Problems Of Information And Psychological Security In Open Information Systems

Ilyos Mirziyotov,

Associate Professor
at the International Islamic Academy of Uzbekistan,
Candidate of Pedagogical Sciences.

ABSTRACT

The article explores the growing challenges of **information and psychological security** within open information systems in the digital era. It examines how rapid technological advancement and the expansion of global information flows influence human consciousness, social behavior, and state stability. The study highlights the dual nature of information — as both a constructive force for social progress and a potential source of psychological and moral threats.

It emphasizes the importance of developing a comprehensive **national information policy** that integrates ethical, psychological, and technological measures to protect individuals and society from destructive informational influences. The article also underlines the need for media literacy, moral education, and responsible information use as essential conditions for ensuring mental resilience and social harmony in the modern information age.

Keywords: Information security, psychological security, open information systems, media influence, information policy, information warfare, national interests, mass communication, social psychology, information ethics.

Rapid development has influenced not only traditional principles but also the proportionality of time and space. The emergence of new approaches and development strategies in all spheres of activity has led individuals and regions to shift from isolation toward integration. Today, information is widely distributed and interpreted in various ways. It is difficult to find any field of knowledge in which information does not play a role. The 21st century is recognized as the century when the theoretical and practical creation of information reached its highest point. Therefore, it is rightly called *the Age of Information.*

Information can be defined as a set of data about individuals, objects, facts, events, phenomena, and processes, regardless of its source or form of presentation. Global experience shows that the development of a state's information infrastructure accelerates social progress by transforming not only all spheres of public and state life but also people's worldview, and their conditions for participation in labor, social, and political life. Various information technologies, automated systems, and databases have become integral components of state governance, economic management, and national defense.

Information, like other products, serves its users and consumers; hence, it has its own clientele. It must meet the requirements of recipients and producers. From the customer's point of view, the quality of information should bring additional economic and moral benefits.

From the observer's point of view, it must ensure the protection of important commercial secrets, enable successful competition in production and service markets, and therefore requires the safeguarding of confidential information.

Humanity now lives in an era in which the flow of information has accelerated dramatically. Modern information technology is capable of changing the mood, psychology, goals, aspirations, and even the entire thinking style of the world's population. This phenomenon, a unique achievement of modern civilization, serves to strengthen relationships among peoples and nations, manage global socio-political processes, and foster a global spirit, mindset, and worldview.

However, a reasonable question arises: for what purposes is this immense and powerful force being used? Who benefits from it? The consequences of information depend on its intended use — it can serve both positive and negative purposes. When used for negative purposes, information can have destructive consequences directed toward society, the state, or individuals.

In an information-saturated society, maintaining the balance and integrity of the *"individual–society–state"* relationship becomes increasingly difficult. The acceleration of information flow and the complexity of living in an information-dense environment directly affect human thinking and worldview.

Today, in the age of advanced technology, various types of information can be easily accessed through mass media. Unfortunately, this includes materials that promote destruction, aggression, and immoral behavior — which is especially alarming due to their influence on the minds of young people.

Under conditions of information-driven psychological conflicts, the task of state information policy is to create reliable mechanisms to protect society from negative informational and psychological attacks. Each new information-psychological conflict may bring new threats to the protected society. The greater the number of threats, the higher the level of fear, anxiety, and distrust. Therefore, it is essential to harmonize, guide, and manage the social mood to maintain stability.

Information and psychological security involves preventing political conflicts, enhancing individual self-awareness, and shaping interpersonal relations based on high moral and educational standards. It also requires using the power of information to foster humanitarian thinking, creativity, and constructive capacities.

Society management today demands the search for new methods and techniques to ensure human progress according to modern standards. This includes finding the most effective approaches across interconnected areas such as political-legal, organizational-economic, socio-psychological, and informational governance — in order to strengthen trust in authority, ensure civic unity, and promote moral and ideological cohesion for state development.

Preventing destructive or mind-corrupting ideas spread through mass media depends primarily on improving the education and upbringing of the younger generation and increasing the quality of positive influence. Teachers, psychologists, parents, and community leaders play a vital role in this regard through their knowledge and life experience.

The mass media system today functions as an **open information system**, since in the global context it is impossible to control or regulate information dissemination from one location or state. Hence, it is known as an *open public information system.*

An **open information system** refers to the transparency of media content and the process of information exchange as a social necessity within the global information space — where information becomes an inseparable part of human life and activity. Society must evolve to a level where its members can select from the dense flow of information those that serve national interests and contribute to its development.

Guaranteeing access to information should become a value that transcends individual interests and aligns with national benefit. In such conditions, prohibiting the

dissemination of information that negatively affects public psychology — such as that which incites social, ethnic, religious conflict, violence, war, pornography, or moral degradation — is crucial. Establishing moral and psychological norms based on conscience, sound reason, and high intellectual standards is vital.

