

Ірина Алексєєнко,

докторка політичних наук, професорка, заступниця
директорки з наукової роботи, Навчально-науковий інститут
публічного управління та державної служби Київського
національного університету імені Тараса Шевченка

КОНСОЛІДОВАНИЙ АНАЛІЗ ЗАГРОЗ НОВОГО ФОРМАТУ БЕЗПЕЦІ ДЕРЖАВИ

Анотація. Авторкою проведено консолідований аналіз видів тероризму нового формату, здійсненого крізь призму міжнародної та національної безпеки держави. В даному контексті нею доведено, що символічним осередком глобальних викликів сучасності як сукупностей найгостріших глобальних проблем, які постають перед світовою цивілізацією на початку XXI ст., став феномен міжнародного тероризму і його різновид – глобальний терор як терор нового типу, що, на відміну від традиційного терору спрямований проти конкретних осіб, характер демоциду (масових убивств).

Концептуалізовано, що світова політика орієнтована на розв'язання проблем, породжуваних глобалізацією. Глобального характеру сьогодні набуває проблема безпеки в глобалізованому світі. Світова політика наголошує на питаннях глобальної безпеки в тісному зв'язку з проблемами національної й особистої безпеки, як стану захищеності життєво важливих інтересів особистості, що й становить предмет дослідження.

Мета дослідження – осмислення сучасних процесів глобалізації, що відображають потребу ствердження пріоритету загальнолюдських цінностей, що для забезпечення довгострокової глобальної безпеки і сталого розвитку засобами політики важливим є розуміння механізмів функціонування світу глобальної політики, в якому істотне значення відіграють характер діючої політичної культури й політичної свідомості.

Виходячи з цих позицій, аналізуються та узагальнюються різні теоретико – методологічні підходи до мікрополітики, у фокусі уваги якої традиційно перебуває людина, а також виходять на перший план фундаментальні проблеми світоустрою, проблеми сталого розвитку і пов'язані з ними зміни, які переживає світ, суспільство, людина в умовах глобалізації, коли мережа взаємозв'язків структурних одиниць мегасуспільства настільки ускладнюється, що зв'язки на мега-, макро-, мезорівнях безпосередньо фокусуються в окремо взятій особистос-

ті на – мікрорівні. Визначено, що тенденція до розгляду мікрополітичних проблем у контексті глобалізації, свідчить про поступове розширення взаємозв'язків світової і мікрополітики як наукових сфер дослідження, спільним предметом яких стає аналіз проблем глобальної й національної безпеки, забезпечення керованості глобальним розвитком на всіх рівнях організації.

Наукова новизна. Визначено, що тероризм являє собою виклик суверенітету націй-держав їх монополії на насильство. За своєю природою він транснаціональний і нівелює здатність суверенних держав контролювати транскордонні зв'язки. Тероризм став методом нав'язування своєї волі шляхом незаконного (несанкціонованого системними нормами) застосування насильства, підриву монополії сучасної держави на насильство – ключового компонента суверенітету.

Цінність /оригінальність. Виявлено, що тероризм сам значно впливає на розгортання глобальних процесів. Він не зупиняється на кордонах держави, а створює мережу відносин, що перетинають кордони таким чином, що боротьба з тероризмом вимагає міжнародних зусиль і набуває транскордонного характеру.

Практичне значення дослідження. Визначено, що світова політика орієнтована сьогодні на пошук ефективних рішень проблем безпеки і вбачає їх у створенні глобальної системи протидії сучасним загрозам і викликам глобалізації. Система покликана забезпечувати міжнародну стабільність і стійкий розвиток на тривалу перспективу насамперед на основі політичного регулювання глобальних процесів. Світова політика знаходиться перед необхідністю встановлення нових пріоритетів політики глобальної безпеки, можливостей і засобів політичного регулювання глобальної сфери.

Авторкою детально аналізуються проблеми управління інформаційною безпекою в Україні в умовах кризового соціуму, викликів і загроз. Показано, що формування та становленням інформаційної безпеки – це складна, комплексна політико – правова та програмно-технічна проблема. Доведено, що інформаційна безпека – складова національної безпеки. Виходячи з цього, актуалізується необхідність розвитку процедурних положень інформаційної безпеки органів публічної влади.

Обґрунтовується висновок про те, що дослідження важелів управління інформаційною безпекою органів публічної влади в умовах інтеграції інформаційних систем слід розглядати як з технічних позицій, так і з урахуванням значущості зовнішньополітичних та внутрішньополітичних її складових, що в сукупності має значення для наукового осмислення проблем забезпечення безпеки політичного процесу на всіх рівнях.



3.7.1. Terrorism: features, transformation, current problems of research. World experience in the fight against terrorism.

Introdoction. Terrorism, in any form of its manifestation, has become one of the most dangerous in its scale, unpredictability and consequences of socio- political and moral problems. Today, the issue of countering global terrorism has moved from the theoretical stage to the stage of practical cooperation between states that seek to maintain strategic stability and prevent undermining the foundations of functioning of public and civil institutions. This general position would be correct if not for one circumstance: theoretical political-legal and economic problems of terrorism, dialectical ratio of its specific purpose and means of its achievement, its historical and transitional nature, etc., all this is little or no study. In the opinion of a number of researchers, terrorism is a phenomenon that does not have a past on a historical scale.

The most researched domestic science, from the point of view of internal national security, is its information component, in particular the methods of its provision (V. Konakh, Y. Maksimenko), the development of international cooperation in this field (Y. Romanchuk), the role in the context of European integration (D. Dubov) and the fight against terrorism (I. Alekseenko, D. Kislov), the mechanisms of implementation in a particular region (V. Kozubsky) or in the media space (G. Saschuk).

The military aspects of national security have also been analyzed in detail, including from the point of view of the states military might (V. Smolyanyuk), integration with NATO (V. Panasyuk, I. Fanin), threats of intensifying information wars (V. Petrov), etc.

