complex program that convincingly mimics human actions on a social network. As a result, they do not arouse suspicion in Facebook, as

invisible to its algorithms for calculating search engines that spread spam. "Smart-bots" accumulate in friends and an active audience and regularly interact with it. Not every specialist will be able to recognize the virtuality of such an account – for this you need to set such a goal, know where to look for flaws and spend a lot of time. By and large, not every page of a real network user looks as believable as these accounts. So, users do not even guess that they see in the tape content created by the machine. They carefully gather and protect their audience. This is an interesting and valuable category, because with its help the customer can really achieve real results. Such bots are able to form or change information on a social network, to influence the opinion of ordinary people, journalists, politicians.

Boots with emotions. Fanatical Leaders of Public Opinion. The top of the food chain is among the search bots that spread spam. Manually created and carefully maintained accounts. Each of them has its own positioning and audience. Many of them have really interesting and unique content. Such accounts are few and they are used to throw the information needed by the customer, rather than to scale it – to overclock them to help attract bots simpler and cheaper.

Community leaders. Experts, journalists, public figures and just people whose accounts have gained mass popularity. For money, other forms of reward or just at the call of the heart write about what is interesting to the customer. All political forces have scraps of different levels of training. Despite a powerful resource of popularity, the attitude to "emotional bots" on the Ukrainian Internet can be classified as skeptical. On the one hand, every opinion leader has an audience that listens eagerly to every word, on the other – criticism of ideological opponents and discrediting through paid publications.

People and other public entities. When accusing bots of information spam, we should not forget about real people who have nothing to do with bots, but work on social media in someone's interests.

Regular users of social media. Forcing ordinary users to write about what the customer needs is the goal of the "bot farm". It is achieved in two ways – by educating the right audience or wrapping it in the right information cocoon. The first option is simple, but unstable, because it involves the regular involvement of a large number of people, which is motivated only by ideas. There are regular slogans, appeals, accents on stimuli, social problems, etc. The second is more complex and requires more time to prepare, but due to the fact that the desired information field is created around the target audience – provides a longer effect when the recipients of the message take the necessary action or disseminate information on an ongoing basis, without guessing that someone controls them (Bot farms in Ukraine).

Consider some structures of bot farms. *"Bot farm"* in this article we consider – *a system or complex of fake users, created to exert informational psychological impact on a specific target audience, or a person to change their behavior and encourage action (manipulation of emotions and thoughts), beneficial to the customer. Consider the elements of the bot farm and determine their purpose.* Figure 1 shows an approximate structure of a bot farm.

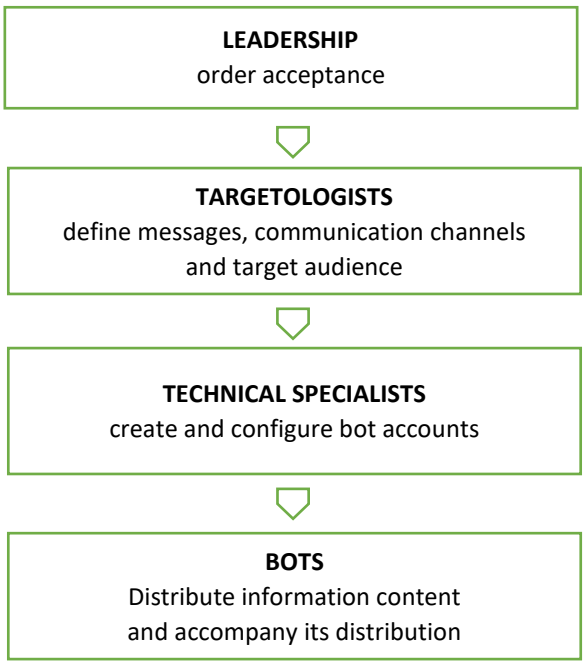

Fig. 1. The simple structure of the bot farm

The Leadership of the bot farm communicates directly with the customer, discusses the price and

the expected effect. After determining the purpose of using a bot farm, *targetologists* determine the target audience depending on age, geographical location, financial opportunities and interests and build a strategy for using bots. Technicians create user accounts (pages) for bots that distribute informational content or comment on posts in favor of the customer or vice versa: discredit a certain person or (circle of people).