The second half of the 20th century was a period of rapid development in information systems and telecommunications technology. These technologies penetrated nearly all aspects of life and human activity, contributing to the globalization of the information space — now recognized as a factor influencing global development. Importantly, people's demand for active information exchange within and outside their countries continues to increase. The rapid growth of the information sector, its potential, and its widespread application in various areas of social and state life make it a key determinant of human progress in the 21st century.

In recent years, **information resources** have increasingly been used as a battleground for inter-state confrontation and geopolitical objectives. This trend is particularly evident among developed countries possessing advanced information technologies that generate significant benefits.

Today, terms such as *"information warfare," "information confrontation,"* and *"information pressure"* are frequently used in international relations, highlighting the urgent need for measures to protect populations from informational attacks. The relevance of this problem lies in the fact that human consciousness (individual, social group, or society) is shaped to a considerable degree by the activities of mass media and information resources.

Therefore, especially under open information system conditions, resolving issues related to the information and psychological security of the individual, society, and the state becomes increasingly important. At the same time, effectively using the potential of the information system to protect and promote national interests, and to create favorable conditions for their realization in the global information space, is of great significance.

Moreover, the field of information — as an independent area of public activity — is still at an early stage of development. Consequently, the study of information-psychological security issues and the training of specialists in this area represent relatively new directions in scientific research. In this regard, there already exists valuable international experience that Uzbekistan can analyze and adapt in line with its national interests.

Conclusion

In the contemporary era of digital transformation and open information systems, ensuring **information and psychological security** has become one of the most pressing challenges for modern societies. The accelerated flow of information, combined with the transparency and accessibility of digital communication, has transformed not only economic and political processes but also the **psychological foundations of human consciousness**.

This study confirms that the influence of information on human cognition, emotional stability, and social behavior can be both constructive and destructive. Properly managed, information contributes to the intellectual and moral development of society, promoting creativity, civic awareness, and innovation. However, when exploited for manipulative or destructive purposes, it leads to disinformation, moral decay, and psychological destabilization — posing real threats to individuals, communities, and the state.

The findings underscore the necessity of **a comprehensive national information policy** that integrates legal, psychological, ethical, and technological measures to protect public consciousness. Moreover, **open information systems**, while vital for transparency and global exchange, require the establishment of strong moral and educational safeguards to prevent the spread of harmful content such as extremism, misinformation, and moral corruption.

Thus, the issue of information and psychological security is not merely technical or administrative; it is deeply **humanitarian and ethical**. It requires a holistic approach —

balancing freedom of information with responsibility, openness with protection, and innovation with moral consciousness.

Recommendations

1. **Develop National Information Security Strategies**
Governments should design and implement comprehensive strategies that combine technological protection with psychological and ethical dimensions. Policies must prioritize national interests while respecting global information exchange principles.

2. **Strengthen Media and Information Literacy (MIL)**
Educational institutions should integrate media literacy programs into curricula at all levels to foster critical thinking, ethical media consumption, and resistance to misinformation — especially among youth.

3. **Promote Ethical Standards in Digital Communication**
Media organizations and online platforms must adopt self-regulation frameworks grounded in moral and psychological responsibility, ensuring that content does not harm public consciousness or social harmony.

4. **Enhance Psychological Resilience and Awareness**
Psychologists, educators, and social institutions should work to develop resilience against informational manipulation, emphasizing emotional intelligence, social empathy, and self-regulation.

5. **Encourage Research and Professional Training**
It is essential to expand academic research on information-psychological security and to train specialists who can analyze and respond to emerging threats in the digital environment.

6. **Foster International Cooperation in Information Security**
Given the global nature of the information space, cooperation between states, organizations, and research institutions is crucial for establishing unified standards of information ethics and security.

7. **Use Information Technologies for Human Development**
Instead of limiting technology, efforts should be made to harness it for creativity, education, and

the promotion of humanitarian values — reinforcing the intellectual and moral potential of society.

References

1. Zinatullin, L. (2016). *The Psychology of Information Security: Resolving Conflicts between Security Compliance and Human Behaviour*. IT Governance Publishing. itgovernanceusa.com+2oreilly.com+2

2. Uchida, K. (2015). "A Psychological Approach to Information Technology Security." In *Human Aspects of Information Security, Privacy, and Trust*, Springer. link.springer.com

3. Baranov, V. V., & Shelupanov, A. A. (2022). "Cognitive Model for Assessing the Security of Information Systems for Various Purposes." *Symmetry*, 14(12), 2631. MDPI

4. Ismoilov, T. I. (2018). "Provision of Information-Psychological Security in Open Information Systems." *CyberLeninka.ru*. КиберЛенинка

5. Yuldasheva, M. M. (2025). "Personal Information Security in a Transforming World." *IJLL (International Journal of …)*. inlibrary.uz

6. Dang-Pham, D. (2025). "Shadow information security practices in organizations: The role of information security transparency, overload, and psychological …" *[Journal unspecified]*. ScienceDirect

7. Totty, S. (2024). "Information Security Research in the Information Systems …" ACM. dl.acm.org

8. Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security* (7th ed.). Cengage Learnin