At the same time, these studies are based on the concept of national security, in which the state plays a leading role, so the focus on the priority of human security in the context of reconceptualization, which took place in the late twentieth century, has not yet been fully reflected in the works of domestic researchers. This is what made this scientific research relevant.

Findings. Only from the 1960s and 1970s, terrorist attacks became widely used as a means of political struggle and methods of influencing political processes taking place in society, and therefore the world community was faced with the need to intensify counteraction to acts of international terrorism. It should be noted



that the geographic scope of terrorist activity, which has now spread to almost all regions of the world, has expanded considerably. As a response to this, the cooperation of the states in the fight against terrorism has intensified. However, against the backdrop of the general accumulated experience of legislative and practical work in this area, the need for its synthesis and analysis has sprung up through the prism of possible creative use in the development of international and national concepts of the fight against terrorism.

Systematizing the existing practice of coordinating the efforts of the international community in countering acts of terror, it should be noted that it is based on a number of universal international conventions. Among them: The International Convention for the Suppression of Unlawful Seizure of Aircraft (1970); the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971); the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973); the European Convention against Terrorism (1977); the Convention against the Taking of Hostages (1979); the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988); Convention for the Suppression of Terrorist Bombings (1997); Convention on the Marking of Plastic Explosives for the Purpose of Detection (1999); Convention for the Suppression of the Financing of Terrorism (1999), as well as United Nations Security Council Resolution 1373 on Combating International Terrorism, etc [6].

Important activities in the framework of international cooperation in combating terrorism are being carried out by international organizations and the main policy outcome documents have been developed. Thus, the Declaration and Program of Action adopted at the United Nations World Conference on Human Rights on 25 June 1993 in Vienna states that acts, methods and practices of terrorism in all its forms and manifestations are activities aimed at the destruction of rights, freedoms and democracy and pose a threat to territorial integrity and security [3].

The adoption of national laws to better control the production, trade and export of arms and explosives was highlighted in a separate paragraph. The document obliged the signatories to abandon any passive or active support for terrorists and to strengthen legal measures to prosecute terrorist activities; to bring to trial any person accused of



committing, preparing or assisting in the commission of terrorist acts. It was also recommended that all States prevent the movement of terrorist groups and their individual members and, to that end, introduce stricter border controls and rules on identity and visa documentation.

The expert group on transnational organized crime, meeting in Paris on 12 April 1996, adopted a number of recommendations, such as: States should review their legislation relating to criminal offences, identify a central authority whose structure should be appropriate to the rapid transmission of requests for acts of terrorism and those under preparation. Criminal acts, methods and practices of terrorism, as well as the expressed determination to act to eradicate them, both bilaterally and through multilateral cooperation, were condemned [7].

In the summer of 2005, the European Union drew a line under the previous development of the European community and developed a new vision for the continent. The European Commission's particular focus was on the security of European citizens and the fight against terrorism. The European Commission has prepared the link of key security events in Europe. It is called «Improving European industrial capacity in security research». The proposed measures aim at bridging the gap between civil research supported by EU programs and national and interstate security initiatives. These measures are part of the EU's Seventh Framework Program (2007–2013). Among the selected projects are: improved protection of rail and subway passengers; safer European borders; protection of computers connected to networks; airline safety information network and training; faster and more effective crisis management, airline protection; path to safety: intelligence compatibility; crisis management: real-time monitoring of people indoors; safety research information support network; interface standardization in harbors and at border crossings; unmanned aviation: air surveillance devices; innovative technologies for security and protection of privacy and human rights; exchange of classified information [9, p.52].

The world's leading countries have come to realize that the criminal world has come together much earlier than their law enforcement agencies have realized that terrorism can only be defeated through joint efforts. Thus, the Law of Ukraine «On Combating Terrorism» states that terrorism is a common challenge against all countries, requiring a joint response, and today all countries of the world must unite to fight this threat, to defeat this evil [11].

As for the situation in the post-Soviet republics, it should be noted that the criminal world, in contrast to the political world, with



the destruction of the common legal space in the former Soviet Union, quickly consolidated. Deprivation of law enforcement agencies and special services of the former Soviet republics of a single core led to fragmentation of their efforts, which was immediately used by criminals. Recent years have seen an increase in the number of serious crimes of a transnational nature. Various manifestations of terrorism, drug trafficking and smuggling of weapons and military equipment are widespread.

A number of major inter-State instruments have been signed since 1991 to coordinate the efforts of the competent authorities of Commonwealth of Independent States Member States to combat terrorism and other dangerous crimes. Among them: The Agreement on the Concept of Military Security of the Member States of the Commonwealth of Independent States is a set of agreed and officially accepted views on the protection of the CIS Member States from external threats, ensuring territorial integrity and political stability, as well as an agreement on cooperation in the field of prevention and elimination of consequences of natural and man-made disasters. In 1995-1996, the Concept of Formation of the Information Space of the Commonwealth of Independent States was adopted, and included a set of measures and conditions of mutually beneficial development of interstate information exchanges in the interests of cooperation of the CIS member states in these areas of activity and in accordance with international principles of information dissemination, as well as the Concept of Collective Security of the Collective Security Treaty states, which recognized the most important stage in the codification of the activity was the adoption in 2000 of the Concept of Collective Security of the States Parties to the Collective Security Treaty. The Council of Heads of State of the Joint Action Program to Combat Crime for the period up to 2002 [4].

However, it should be noted that the provisions referred to in the international instruments discussed above are usually not sufficiently specific, which significantly slows down their use by law enforcement and intelligence agencies of States for specific practical purposes.