By inertia in the formation of the information field are still widely used publics and groups, but their role is gradually weakening. There are two reasons for this: Facebook's algorithm, which gives them a low rank when issuing a post in the feed, as well as the low quality of content of such publics and groups, multiplied by harmful and unsystematic tools for their promotion (I am bot).

Next, we will carry out ways to identify a given content, including destructive). Each popular search engine (Google, Bing, etc.) has services of targeted (targeted) information retrieval on the Internet, developed a large number of special software for monitoring and content analysis of the Internet environment with different types of visualization. The main functions of these services and software:

provide information retrieval in the Internet environment with the help of an operator or automated;

detect content with searchable words, phrases or graphics;

to analyze the content, namely the automatic processing of information flows, detection of facts and events in news Internet resources;

visualization of the obtained data search results in the form of diagrams, graphs and other types of reports.

Monitoring of Internet-sources means the process of constant collection of information from social media and other Internet media for further analysis. The main task of collection information is to identify social media pages with content that is relevant to search. Representatives of the security and defense sector are primarily interested in the information content, which poses an information threat to the national security of the state, society and ways to increase the authority of law enforcement agencies and the level of patriotic consciousness of citizens. One of the areas of effective tools of content analysis is Opinion Mining – a technology for intelligent detection of "subjective" information (opinions, judgments in the form of feedback with emotional color) from textual information posted on Internet resources (Pang B., Lee L.). Systems and technologies for extracting evaluation judgments are used for automated evaluation (positive, negative, neutral) of events from Internet resources. Developed automated systems for classification and analysis of Internet texts are based, as a rule, on the correlation of the text fragment with pre-compiled tonal dictionaries. According to the set of revealed emotional vocabulary, the text is evaluated as positive or negative. However, the information content of discussion pages of numerous groups in social media is generated directly by users of social media with its features: non-standard word order in expressions, a large amount of colloquial vocabulary, with ambiguous content depending on the direction of discussion or expression of emotions. Therefore, it can be concluded that there is no ideal monitoring system for social media. Another controversial issue regarding the analysis of virtual communities is the uncertainty of assessing the information threat of a large group. In research (Gorbulin, V. P., Dodonov, O. G., Lande, D. V.) the indicator of information threat is the quantitative dynamics, which is characterized as the number of events per unit time or the number of messages related to their content in the media. This definition of information threat is suitable for the analysis of information news Internet resources as an assessment of the intensity of publications on relevant topics. One of the methods of collecting operational information is the use of intelligence from open sources, namely OSINT (open-source intelligence). Today, there is an increase in interest in OSINT not only from journalists, analysts of private companies and ordinary citizens, but also from intelligence analysts, because OSINT has certain advantages over the collection, processing and analysis of information with limited access, rather than requiring special access to information, which saves user time, does not require special skills, significant costs. OSINT – is the collection, analysis, processing of data that are to be shared, but it is always specific data that is

collected and structured in a special way, to answer specific questions. In 1947, CIA analyst Ken Sherman noted that the state received almost 80% of intelligence from open sources.

Analyzing the information threats of Internet communities, which are formed through social media, it will be appropriate to determine the level of information threat Z_i, which considers the following indicators:

information content (coefficient of interest of information) – I_i;

number of members of the Internet community – N_{vc};

frequency of visiting a group or page – F_{pv};

$$Z_i = I_i \cdot N_{vc} \cdot F_{pv}$$

Methods of monitoring and analysis of the content of information flows on the Internet are complicated by the lack of standard methods and solutions, the incompleteness of appropriate technological approaches. Today, research on the analysis of information flows is often narrowly focused. The choice of methods depends on the model by which numerous groups are represented. Thus, formal models of virtual communities based on platforms have been developed in research in this area, but they do not consider the relationship between discussions in the Internet community and virtual communities in social media. Therefore, monitoring and analysis of information threats of numerous groups in social media should provide the following functions:

search in accordance with the keywords in the information content of the pages, areas of discussion of the virtual community on social media;

analysis of the content of the discussion pages of the virtual community in order to form virtual communities (destructive, positive) in accordance with their information content and its focus;

analysis of information risks in accordance with the information content, the number of members of the virtual community; provide recommendations for counteracting the information and psychological impact of the virtual community. Visually, the structure of the model of monitoring social media for the identification and analysis of information threats can be represented by the algorithm presented in Figure 2.

