ACUMEN: INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH
ISSN: 3060-4745 IF(Impact Factor)10.71 / 2025 Volume 2, Issue 10

INFORMATION ATTACKS AND THREATS ON SOCIAL NETWORKS

Mahmudov Murodjon Alisher og'li
3rd-year student, Faculty of International Journalism, UzSWLU

Abstract. Today, social networks have become an integral part of society. Almost every activity is connected to them. Through social networks, one can find sufficient information on any topic, exchange ideas, and gain knowledge. However, due to the vastness of the network, establishing full control over it is a challenging issue. This article discusses the threats and information attacks frequently encountered by users. The information presented below helps users avoid becoming victims of such dangers.

Keywords: virtual social space, cybercrime, social consciousness, cyberbullying, trolling, communication platforms.

INTRODUCTION

Today, it is impossible to imagine human life without social networks. Every person relies on the internet and social networking platforms to stay informed, communicate, express opinions, find jobs, or study. However, the openness and rapidity of information exchange also increase new risks and threats. Information attacks, manipulations, and cybercrimes occurring in the virtual environment directly affect not only a person's digital life but also their psychological state, morality, worldview, and social security.

Observations show that many young people using social networks are not sensitive in selecting information; most of them quickly believe unverified news and rush to make conclusions. This creates conditions for the formation of false beliefs in society. Cybercrimes, misinformation, cyberbullying, pressure, and psychological attacks are among the most damaging factors today. Dangerous ideas, extremist messages, and political manipulations are also spread through social networks. Such threats negatively affect social security. The main reasons are the insufficient development of media literacy among youth and the incomplete content control on social platforms. Media literacy plays an important role in preventing these risks. Without critical thinking skills, a person becomes easily influenced, controlled, and manipulated by social networks.

ISSN: 3060-4745 IF(Impact Factor)10.71 / 2025 Volume 2, Issue 10

LITERATURE REVIEW AND METHODS

In the past, social networks were primarily used to strengthen relationships between people, expand areas of interest, and create opportunities for new connections. Today, social networks have transformed into a "virtual social space" of society. They are no longer just online platforms but powerful tools that deeply penetrate users' personal lives, influencing real-life relations and decisions, especially with the development of artificial intelligence.

A social network is an online platform used for communication, establishing social relations among people with similar interests or offline connections, as well as for entertainment (music and films) and work purposes. The term "social network" was first introduced by sociologist James Barnes in 1954. Social networks hold significant importance in various fields, including education, which has become an integral part of our life. Social platforms enhance learning opportunities, allow users to find study materials and lectures on any topic, and enable students to communicate with peers worldwide at any time. As a result, ideas, experiences, and resources are exchanged. These processes help develop critical thinking, collaborative problem-solving, and the creation of new knowledge.

Characteristics of Information Attacks on Social Networks

Information threat refers to the disruption of protected information in society due to internal or external attacks or malicious intentions. Examples include cybercrime, hacking, dissemination of fake news, and deliberate theft or disclosure of data.

Threats can be classified according to the following criteria:

- **Threats to the main components of information security:** Information security relies on confidentiality and integrity. Sometimes servers freeze or stop functioning. In such cases, signals indicate intrusion attempts, requiring immediate protection. The next stage often involves sending viruses that disable protection systems, causing data leakage or theft.
- **Threats to the components of information systems:** This includes both databases and software. Malicious codes or programs disrupt system stability. In some cases, attackers take advantage of short power surges.

- **Threats by the method of execution (natural, technogenic, accidental, malicious):**
  In this category, attackers play a key role at the final stage. Weak or outdated software often becomes the main "cause." When carried out maliciously, hackers send numerous codes to breach a system. If even one succeeds, the server becomes vulnerable.
- **Threats by the position of the threat source (internal or external):** Internal threats involve individuals directly connected to the system. Sometimes mistakes by employees lead to risks. External threats include all forms of hacking, virus attacks, and bot-generated overloads.