If we look at the legislation of the United States, Italy, the United Kingdom, France and other countries, then its analysis allows us to identify certain regularities in the fight against terrorism:

Codification of legislative norms in the field of combating terrorism contributes to its more effective implementation;

Domestic law should respond in a timely manner to changes in international treaty practice in this regard, consistently reflecting all its positive aspects;



Despite the trend towards democratization of their legislation in the developed world, States provide for a higher degree of responsibility and punishment for terrorist acts and participation in terrorist activities;

When preparing and adopting legislative and other normative acts regulating the fight against terrorism, it is advisable to proceed from the peculiarities of the complex socio-political and criminogenic situation in the country or region, rather than to adhere to the so-called principle of modeling.[15]

Thus, according to the author, it is obvious that in order to combat this common threat it is necessary to unite the efforts of all state and public structures, branches of government, mass media. A strategy to combat terrorism is needed.

Today, international terrorism creates additional challenges for national and international security, requires the improvement of anti-terrorist policy measures and the fight against terrorism at both the national and international levels. The efforts of many countries are aimed at strengthening protection against the terrorist threat. From the current trends of counterterrorism, we can highlight the following:

1. International cooperation and information exchange between countries on counter-terrorism issues. This was the subject of discussion at the meeting of the United Nations Security Council on 12 December 2016, when resolution No. 2322 (co-authored by Ukraine) was adopted calling on States to strengthen and expand inter-State cooperation and mutual assistance in the field of combating terrorism, exchange of information on terrorist organizations and terrorist fighters, including their biometric and biographical data. Emphasis is placed on the importance of judicial and law enforcement cooperation in the investigation of terrorism-related offences [13].

In this context, we can highlight as an example of the long-term cooperation on counterterrorism the U.S. interaction with the European Union (primarily France, Germany and the United Kingdom), which has been expanding since 2001, when the administration of George W. Bush signed a key agreement with the EU Police Service (Europol). This enabled the exchange of strategic and technical information on counterterrorism, money laundering, and illicit trafficking in drugs, nuclear, radiological substances and human beings. Supplementary agreement concluded in 2002 Europol and the US authorities have allowed for the exchange of personal data of suspects and have also introduced the institution of liaison officers. Cooperation between the EU and the



U.S. has since expanded to include counterterrorism financing, illegal migration and foreign terrorist fighters. Extradition procedures have been simplified and legal cooperation has been strengthened (for example, joint investigation teams or videoconferences on specific criminal proceedings have been introduced) [12].

Two new agreements with Europol on countering illegal migration and foreign fighters were signed by the relevant U.S. agencies in February 2015, providing a platform for information exchange regarding individuals who facilitate the recruitment, transfer and financing of foreign fighters [17, p.79].

1. At the national level, strengthen cooperation and exchange of information on counter-terrorism issues among the competent authorities. A number of measures have been taken by EU Member States, primarily to improve the efficiency of interaction and information exchange between national intelligence and police services, as well as to strengthen border control. Based on information provided by the Anti-Terrorist Group (The Hague), in 2016, a single database was created, in which more than 20 European intelligence services have access in real time. It is planned to implement a pilot project on automated data exchange between law enforcement agencies of the EU member states regarding persons with criminal records. Also, the work on the introduction of the European Travel Authorization Information System is being intensified [1, p.77].

2. Prevention of terrorism, including counteraction to radicalization. Today, specialized programs have been introduced and are being implemented in many countries to prevent the spread of extremist views in society, to prevent young people from being drawn into terrorist organizations, and to apply procedures for granting amnesty to individuals who have participated in terrorist activities and adapting them to peaceful life. Thus, a new OSCE Special Representative has been appointed to coordinate the exchange of experience gained through the implementation of such programs by the 57 member countries of the organization. Governments have drawn attention to the possibility of radicalizing people in places of detention. In order to prevent this threat, the PRC is now considering isolating convicted terrorists from other prisoners [16].

3. Introduction of new technologies to combat terrorism by state authorities. The establishment of the European Centre for Combating Terrorism and Radicalization on the Internet is planned to promote and recruit new followers, given the active use of the Internet and social networks by terrorist organizations. This will be part of the Europol



Internet reference office. In the Czech Republic, the Centre for Combating Terrorism and Hybrid Threats has recently been established within the Czech Ministry of the Interior, focusing on Internet content analysis and response. In the U.S., another area of interest is the fight against terrorism, given the specifics of the 2016 terrorist attack in Nice, France, when the attacker used a truck [10, p.179].

For example, in the United States alone, some 250 million vehicles will be connected to the Internet of Things by 2020, which can be managed through the World Wide Web, enabling terrorists to intercept the management of such assets and carry out terrorist attacks remotely, even without crossing the national border.

Therefore, in the U.S.A. Department of Justice, in view of such a potential threat, a separate group that deals solely with Internet matters has begun to function.

4. It is necessary to specify the sources and determinants of terrorist manifestations, which may include: a sharp drop in living standards of the population, reduction or lack of social protection, strengthening of social injustice, exacerbation of political struggle, growth of nationalism and separatism, imperfection of legislation, decline in the authority of the authorities and its representatives' ill-considered decisions [7].

Analyzing the state of the fight against terrorism in Ukraine, it should be noted that currently the Concept of the fight against terrorism (hereinafter – the Concept), adopted by the Decree of the President of Ukraine on April 23, 2013 No. 230/2013, according to which the main threat to Ukraine is the activity of international terrorist organizations. Thus, it states: «Currently, due to the effective implementation of domestic and foreign policy of Ukraine, it does not apply to states with a high probability of terrorist acts or terrorist attacks on their territories by international terrorist organizations against their representations abroad. In Ukraine, there are no internal prerequisites for the emergence of organizations that have used terrorist methods as a means of achieving political goals or drawing public attention to their ideological or other views» [4].

It is clear that such an assessment of the terrorist threat is no longer true. However, it is difficult to disagree with the Concept's definition of a number of external and internal factors that may become the basis for increasing the level of the terrorist threat in the country. Analysis of the activities of international terrorist organizations and the conduct of ATU in Ukraine in recent years allows us to expand the



list of such impacts. This document identifies eight main directions of implementation of measures and five priorities of the state policy in the field of combating terrorism, based on a comprehensive systemic approach to solving the problem and covers all generally recognized components of the process of countering terrorism, including: prevention of terrorist activities, detection and cessation of such activities, elimination and minimization of its consequences, as well as information, scientific and other support for the fight against terrorism, international cooperation in combating terrorism [18, p.46].