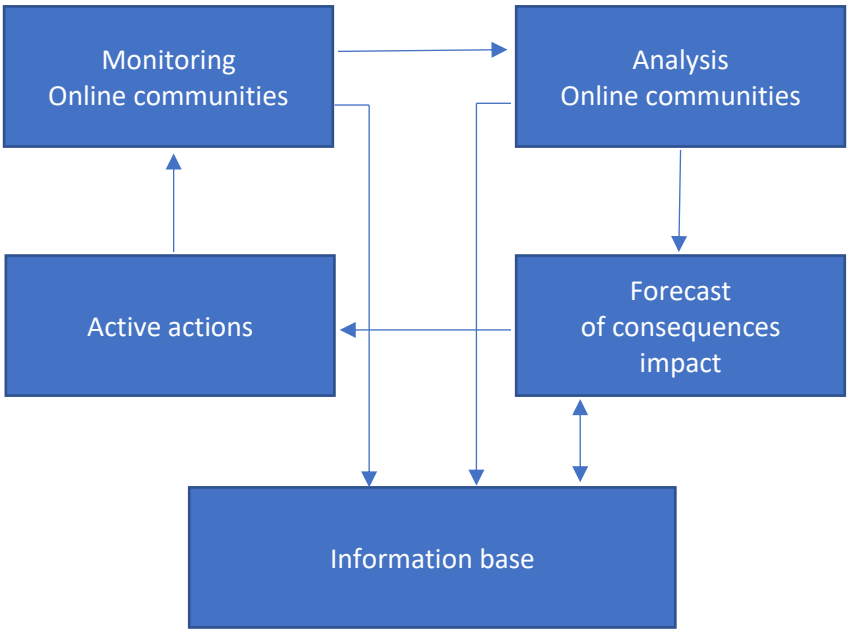

Fig. 2. General scheme of monitoring Internet communities.

Operations of certain blocks can be performed automatically – using special software. Today, media and social media monitoring products are presented in large numbers. The current level of content monitoring (content analysis of information

flows) realizes the identification of the relationships of individual categories in the messages, grouping of these categories, their visualization. The methods of cluster analysis are used, which allow to form compact groups of categories on the basis of detection of latent features, to reveal the main ones, to visualize interrelations (Berko A. Yu., Kis Ya. P., Sukhoversky V. I., 2011).

Existing software allows you to define the characteristics of information messages, such as:

quantitative dynamics (number of events per unit time);

definition of the main plots of publications in the media on the selected phenomenon;

ranking and analysis of the dynamics of development of individual manifestations;

statistical, correlation analysis of the general dynamics and dynamics of separate manifestations;

forecasting the development of the phenomenon and its individual manifestations.

To research the relationship between real events and publications about them on the Internet created services for monitoring, systematization and analysis of information (Information system InfoStream, Information and Analytical Agency “Context Media”, Automatic Information Service "Tape.com", etc.) with access to operational information and analytical work (construction of tables, diagrams). The tasks of monitoring social media (Hootsuite, YouScan, Twitalyzer, WildFire, including free: SocialMention, SocialSeek) are also successfully solved. At the same time, the algorithms of this software work by detecting the semantic content of the content and do not allow to identify images and videos that are rapidly gaining popularity on social media.

Conclusions

Thus, the new challenges of modern life of a conscious person, who is born in an aggressive communication web, force to develop new types of protection of consciousness from infection by the outsiders, who pursue their personal goals, changing the behavior of target audiences. The political intentions of people who are capable of achieving their goals by neglecting thousands of victims are destroying democracy and destroying the reality of the worldview of modern media users. Today we can no longer trust what we have heard or seen, we cannot trust the influential people or authorities of today – we must analyze and filter the entire flow of information, making conclusions about whether we need this information and how safe it is for us. Thus, it is safe to say that social media from a broad communication portal are gradually becoming an information weapon against different target audiences of society, and instead of uniting users – social media divide and set users against each other. Cyberspace has already acquired the status of a new theater of combat use by influencing the mass consciousness, and the main threat of action in cyberspace is the problem of identifying and neutralizing the source of “information infection”. To prevent destructive influences on users through social media, it is necessary to adjust the regulatory framework for information policy, namely:

- every Internet user must log in, which will identify the source of destructive influence;
- special state services must constantly monitor cyberspace and influence all sources of mass broadcasting (social networks, blogs, news and Internet sources, etc.). However, in cases of detection of a threat of destructive information influence, such services should be able to neutralize the communication channel of information transmission rapidly;
- it is necessary to create a regulatory framework for the use of cyberspace in our country. Information sources of other countries must follow the rules of cyberspace use;
- practical experience in combating botnets (bot farms) and destructive influences in cyberspace is set out in many US military regulations and military standards of other NATO member countries, the basics of which need to be adapted for use in the Armed Forces of Ukraine (Rossiytsev, V., 2020; FM 3-12).