ANALYSIS AND RESULTS

Below are explanations of some scientific terms used above:

Cybercrime – Cybercrime refers to acts committed by individuals for malicious purposes, such as spreading malware, cracking passwords, stealing personal card details and other bank information, or distributing illegal content using the internet. Cybercrime includes a wide range of activities from financial crimes to fraud, cyberpornographic trade, and advertising scams. If malware infects a device, it can damage both the device and the stored data.

Trolling – Trolling refers to posting provocative articles or messages online to incite conflict, provoke users, insult others, and escalate arguments. Trolls are often anonymous and use fake profiles, nicknames, or bots. They may spread fake information on social and political topics. According to researchers, sometimes competing brands spread such "advertisements" to outperform others.

Cyberbullying – Cyberbullying refers to insulting or threatening users through social media posts, instant messages, emails, or SMS. Examples include:

- spreading false information about someone or posting embarrassing photos online;
- sending harmful or threatening messages via messaging platforms;
- impersonating someone and sending offensive messages on their behalf.

Prolonged exposure to cyberbullying negatively affects a person's mental health. Such individuals may frequently become angry, lose their sense of belonging in society,

and have few friends. In some cases, symptoms such as inactivity, headaches, and fatigue are observed.

The analysis of these terms shows that cybercrime, trolling, and cyberbullying in the digital environment are closely interconnected and pose serious threats to information security. In all three cases, the primary target is the human factor. While technical systems can be protected, safeguarding a person's emotions, psychological resilience, and social consciousness is much more complex. The destructive content we encounter daily often aims to influence users' psychological state, manipulate them, or distract them. Cybercriminals prioritize data theft through technical means, whereas trolls and cyberbullies aim to inflict psychological pressure and spark social conflicts. Thus, threats are not only technical but also psychological.

Furthermore, users themselves contribute to the rapid spread of negative content online. For example, when people encounter sensational news, they instantly share it with friends or discuss it publicly. As a result, the information spreads widely and turns into discussions or conflicts. Therefore, content related to trolling and cyberbullying often collects more "views" and audience, increasing its negative impact on society.

As mentioned earlier, cyberbullying severely affects mental health. Individuals exposed to constant pressure experience heightened anxiety, depression, insecurity, and fear of social communication. Gradually, they become easier to manipulate. In extreme cases, cyberbullying may lead to self-harm or suicide attempts. This proves that online aggression and seemingly harmless virtual activities can have serious real-life consequences.

CONCLUSION

The threats discussed above negatively affect not only youth but also minors, whose psychological stability is not yet fully developed and who are more vulnerable to cyberbullying. This poses a significant social risk for the entire community.

To prevent these processes and avoid becoming victims of threats, the following important factors must be strictly observed:

– increasing media literacy;
– developing digital culture;
– enabling two-factor authentication on social platforms;

– installing and updating protective software on mobile devices;
– acquiring skills related to information security and promoting awareness;
– improving legal measures.

The rapid development of the digital environment has fundamentally changed communication among people. While the internet and social networks offer convenience in all areas of life, they have also introduced new types of dangers. Developing media literacy, strengthening personal data protection habits, and cultivating skills for verifying information reliability are essential needs of today. Effective security in the digital space consists of technical protection, legal systems, and human awareness. Only through the integration of these three elements can society build strong immunity against digital threats. Thus, ensuring information security should be viewed as personal responsibility, a strategic duty of the state, and an indicator of society's overall cultural maturity.

REFERENCES

1. Uzwikipedia.org. Terms: "Cybercrime," "Social network." Electronic source.
2. Ernazarov A.E., Jumanov V.I. "Types of Social Networks and Their Importance in Modern Education." Journal of Marketing, Business and Management.
3. Akbarova M.R., Akbarov J.M. Threats to Information Security. . "Экономика и социум", №6(85), ч.1, 2021.
4. "Cyberbullying: What It Is and How to Stop It?" Electronic article.
5. "10 Things Teenagers Want to Know About Cyberbullying." Electronic article.