Thus, it is advisable to identify the priorities of the state policy in the field of counterterrorism, including the following:

5. Prevention and elimination of threats to the life and security of citizens, the interests of society and the State, which arose as a result of the Russian Federation's aggression against Ukraine, and had an armed conflict on the territory of Donetsk and Luhansk oblasts;

6. Ensuring the necessary level of anti-terrorist protection after returning to the control of certain areas of the Donetsk and Luhansk regions;

7. Predicting and suppressing possible terrorist manifestations in the rest of Ukraine as a result of Russia's hybrid aggression;

8. Updating the effectiveness of the unified state system of prevention, response and termination of terrorist acts and minimizing their consequences.

We can agree with the idea of domestic researchers that the main tasks in the field of improving the state system of counterterrorism in Ukraine are:

9. Regulation of the procedure of interaction between the subjects of the fight against terrorism in various situations;

10. The procedure for interaction between the State and citizens and society in the implementation of the main objectives of State policy in the relevant area (ensuring public awareness of the danger and the scale of response to the threat, including):

11. Prevention (avoidance of involvement in terrorist activities);

12. Prosecution (cessation of terrorist attacks and investigations);

Strategic context;

Protection (improving the security of suspending terrorist attacks);

– Preparedness (minimizing the consequences of an attack and early recovery);

– the actions of a foreign country



Besides, the following questions require special study: terrorism is generated by growing contradictions between the West and the East, the North and the South, it is not one of the causes of terrorism «hybrid» and local wars, which are sometimes waged by reactionary forces of so-called «civilized» states against «uncivilized» peoples, what is the role of arms and drug trafficking in the emergence of terrorism?

Conclusions. The world policy is focused today on the search for effective solutions to security problems and sees them in the creation of a global system to counter modern threats and challenges of globalization. The system is designed to ensure international stability and sustainable development in the long term, primarily through political regulation of global processes. The international anti-terrorist coalition, as well as the network of mechanisms and agreements created by its participants to ensure security in the world in response to the challenges of terrorism, is considered as the prototype of the system, which is based on a strategy of coercion for short-term prevention of terrorism. At the same time, it is increasingly clear that a strategy of coercion and deterrence of extremism cannot guarantee long-term security in a globalized world. Global politics is faced with the need to set new priorities for global security policy, opportunities and means of political regulation in the global sphere.

The fight against and elimination of terrorism is a long-term process that involves the creation of the necessary objective and subjective conditions to achieve this goal. At the same time, it is impossible to destroy terrorism by force alone: violence inevitably generates new violence.

The most important prerequisite for eradicating terrorism is the stabilization of the economic and political situation in countries and the strengthening of democratic principles in public and political life. It is necessary to form a society in which the social base of terrorism will be sharply reduced. It is especially important that stable democratic political systems, mechanisms of civilized political dialogue and rotation of power are formed in the states. To supplant terrorism from life, a high level of political and legal culture in society is needed, as well as a clear establishment of legal sanctions for terrorist actions.

It is necessary to create favorable conditions for the normal even development of different ethnic groups and ensure the realization of their interests in order to prevent conflicts on the national basis. The



task of the states is to form the self-awareness of all ethnic groups living in the given country, at which the feeling of belonging to the state would be a priority before the factor of ethnicity in the process of self-identification of citizens.

In addition, there is a need to strengthen the efforts of State bodies in carrying out preventive activities. Necessary measures to strengthen border protection, increase control over the activities of foreign organizations to minimize the possibility of importing extremism from other countries. Measures aimed at reducing unemployment and solving urgent social and economic problems can reduce social tension in society and neutralize the main source of potential social excesses.

Meetings and agreements at the highest level alone are not sufficient to eradicate terrorism. An effective response to international terrorism requires the development and implementation of a comprehensive program that includes political, social, economic, legal, ideological, special and other aspects. It must take into account the interests of the population, the problems and the conflict-generating potential of terrorism around the world. There is also a need for interaction and coordination of all forces of society interested in solving this topical problem.

One of the most important areas of activity of the heads of state should be joint cooperation to prevent, localize and stop regional outbursts of extremism, as some conflicts caused by terrorists may cause destabilization in other states. The tragic results of terrorism, which characterize modern politics, should serve as an important warning to all political forces that attempts to solve political, economic and other problems with the help of violence do not contribute to the solution of the set tasks, but, on the contrary, lead to the increase and growth of contradictions in society.

3.7.2. Modern cyber terrorism is a threat to the peace and security of mankind

Formulation of the problem. Globalization trends, along with the emergence of the new power centers and political characters, provoked an interest of the scientific community in the study of legal problems of ensuring information security of the political process, its prerequisites, and factors for ensuring.

The growing interdependence of countries and peoples is one of the most influential global political trends of the modern period.



This is an external prerequisite for the development of information security of the political process. Information security is characterized by both the presence of positive factors and the growth of international information threats in the economic, military, and political spheres of the life of the state, which weakens the stability and cooperation of countries on the world stage.

These information threats are carried out through certain foreign policy characters. Their distinctive feature is the desire to dominate the information space through an informational impact on political associations, individuals and social groups. Along with the foreign policy component, threats are realized by using modern technologies in the field of informatization, that are aimed at destroying the political system, destabilization traditional values, blurring the personality, violating the territorial integrity and sovereignty of states. These are the distinctive characteristics of the internal political component of information security [19, p. 67].

Obviously, the researchers put into focus the problems associated with the development of principles and new technologies of information manipulation in the political sphere, as well as identifying sources to combat emerging threats and implementation of information security at the global, regional, and national levels.

The theoretical aspect of the research topic, in general, is associated with showing the importance of foreign and domestic information security components.

