

Summary

The article deals with the use of techniques and tools that are actively used today to ensure public order. The set of measures for personal security is characterized, characterized by the need to possess police skills, special knowledge and skills in dealing with a large number of people and in the presence of numerous provocations, as well as possible terrorist manifestations while ensuring public security. To accomplish this task, innovative tools and techniques are created to counteract the violation of the procedure established by law. That is why law enforcement officers, according to the requirements of the time, develop a method of counteracting the attempts of public disorder. Profiling is a progressive method of ensuring public safety and order that is used in the context of combating terrorist acts. The main purpose of profiling is to identify potentially dangerous persons, and its basis is the visual diagnosis of the psycho-emotional state of the person (observation and special survey; fixation). The most severe and problematic measure of coercion is the use of firearms, so tactical skills and knowledge of the field. The use of firearms by police officers always entails certain consequences, the assessment of which depends on the reaction of the public and the authorities.

The combination of theoretical profiling training with the practical experience of Ukrainian MIA staff and other law enforcement agencies can become a serious weapon in the fight against terrorism.

Keywords: *personal security, public order, public security, terrorist acts, terrorism, profiling, stun gun, special means, coercive measures.*

UDC 351.7

DOI: 10.31733/2078-3566-2019-5-50-53



Nazgul SHARSHENOVA[©]

Ph.D

*(Academy of the Ministry of Internal Affairs
of the Kyrgyz Republic)*

SECURITY ISSUES OF THE KYRGYZ REPUBLIC: POLITICAL AND LEGAL ASPECTS

Назгуль Шаршенова. ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ: ПОЛИТИКО-ПРАВОВЫЕ АСПЕКТЫ. Рассмотрены теоретические аспекты обеспечения национальной безопасности, на основе анализа которых уточняется определение данного понятия. К проблемам, требующим повышенного внимания, в последнее десятилетие прошлого и настоящего века отнесены неравномерное экономическое развитие регионов, истощение природных ресурсов и разрушение окружающей среды, нелегальная миграция, этнические и религиозные конфликты, транснациональная организованная преступность и международный терроризм. Иначе говоря, произошел переход от «жестких», милитаристских вызовов безопасности к «мягким», носящим преимущественно гуманитарный характер, «выплескивающимся» за пределы государства. Для полноты картины необходимо указать на эволюцию «мягких» угроз безопасности. В начале 1990-х годов на первом месте по значимости находились экологические и природоохранные проблемы, наряду с нелегальной миграцией. К началу 2000-х годов акцент все более смещается на такие вызовы мировой безопасности, как транснациональная организованная преступность и международный терроризм. Прямым подтверждением тому служит повсеместный рост проявлений насилия в виде терроризма, имеющего одним из источников усиливающееся экономическое и социальное неравенство. Не менее актуальным остается и вопрос о будущем международных отношений как исходной точки в формировании системы международной безопасности. Дискуссии характеризовались разноречивым видением ее будущего, положив начало продолжительному обсуждению данной проблематики.

Ключевые слова: *национальная безопасность; угроза информационной безопасности; обеспечение информационной безопасности; цель; задачи и субъекты обеспечения политических механизмов в обеспечении безопасности; выявление и противодействие угрозе национальной безопасности.*

Problem statement. Recent achievements of science and technology have led to rapid changes in social, economic and political processes due to information and technologies spheres development. At the same time, information technology is becoming one of the main factors affecting the lives of people, societies and even whole countries. Information society was formed

gradually, sequentially, with the development of information technology. Technologies development, as well as their use by government institutions assumes that they will help realize constitutional rights of citizens, contribute to improving human wellbeing by increasing business competitiveness in the country, which will have a positive impact on statehood strengthening.

The increasing role of the media and communications including electronic ones in manipulating public opinion contributes to the intervention of some states in the internal social and political spheres of Kyrgyzstan turning it into a battlefield of information and psychological information war [1, p. 1].

The article's objective. In this regard there is a need to develop an effective state policy in the information sphere in order to maintain sovereignty and strengthen the political, economic and military stability of the country. The national security of the Kyrgyz Republic in modern world is heavily determined by the degree of information and psychological field security and the effectiveness of society information sphere.

Basic content. The state information protection system in the Kyrgyz Republic was established in 1973 on the basis of the Soviet Union political situation which mainly operated in the interests of the Ministry of Defense and the Military and Industrial complex. Information protection was realized on the «secrecy» principle. Much has changed in the field of information security protection after the USSR collapse and the Kyrgyz Republic sovereignty, meanwhile information field has remained unprotected.

The following measures to secure information security have been taken in the country in recent years, in particular: the formation of National Agency for Information Resources, Technologies and Communications (2006); the Interagency Commission on Information Security (2007); Advisory Board of the State Communications Agency under the Government of the Kyrgyz Republic (2010); Information Policy Council under the Ministry of Culture, Information and Tourism and the State Committee of Information Technologies and Communications (2016).

