Social media: from communication to security threats

UDK 316.35

Olha Vasylieva

National University "Chernihiv Polytechnic", 1olga.vasiljeva37@gmail.com

Today, the majority of the world's human resources are users of social media, which in turn serve as a mechanism for accumulating and disseminating information. Different social networks have different interfaces and purposes, as well as their own audiences and mechanisms. There is no universal classification of social media types today, and the author [1] suggests the following: professional such as LinkedIn, traditional or universal such as Facebook, "for author's records" or "microblogs" such as Twitter, thematic or academic such as Academia.edu, educational such as TheMathForum.

Other studies distinguish between informative and collaborative social networks [Wellman et al., 1996; Haythornthwaite and Wellman, 1998; Butler, 2001]. Informative social networks are related to the exchange of information and knowledge in the network. They are based on discussing topics and updating information in a chronological order. Communicative social networks are built around a user profile and various applications to enable communication between users. It is this type of social network that is usually regarded as real and represents a model of the relationships that develop between people.

One of the tasks of social networks is the process of communication, and now it is not only non-verbal. According to D. Brass, the following properties of social network subjects can be distinguished (see Table 1) [2].

Table 1

Typical indicators of some social media entities

Characteristics	Definition
Degree	number of direct links to other entities
In-degree	number of references to the entity from other entities
Out-degree	number of references of the entity to other entities
Range / diversity	number of relationships with unrelated entities
Closeness	the extent to which one entity can easily reach another entity
Betweenness	the extent to which the organisation acts as an intermediary between two organisations, providing the shortest route from one to the other
Centrality	the extent to which the entity is central to the network
Prestige	a measure that reflects the centrality of the subject, taking into account the direction of relations. In this case, the prestigious subject is not the source of the relationship, but the object to which the relationship is directed
Roles	
Star	an entity is largely central to the social network

Liason	an entity that has links with two or more unrelated groups, but is not a member of any of them
Bridge	entity that is a member of two or more groups
Gatekeeper	a user who is a sole intermediary or controls the flow of two parts of a social network
Isolate	an entity that has no or relatively few links with other entities

Such properties are determined by the social and psychological characteristics of a person, which encourage him or her to "virtual" life and satisfy his or her needs. Summarising publications and presentations on this issue, we can state that social networks satisfy the following needs of users:

- self-presentation;
- communication;
- in cooperation;
- socialisation.

Today, a person can "log in" to a social network at any time, where all barriers are changing - age, distance, social affiliation are no longer an obstacle to communication. Here you can act both openly and incognito. Anonymity in communication can encourage a person to implement their destructive thoughts online. The user is easily able to find like-minded people in cyberspace, to create groups based on common interests, which may have no analogues in real life. Therefore, communication in cyberspace is extremely attractive and stimulating.

The popularity of social networks has already outgrown the need to intensify communication links, search for friends and strangers, maintain constant contact with friends, and find like-minded people. The human need for self-expression, the desire to be heard, and the impulse to share information about oneself and present one's own image to others are now coming to the fore.

It is also worth highlighting the problem of humanity's use of social media as the formation of a "mass" person. Social networks create a type of communication in which there are no real punishments and no real incentives to reward a particular action, which allows a mass person to avoid unwanted sanctions, which are indispensable in real communication when it is difficult to ignore the interlocutor's negative opinion or objections. Therefore, communication on social media is diluted, losing quality, and quantitative characteristics become the main ones, which is the norm for the mass person, because society considers them only in quantitative terms, and not as a person.

The psychological and social needs of social media users, which shape their self-representation on the network, affect what information the users post about themselves, how they perceive the content they share, and how they communicate with other network members. These indicators determine the degree of vulnerability of a particular user. Using the methods of open source intelligence (OSINT), social media intelligence (SOCMINT), Social Network Analysis (SNA), Sentiment analysis, geolocation data detection, pattern recognition, etc., it is possible to obtain various types of data about a person.

The acquired content is structured or unstructured and is represented by text (posts, reposts, comments), photo and video data, personal data, technical identifiers, a person's

environment, connections, interests, preferences/dislikes, places of stay (residence, work, leisure), professional skills, demographic information, personal traits, etc.

After collection and analysis, such a data set allows third parties (attackers, enemy intelligence services, propagandists, etc.) to carry out various illegal or destructive actions, such as:

1. **Phishing**: Data from social network profiling allows attackers to prepare phishing emails.
2. **Cyberbullying**: Attackers can use information obtained from social media profiles to harass or bully. This may include spreading defamatory information, publishing personal photos without consent, and sending threatening or abusive messages.
3. **Use of data for manipulation or fraud**: Attackers can analyse users' personal information, such as their interests, location, age and other data, to create specialised fraudulent schemes. This can include large-scale scams such as investment fraud or the sale of non-existent goods.
4. **Distribution of malware**: Social media can serve as a platform for the distribution of malware. Attackers can send files or links containing malware to infect victims' computers for further data theft or other fraud.
5. **Identity fraud**: Attackers may collect personal information from users to use it to open accounts, obtain loans, or conduct other financial transactions under a false name.
6. **Spreading fake news and disinformation**: Social media is often used to spread fake news and disinformation. Attackers or manipulators can use detailed analysis of the target audience to create and disseminate distorted information that resonates most effectively with certain groups of users. This can be aimed at sowing discord, influencing political opinions, or manipulating public opinion for commercial or political purposes. Due to the large number of users and the speed at which information spreads on social media, fake news and disinformation can quickly reach large audiences, posing significant challenges to public safety and information accuracy. In addition, automated bots and trolls are often used to amplify the spread of this disinformation, making it even more widespread and difficult to detect.

All of these methods demonstrate the importance of being careful about what information we share on social media, and the need to use appropriate security measures such as two-factor authentication, complex passwords, and regular checks for security updates. It is also important to think critically, check sources of information and use reliable fact-checking tools, which are key to protecting against the impact of disinformation on social media.

1. Pinchuk O. P. Historical and analytical review of the development of social network technologies and prospects for their use in education, Information Technologies and Learning Tools, 2015, Vol. 48, No. 4, pp. 17-19.
2. D. Brass A Social Network Perspective on Human Resources Management Networks in the Knowledge Economy (pp.39-79) Publisher: JAI Press https://www.researchgate.net/publication/234021381_A_Social_Network_Perspective_on_Human_Resources_Management