Scientific cognition of the definition of the concept of «information security» is relevant both in theoretical terms and in practice. Some researchers consider this concept as the security of networks and information systems, which is interpreted as cybersecurity. Some researchers of this issue interpret information security as manipulation of information, the impact of information on the consciousness of society, propaganda on the Internet. The study of security threats by using information and computer technologies in the implementation and implementation of socially dangerous crimes, the commission of terrorist acts, interference in the affairs of sovereign states, the unleashing of interstate conflicts, incitement of interethnic hatred is also relevant and very important in the study of information security. Information security is considered the most important component of national security in the conceptual and key regulatory documents of many states. Thereby, the study of goals, objectives, a comparative



analysis of approaches, and key problems of ensuring the security of the political process, assessment of the effectiveness, and efficiency of these approaches seem to be an issue of topical interest. Ukrainian society has passed into a qualitatively new state in the process of social and political transformations of our time. Among other things, it is characterized by the merger of local government bodies with business structures, which brings to a revision of the goals and objectives of state bodies, bodies for ensuring national and regional security [10, p. 317].

The appearance of completely new threats to both national security as a whole and its main components namely to social and economic, public, and information security, causes the transition to a new condition of the state. The emergence of these threats today is dictated primarily by the inconsistency of the legislative framework, its slow and insufficient development, with the rapid development of market relations, Ukraine's integration into global world socio-political relations. All this requires rethinking and developing new mechanisms for organizing counteraction to national and transnational crime, as well as for neutralizing internal and external threats.

Ensuring the reduction of the crime rate is one of the important conditions for the social and political development of Ukraine. Currently, the existing levers and methods of combating crime do not fully correspond to the dynamics of the development of organized crime.

Moreover, they do not help to reduce drug trafficking, human trafficking, extremism, terrorism.

The revolution in the field of information technologies facilitates the creation and implementation of innovations in the social and political system, which is sufficient to effectively solve modern state and regional problems, to ensure the rational use of natural resources, political, social, spiritual, and cultural development of society, as well as its safety. It is notable that criminals also use these advances in information technology. They have unlimited opportunities regarding access to informational, technical, and economic resources, their increase, and adaptation to their activities. These circumstances call for a rethinking of current views and developing new conceptual approaches to information security issues, solving problems with such phenomena as cyber-terrorism and cybercrime to ensure both information security and national security in general [13].

Analysis of recent research and publications. The study of information security issues is carried out primarily with technical positions. This has been happening since 1816.



Such classics of the political thought of that time as David Easton, Gabriel A. Almond and G. Bingham Powell actively participated in the study of the political process. The information and communication model of the political system presented by Karl Wolfgang Deutsch is suitable for the study of information security

The theoretical and methodological basis of this study is based on the treatises of foreign and domestic researchers on information protection and information security, including Bryzhko V., Tsymbaliuk V., Orekhov A., Halchenko O., Kaliuzhniy R., Shamray V., Mezentseva N., Oliinyk O., Savruk M., Arsentieva M., Baturina Y., Vetrova N., A. Krutskikh A., Panferova V., Chernyak L. The problem of information security and its state regulation began to be studied in the second half of the XX century in parallel with the development of the world exchange of scientific and technological achievements. An invaluable contribution to this area was made by: Artamonov G., Azarov Y., Bachilo I., Galushkin A., Dorfman Y., Emelyanov G., Kopylov V., Kulikov S., Lopatin V., Pocheptsov G., Chebotareva A.

Formulation of the goals of the article. The object of the research is an information security of the political process in the system of public administration and local self-government.

The subject of the research is a comprehensive analysis of ensuring information security of the political process, including the regional aspect.

The purpose of the study is to identify effective areas and mechanisms for ensuring the information security of state administration and local government.

Presentation of the main research material. Global trends in the development of the information society dictate the conditions for the complete information transparency of public authorities. In this regard, standards that regulate the access of interested parties to the information resources of the state are being formed. The state power is also dependent on these information resources when developing management decisions. Especially this dependence is manifested in local government, as it is directly related to all spheres of human life and the accumulation of operational information. According to E. Gorshkova the growth of informatization processes in the provision of services by public authorities and local governments with the help of electronic document management contributes to the strengthening of the need for self-government bodies to use information, timeliness, and reliability of its receipt.



According to experts, many databases are exposed to threats of unauthorized access, which entails a negative impact on confidential information, as a result of which the regime for achieving information security is violated. [1, 97] The risk factors in ensuring the security of confidential information in local governments are not clearly identified in any sources. Therefore, we pay special attention to the identification of the risk factors in our study.

- Threats to the constitutional rights and freedoms of man and citizen in the field of information activities and spiritual life.

- Threats to the informatization of management of the development of the territory of the municipality

- Threats to the development and formation of the local information industry, which include the industry of information technology, communications and telecommunications, the efficiency of using local information resources.

- Threats to the security of information systems on the territory of the municipality. The analysis of the problems of information support of local self-government bodies in the regions of Ukraine is carried out, that can be applied from the perspective of our sociological research [17, 78].

The sphere of legal regulation of information support of local self-government should cover the entire life cycle of information support: «design – creation – running – replacement». The last stage is to maintain information support up to date. System replacement strategies based on integral operating costs or on a revaluation basis are possible. There are factors that directly affect the implementation of information security. They were formed according to the results of a sociological survey of local self-government bodies of the regions of Ukraine:

1. Unqualified personnel responsible for providing information support. This is one of the main factors in the formation and enhancement of this type of activity.

2. Lack of resources is also a significant factor. This is due to the fact that it is he who is a prerequisite for the purchase and modernization of ICT and its software.