The state policy in the field of ensuring information security is based on compliance with the Constitution and legislation of the Kyrgyz Republic, in particular, on the laws «On Information», «On Guarantees and Freedom of Access to Information», «On Communications», «On Copyright and Related Rights», «On obligatory copy of documents», «On the protection of State Secrets of the Kyrgyz Republic», «On the Media» as well as the Criminal Code, the Civil Code of the Kyrgyz Republic, etc. A draft version of the Concept of Information Security of the Kyrgyz Republic is being developed currently. In addition, the Kyrgyz government is taking steps to realize extensive measures to improve information security. In particular, the legal framework for information security and the mechanisms for its realization are being formed, work on preparation of draft laws regulating public relations in the information sphere with reference to the requirements of modern realities is in progress.

At the same time, an analysis of the state of information security shows that legislative base in force is insufficient, since many issues do not have appropriate legislative regulation and the issue of national information space forming is not touched upon, when covert attacks are carried out by «external players» using the latest technologies.

As of today, the current information infrastructure in the republic is at the formation stage and information systems included into it do not often have access to open communication networks. Specific state policy in the field of national information space creation, the media system development, international information exchange organization is absent. In this context we can note the deterioration of the situation in safety ensuring of information consisting state secrets.

In addition, there has been a significant expansion of space and methods of information safety ensuring in the past 15 years. This process is well represented in special studies on global security, taking into account the transition to orientation to the so-called «soft power 2.0» and those challenges that form global information society and emergence of new sources of threats and crimes [2, p. 98-103].

At the same time, the use of information and communicative technologies (ICT) by state bodies makes it possible to effectively transform the procedures of providing services to citizens, increase efficiency and transparency of its apparatus work and, respectively, the level of citizens' trust towards the state. The development of ICT has also led to media new format formation – all Internet users act as media audience now. Many information agencies have not only their broadcasting web portals but also pages on social networks. According to research, almost 80% of all Internet users in Kyrgyzstan are signed up on one or another social network, automatically increases the visibility of all articles in this kind of media. So-called Internet blogs can be considered separately.

With the current development of technology goals are achieved much faster and more efficiently as a result of new types of struggle, namely, struggle for information space. As a result of this struggle, a new spectrum of so-called information threats appears. Threats of this type are mainly carried out with the help of a special selection of information aimed at society splitting. Such information can be notionally named «an information tool» and with its help it becomes possible to damage the vital interests of the state and this damage can be significant in its destructiveness.

Thus, the destructive effect of an information tool can affect all areas of society functioning. As of today, the information sphere of the Kyrgyz Republic, like any other modern state, has an active impact on all components of national security of the state, namely the political, economic, military, social, environmental and other spheres. And as information and communicative technology formation is developing rapidly, there is a direct correlation between national security ensuring and state information sphere, that is, state information security ensuring becomes one of the most prioritized areas of ensuring and with the development of ICT this dependence will be traced even more. And that is why the information security theory studying and ensuring its application in practice becomes an urgent task not only for state bodies but also for academic community in the Republic.

One of the most important factors in public administration optimizing is the target management of the information sphere in the state domain. It includes the formation and expansion of various kinds of information impacts and the management of information resources and information flows. Along with this, management includes the development of both the state information and communicative infrastructure and information products, services and technologies market.

The idea of open information society forming in the form of a sovereign state space, which could integrate into global information space and at the same time serve national interests and features ensuring state information security, is the goal of information security policy of Kyrgyzstan. The creation of a developed information space implies the active use of information sharing networks and telecommunication systems, mass computerization of collecting and processing information processes in all spheres of activity. This process has covered practically all countries of the world and is currently one of the main factors of their social, scientific, technical and, as a consequence, economic development.

A necessary condition for the effective implementation of policy of ensuring and maintaining the state of information security is the development of technological and organizational measures to protect public administration structures from unauthorized influence on state communication systems carried out with the aim of causing damage to the especially important interests of both the state as a whole and society and each citizen.

With the information and communication technologies development, especially if to consider what impact so-called social networks have on information space of any state, it has become especially relevant during the recent events in Syria when terrorist organization actively used social networks such as Facebook, Instagram and others for recruitment. In social networks of this kind, developers put privacy (secrecy, that is, protection against unauthorized access) of the users' correspondence and messages in closed groups to the foreground, it is almost impossible to track illegal activities of such organizations. Moreover, not only the Kyrgyz Republic but also countries with more developed information and communication infrastructure were not ready for threats of this kind of information and, as a result, national security.