The development of information technologies raises the question – *"Can freedom of speech be more important than the security of the citizens of*

Ukraine?". The answer to this question is in the basic law of Ukraine:

article 34 of the Constitution of Ukraine – Everyone is guaranteed the right to freedom of thought and speech, to freely express their views and beliefs. Everyone has the right to freely collect, store, use and disseminate information orally, in writing or otherwise – of their choice, but – the exercise of these rights may be restricted by law in the interests of national security, territorial integrity or public order in order to prevent riots or crimes, to protect public health, to protect the reputation or rights of others, to prevent the disclosure of confidential information or to maintain authority and impartiality of justice;

article 3: Human, his life and health, honor and dignity, inviolability and security are recognized in Ukraine as the highest social value.

So, of course, the government must support and respect freedom of speech in a democratic society, but information sources cannot be hidden and intentionally harm the national interests of the state.

References

Berko A. Yu., Kis Ya. P., Sukhoversky V. I. (2011) Content monitoring system of news Internet resources. *National University "Lviv Polytechnic"*. Vol. 699. [In Ukrainian]

Bot farms in Ukraine: how much. Available from: https://nakipelo.ua/uk/botovodstvo-v-ukraine-chto-pochjom/ [In Russian]

Carley K., Lee J., Krackhardt D. (2002) Destabilizing networks. *Connections*, Vol. 24. №. 3. Available from: https://www.andrew.cmu.edu/user/krack/documents/pubs/2001/2001%20Destabilizing%20Networks.pdf

Constitution of Ukraine. Available from: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text. [In Ukrainian]

FM 3-12. Cyberspace and Electronic Warfare Operations. Available from: https://fas.org/irp/doddir/army/fm3-12.pdf

Gorbulin, V. P., Dodonov, O. G., Lande, D. V. Information operations and security of society: threats, counteraction, modeling: monograph. Kyiv: Intertechnology, 2009. [In Ukrainian]

Hrynenko I., Prokofieva-Yanchylenko D. (2012) Influence of virtual communities on information security: current state and development trends. *Legal, normative and metrological support of information protection system in Ukraine*. № 1 [In Ukrainian]

I am bot. Available from: https://hromadske.ua/posts/ya-bot-film-rozsliduvannya-pro-te-yak-pracyuyut-ukrayinski-botofermi-ta-hto-z-politikiv-koristuyetsya-yihnimi-poslugami/ [In Ukrainian]

Pang B., Lee L. Opinion Mining and Sentiment Analysis // Foundations and Trends in Information Retrieval. Now Publishers Inc. 2008. Vol.2

Porter, Constance Elise. (2004). "A Typology of Virtual Communities: A Multi-Disciplinary Foundation for Future Research".

Removing Coordinated Inauthentic Behavior From Russia, Iran, Vietnam and Myanmar. Available from: https://about.fb.com/news/2020/02/removing-coordinated-inauthentic-behavior/

Rossiytsev, V. (2020). US Army doctrine foundations review and development recommendations on initiation of US Army doctrinal studies for beginners in the context of Ukrainian Armed Forces transition towards NATO standards. *Journal of Scientific Papers "Social Development and Security"*, 10(5). Available from: DOI: 10.33445/sds.2020.10.5.7 [In Ukrainian]

Types of market segmentation. Available from: https://solydus.ru/uk/vidy-segmentacii-rynka-marketing-segmentirovanie-rynka-v-marketinge.html [In Ukrainian]

Zuckerberg told how much Facebook spends on security. Available from: https://www.ukrinform.ua/rubric-technology/2877271-cukerberg-rozpoviv-skilki-facebook-vitracae-na-bezpeku.html [In Ukrainian]