3. Lack of broadband Internet and lack of providing all local inhabitants with high-quality communications and the Internet

4. Deterioration of hardware and its support, etc [26, p. 75].



These areas will help guide the administration not only on the formation of systematic activities to ensure information security, but also on the development of specific measures in these areas. This will increase the level of information security of local self-government bodies. Rationalization of paper workflow is considered as a significant course of formation security improvement. The amount of information that is processed and transmitted in electronic form is growing significantly. In the modern period, in the context of informatization of communication channels and the transition to electronic document flow. Large amounts of information contained on paper are stored stably and require archival storage in paper form. Moreover, local authorities use organizational and administrative documents, which should be drawn up in paper form. Government regulations or decisions require protection from unauthorized access. It is necessary to reduce the number of specialists in the administration departments involved in making managerial decisions. It is also necessary to guarantee the impersonality of the request, keeping the applicant's personal data only in the department where he applied for getting a permission. It is argued that effective methods of protecting information in subdivisions of local administrations can be implemented with intensive work on the implementation of electronic document management systems. It is necessary to configure the access restriction mode at the electronic document flow [22, p.103]. Unlike paper workflow, it is recommended to grant editing access rights to responsible users for electronic archive folders. Other users can only read these documents. In this case, the information will be protected not only from distribution, but also from unauthorized copying. The protection of paper media can be supported by the obligatory prescription in the specialist's duty regulations of conditions on personal responsibility for the distribution or transfer to third parties of information related to confidential information or state secrets [24, p. 177]. To date, such measures are provided for in specialist's duty regulations of the personnel department, which mainly concern information about state secrets, confidential information and information with limited access. These restrictions are associated with separate types of information, however, do not apply to other types, that reduces the level of security of local governments.

Research objectives required to achieve the purpose of the study:

To carry out a scientific analysis of theoretical approaches to the study of the political process, information security, and information integration as a stage in the development of public administration and local self-government.



To create a model of information openness and to identify the directions of information threats for state authorities and local governments.

The following factors affect the information threats of the first category, proposed in Figure 1:

- adoption of legal acts that infringe upon the rights of citizens in the field of information activities
- establishment of a monopoly on the distribution of telecommunication systems and information within the territory;
- counteraction to criminal structures and protection of the family and personal secrets, telephone conversations, and correspondence;
- restriction of access to publicly needed information;
- unlawful sale of funds that influence public consciousness;
- non-compliance with the statutory provisions, which regulate relations in the informational sphere, by the authorities and public;
- restriction of the access for the public to open information resources, including archival materials and socially significant information;
- aging of systems that accumulate cultural values in education;
- manipulation through information;
- human resources decrease. This makes it difficult to train and retrain personnel for the formation and use of information and telecommunication know-how of technologies;
- non-observance of rights and freedoms in the field of mass communication and information.

Threats to information security of the socio-economic development of state authorities and local governments are:

- monopolization of the information space by a narrow group of information ventures;
- interference in the activities of the media to inform citizens, particularly in the field of education;
- low provision of information resources due to a shortage of qualified personnel, inability to effectively implement it into local information policy.

It is important to analyze the most common factors provoking information security threats. State and local authorities note the technological insecurity of information systems created on the area of the respective entity. Threats to state bodies and local governments are:

- illegal use and collection of information;
- non-compliance with information processing technologies;
- engraftment of unlicensed software components;



- use of elements that destabilize the activity of information security systems;
- damage to processing facilities of information and telecommunication systems;
- active intervention in key data protection systems;
- cracking passwords and information security;
- information leakage through the information transfer path;
- introduction of devices for intercepting information through communication channels;
- theft and destruction of data bearers;
- capturing of information in networks, decryption of information;
- use of unlicensed and uncertified foreign and domestic data protection tools;
- unauthorized access to databases information;
- violation of regulatory legal acts restricting the information dissemination .

Political scientists divide the sources of threats to the information security of the political process at different levels of government into external and internal. The peculiarities of local self-government bodies make it possible to take into account only internal sources. At the same time, it is difficult to distribute external ones, since local information resources are closely related to the resources of the state.

It is challenging to determine the specific boundary of the difference between some specifications from others. It is possible to assume that such a source as the level of corruption in local government is significant.

Corruption is directly related to the information security of the political process. This is due to the existence of organized economic groups and criminal structures. Due to the introduction of admission to confidential information, the influence of criminal structures on the interests of citizens is increasing.

The security in the information sphere of the local community and the whole country decreases. Increasing the transparency of local government information systems enhances the likelihood of a significant reduction of corruption. Information and data about the activities of authorities can be limited and controlled.

The very prerequisites are the basis for the emergence and development of corruption in this case. There is a need to create responsive systems for managing information and resources of local governments, which is limited by financial and labor capabilities.



Small subsidies for the information security of local self-government bodies are associated with the traditions of forming regional budgets (this happens either if necessary or in compliance with regulatory conditions). In addition, the formation of a productive security system requires technological processes, the implementation of which should occur on an ongoing basis.

This requires large-scale funding. As a rule, the local government budgets are not able to provide security. In turn, the irregularity of funding does not contribute to the provision of productive information protection. These prerequisites for the emergence of threats to information security in local governments are associated with the effectiveness of managing the economic development of the territory.

Their low dynamism in providing data to the environment, underdevelopment of the concepts of access to information resources of the community contribute to the formation of alternative methods of data extraction. In this case, local government, restrains users' access to data, this reduces the degree of security of informative data instead of applying the concept of informative security. Sources of threats to protection in local government are difficult to structure, which makes it difficult to eliminate them. These circumstances indicate the relevance of organizing the protection of information and data in the information systems of local government bodies...