The Internet has become not just a system but a social and technical system of systems. All spheres of human life as well as information flow in government bodies and agencies to a greater or lesser extent depend on software and information and communication technologies. With the growing role of this system, the number of crimes committed with the help of computer technologies is growing and, thus, when it comes to the exchange of information of national importance, the risks for state information security are growing. Although many models for analyzing cybercrime have been proposed, in the human mind a crime committed in cyberspace is not a crime to be punished.

The experience of recent history shows that information can serve as a source of political and social threats. It is for this that political and legal mechanisms for regulating information and information flows are necessary.

Conclusion. To sum it up, we find it efficient to determine the following areas:

- to create a single body coordinating safe collection, storage, processing, transmission and data dissemination. To do this, it is necessary, first of all, to develop a regulatory framework which would define information security levels, what kind of information is related to a

particular level, it is also necessary to consider and standardize cryptographic means of information confidentiality and integrity protection. On the basis of this system it is necessary to develop political and legal mechanisms regulating the activity of these structures;

-to sign agreements with other states in the field of cooperation to prevent cybercrime, as well as the impact of religious extremist and terrorist groups through ICT; with the increasing role of the Internet in the information space, the need to protect human rights and freedoms and society from information that promotes violence and cruelty, imposing false and inaccurate information, from the purposeful formation of a negative worldview of the young generation arises. Moreover, sources of external threats may be outside the jurisdiction of the legislation of the Kyrgyz Republic, which significantly complicates the application of the system of legal measures;

- as it was noted many times, it is necessary to train personnel to counter technical intelligence, protect from information weapons and improve legislative framework in this area;

-it is necessary to support and encourage the capabilities of state and public mass media in order to provide reliable and balanced information in timely manner to all citizens of Kyrgyzstan and foreign audience and also provide government support for the activities of domestic news agencies in promoting their products on the foreign market. But, in our opinion, it is necessary to recognize the objective necessity of legislative restriction (regulation) of media freedom, which is the only way to ensure legal equality in information relations;

- the media, acting as an instrument of interaction, should not strike into the state and society on the path of their confrontation, especially for the purpose of demonstrating their own independence, which sometimes happens in our reality. Independence of the media is not a guarantee of its objectivity. It is well known that the press supporting only the ideas of its own freedom and independence in the future stops reflecting the interests of the individual, society, and the state, that such press creates situations of information danger;

-to improve the legislative framework on the media, to develop the branch of information law and personnel policy on this problem in Kyrgyzstan. It is imperative to organize such a system for training personnel working in the field of information and information technologies (government order) so that they are not subject to unfriendly influence from the outside and theoretically skilled in the field of information security.

We consider it necessary to carry out international cooperation in the field of ensuring information security of the state and to represent the interests of the Kyrgyz Republic in appropriate international organizations.

References

1. Проект Концепции информационной безопасности Кыргызской Республики на 2019-2023 годы развития.

2. Смирнов А. И. Кохтюлина И. Н. Глобальная безопасность и «мягкая сила 2.0»: вызовы и возможности для России. М. : ВНИИГеосистем, 2012. 212 с.

Received to editorial office 10.12.2019

1. Proyeckt Kontseptsii informatsionnoy bezopasnosti Kyrgyzskoy Respubliki na 2019-2023 gody razvitiya, S.1 [Draft on the Concept of Information Security of the Kyrgyz Republic for 2019-2023 years of development], S.1.

2. Smirnov, A. I. Kokhtyulina, I. N. (2012) Global'naya bezopasnost' i «myagkaya sila 2.0»: vyzovy i vozmozhnosti dlya Rossii [Global Security and «Soft Power 2.0»: challenges and opportunities for Russia]. M. : VNIIGeosistem, 2012. 212 s.

Summary

The theoretical aspects of ensuring national security are considered, based on the analysis of which the definition of this concept is clarified. In the last decade of the last and present centuries, the uneven economic development of the regions, the depletion of natural resources and the destruction of the environment, illegal migration, ethnic and religious conflicts, transnational organized crime and international terrorism have been identified as issues requiring increased attention. In other words, there was a transition from «hard», militaristic security challenges to «soft» ones, which are mainly humanitarian in nature, «spilling out» of the state. To complete the picture, it is necessary to point out the evolution of «soft» security threats. In the early 1990s, environmental and environmental issues, along with illegal migration, were in first place in importance. By the early 2000s, the emphasis was increasingly shifting to such global security challenges as transnational organized crime and international terrorism. A direct confirmation of this is the widespread increase in the manifestations of violence in the form of terrorism, which has one of the sources of increasing economic and social inequality. No less relevant is the question of the future of international relations as a starting point in the formation of an international security system. The discussions were characterized by a contradictory vision of its future, laying the foundation for a long discussion of this issue.

Keywords: *national security; threat to information security; ensuring information security; target; tasks and subjects of ensuring political mechanisms in ensuring security; identification and counteraction to a threat to national security.*