Conclusions. Thus, the above-mentioned directions for ensuring information security in the administration of local self-government bodies are associated with the formation of know-how and modern information technologies that have new methods of protecting automated systems and software in order to introduce electronic document management. Forms of personal responsibility and control over the use, distribution and unauthorized copying of information are required. This surveillance guarantees technical means, but, in our opinion, a combination of technical means with administrative control measures will be more effective. Restricting functions carried out with documents that contain confidential information will allow reducing the risk of information leaks. Optimization of internal processes and Optimization of personnel management of local administrations are the first priority measures to improve information security. In addition, the information openness of local governments and authorities, as an innovative factor in the development of management informatization, must also be taken into account. It is necessary for an effective organization of information security



Список використаних джерел

1. Брижко В. М, Цимбалюк В. С. Орехов А. А, Гальченко О. Н. Е-будущее и информационное право / под ред. Р. А. Калюжного, М. Я. Швеца. Киев : Интеграл, 2002. 264 с.
2. Вакулич В. Державна інформаційна політика як механізм реалізації інформаційної функції сучасної держави. *Публічне управління: теорія та практика*. 2014. № 1 (17). С. 97–107.
3. Global Risks Report 2018. URL: <http://www.weforum.org>
4. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії та практики : монографія ; за ред. Р. А. Калюжного, В. О. Шамрая. Київ, 2002. 296 с.
5. Мезенцева Н. Б. Правові засади протидії загрозам інформаційній безпеці та розвитку інформаційного законодавства. *Наукові записки Львів. ун-ту бізнесу та права*. 2013. № 10. С. 214–216.
6. Олійник О. В. Принципи забезпечення інформаційної безпеки України. *Юрид. вісн. повітряне і космічне право*. 2016. Т. 4. № 41. С. 72–78.
7. Саврук М. В. Актуальність проблеми забезпечення інформаційної безпеки України та шляхи її розв'язання системи обробки інформації. 2010. № 3(84). С. 77–79.
8. Тептюк Є. П. Конституційно-правове визначення поняття права на доступ до публічної інформації. *Наук. вісн. Міжнар. гуманітар. ун-ту. Сер. Юриспруденція*. 2014. № 7. С. 85–87.
9. Топчій В. В. Кібертероризм в Україні: поняття та запобігання кримінально-правовим та кримінологічними засобами. *Наук. вісн. Херсон. ун-ту. Сер. Юридичні науки*. 2015. Вип. 6. Т. 3. С. 65–68.
10. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення боротьба з організованою злочинністю і корупцією (теорія і практика). 2012. Вип. 1 (27). С. 312–320.
11. Arquilla J., Ronfeldt D. Networks and Netwars. The Future of Terror, Crime and Militancy. Santa Monica. 2001. 122 p.
12. Dartnell M. A Legal Inter-Network for Terrorism: Issues of Globalization, Fragmentation and Legitimacy. The Future of Terrorism. 2001.
13. Definitions of Community Resilience: An Analysis: A CARRI Report. URL: <http://www.resilientus.org/publications/reports.htm>.
14. EU terrorist list. URL: <http://www.consilium.europa.eu/en/policies/fight-against-terrorism/terrorist-list>
15. European Union Terrorism Situation and Trend Report (TE-SAT). URL: https://www.europol.europa.eu/sites/default/files/documents/europol_tesat_201.pdf
16. Foreign Terrorist Organizations. Bureau of Counter terrorism. URL: <https://www.state.gov/j/ct/rls/other/des/123085.htm>



17. Gunaratna Rohan. After Nice: The Threat Within Europe: URL<https://www.rsis.edu.sg/wp-content/uploads/2016/07/CO16183.pdf>
18. Knutson J. The Terrorist' Dilemmas: Some Implicit Rules of the Game. *Terrorism: An International Journal*. 1980. N 4. P. 192–296.
19. Merari A. Terrorism As a Strategy of Struggle: Past and Future. The Future of Terrorism. Eds. Max Taylor and John Horgan. London : The Guilford Press. 2001. P. 46–60.
20. Nef J. Human Security and Mutual Vulnerability: The Global Political Economy of Development and Underdevelopment. 2nd ed. Ottawa. 1999 245 p.
21. Pollack Joshua H., Wood Jason D. Enhancing Public Resilience to Mass-Casualty WMD Terrorism in the United States: Definitions, Challenges, and Recommendations. Defense Threat Reduction Agency, Advanced Systems and Concepts Office, Report Number ASCO 2010 042, Contract Number DTRA01–03-D0010018. URL: <https://fas.org/irp/agency/dod/dtra/resilience.pdf>
22. Proscribed Terrorist Organisations. UK, May 3, 2017. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/578385/201612_Proscription.pdf
23. Proscribed Terrorist Organisations. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/612076/20170503_Proscription.pdf <http://www.fsb.ru/fsb/npd/terror.htm>
24. Scholte J. A. Globalization. A critical Introduction. London: Palgrave. 2000. 216 p.
25. Schori Liang Christina. The Criminal-Jihadist: Insights into Modern Terrorist Financing. Strategic Security Analysis. URL: <http://www.gcsp.ch/download/6084/137684>
26. Special Report: Building National Resilience to Global Risks. The Global Risks 2013 report, Eighth Edition. World Economic Forum. URL: <http://www.weforum.org>
27. Taylor M., Horgan J. Future Developments of Political Terrorism in Europe. The Future of Terrorism. Eds. Max Taylor and John Horgan. London : Routledge, 2001. 231 p.
28. The Global Terrorism Index 2019. The Institute for Economics and Peace and University of Maryland. P. 45–48. URL: <http://economicsandpeace.org/wp-content/uploads/2019/11/Global-Terrorism-Index-2019.pdf>

References

1. Bryzhko, V. M., Tsybaliuk, V. S., Orekho, A. A., Halchenko, O. N., Kaliuzhnoho R. A. (ed.), Shvetsa M. Ya. (ed.) (2002), E-budushchee y ynformatsyonnoe pravo [E-future and information law], Kyiv, 264 p. (in Ukrainian).
2. Vakulych, V. Derzhavna informatsiina polityka yak mekhanizm realizatsii informatsiinoi funktsii suchasnoi derzhavy [State information



policy as a mechanism for the implementation of the information function of the modern state], *Public Administration: Theory and Practice*, 2014, no 1(17), pp. 97–107 (in Ukrainian).

3. Global Risks Report 2018, Retrieved from: <http://www.weforum.org>. Date of application 01.09.2020.

4. Kaliuzhnoho, R. A. (ed.), Shamraia V. O. (ed.) (2002), *Informatsiine zabezpechennia upravlinskoï diialnosti v umovakh informatyzatsii: orhanizatsiino-pravovi pytannia teorii ta praktyky : monohrafia* [Information support of managerial activity in the conditions of informatization: organizational and legal issues of theory and practice], monograph, Kyiv. 296 p.

5. Mezentseva, N. B. (2013), *Pravovi zasady protydyi zahrozam informatsiinii bezpetsi ta rozvytku informatsiinoho zakonodavstva* [Legal bases of counteraction to threats to information security and development of information legislation], *Naukovi zapysky Lvivskoho universytetu biznesu ta prava*, no 10. pp. 214–216 (in Ukrainian).

6. Oliinyk, O. V. (2016), *Pryntsypy zabezpechennia informatsiinoi bezpeky Ukrainy* [Principles of information security of Ukraine], *Yurydychnyi visnyk povitriane i kosmichne pravo*, vol. 4. no 41. pp. 72–78 (in Ukrainian).

7. Savruk, M. V. (2010), *Aktualnist problemy zabezpechennia informatsiinoi bezpeky Ukrainy ta shliakhy yii rozviazannia* [The urgency of the problem of information security of Ukraine and ways to solve it], *Systemy obrobky informatsii*, no 3 (84). pp. 77–79. (in Ukrainian).

8. Teptiuk, Ye P. (2014), *Konstytutsiino-pravove vyznachennia poniattia prava na dostup do publichnoi informatsii* [Constitutional and legal definition of the concept of the right to access public information], *Naukovi visnyk Mizhnarodnoho humanitarnoho universytetu. Ser. Yurydsprudentsiia*, no 7. pp. 85–87 (in Ukrainian).

9. Topchii, V. V. (2015), *Kiberteroryzm v Ukraini: poniattia ta zapobihannia kryminalno-pravovym ta kryminolohichnymy zasobamy* [Cyberterrorism in Ukraine: the concept and prevention of criminal law and criminological means], *Naukovi visnyk Khersonskoho universytetu. Ser. Yurydychni nauky*, no 6, vol. 3, pp. 65–68 (in Ukrainian).

10. Shelomentsev, V. P. (2012), *Pravove zabezpechennia systemy kibernetychnoi bezpeky Ukrainy ta osnovni napriamy yii udoskonalennia borotba z orhanizovanoi zlochynnisti i koruptsiieiu (teoriia i praktyka)* [Legal support of the cyber security system of Ukraine and the main directions of its improvement fight against organized crime and corruption (theory and practice)], no 1 (27). pp. 312–320 (in Ukrainian).

11. Arquilla, J., Ronfeldt, D. (2001), *Networks and Netwars. The Future of Terror, Crime and Militancy*. Santa Monica. 122 p.

12. Dartnell, M. (2001), *A Legal Inter-Network for Terrorism: Issues of Globalization, Fragmentation and Legitimacy, The Future of Terrorism*.

13. *Definitions of Community Resilience: An Analysis: A CARRI Report*, Retrieved from: <http://www.resilientus.org/publications/reports.html>



14. EU terrorist list, Retrieved from: <http://www.consilium.europa.eu/en/policies/fight-againstterrorism/terrorist-list/>

15. European Union Terrorism Situation and Trend Report (TE-SAT), Retrieved from: https://www.europol.europa.eu/sites/default/files/documents/europol_tesat_201.pdf

16. Foreign Terrorist Organizations. Bureau of Counter terrorism Retrieved from: <https://www.state.gov/j/ct/rls/other/des/123085.htm>

17. Gunaratna, Rohan, After Nice: The Threat Within Europe, Retrieved from: <https://www.rsis.edu.sg/wp-content/uploads/2016/07/CO16183.pdf>

18. Knutson, J. (1980), The Terrorist' Dilemmas: Some Implicit Rules of the Game, *Terrorism: An International Journal*, no 4, pp. 192–296 (in English).

19. Merari, A., Taylor M. (ed.), Horgan J. (ed.), (2001), *Terrorism As a Strategy of Struggle: Past and Future, The Future of Terrorism*, London, pp. 46–60 (in English).

20. Nef, J. (1999), *Human Security and Mutual Vulnerability: The Global Political Economy of Development and Underdevelopment*, 2nd ed. Ottawa. 245 p. (in English).

21. Pollack, Joshua H., Wood, Jason D. (2010), *Enhancing Public Resilience to Mass-Casualty WMD Terrorism in the United States: Definitions, Challenges, and Recommendations*. Defense Threat Reduction Agency, Advanced Systems and Concepts Office, Report Number ASCO 2010 042, Contract Number DTRA01–03-D0010018, Retrieved from: <https://fas.org/irp/agency/dod/dtra/resilience.pdf>

22. Proscribed Terrorist Organisations. UK, May 3, 2017, Retrieved from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/578385/201612_Proscription.pdf

23. Proscribed Terrorist Organisations, Retrieved from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/612076/20170503_Proscription.pdf <http://www.fsb.ru/fsb/npd/terror.htm>

24. Scholte, J. A. (2000), *Globalization. A critical Introduction*, London, 216 p. (in English).

25. Schori Liang Christina, *The Criminal-Jihadist: Insights into Modern Terrorist Financing*, Strategic Security Analysis, Retrieved from: <http://www.gcsp.ch/download/6084/137684>

26. Special Report: Building National Resilience to Global Risks, *The Global Risks 2013 report*, Eighth Edition, World Economic Forum, Retrieved from: <http://www.weforum.org>

27. Taylor, M., Horgan, J. (eds.) (2001), *Future Developments of Political Terrorism in Europe, The Future of Terrorism*, London, 231 p. (in English).

28. *The Global Terrorism Index (2019)*, The Institute for Economics and Peace and University of Maryland, pp. 45–48. Retrieved from: <http://economicandpeace.org/wp-content/uploads/2019/11/Global-Terrorism-Index-2019.pdf>

