Pronoza I.I.

Information counteraction terrorism as a part of state policy fighting terrorism

Pronoza I.I.,
The Candidate of Political Sciences,
Senior Lecturer in Information
and Records of Kyiv National University
of Culture and Arts

This article examines the phenomenon of information terrorism at modern stage. The greatest attention is focused on concepts such as the media- and cyber-terrorism, which are the main component of information terrorism. In this article the essence of this phenomenon is reflected, as well as the degree of legal regulation and prevent terror information at both the international and national level are charactarised. Also, the recommendations for the prevention of information terrorism in Ukraine are provided.

Talking about the information nature of terrorism, it is different from the general concept, primarily because that the the political objectives are achieved indirectly. The violence serves as a cause for manipulation. Terrorism has always informative character, regardless of whether it is a global event, or the localized event, so that the main task is the manipulation (for example intimidation of the population for the emergence of panic or in the form of direct threat, etc.).

Thus, fundamental difference of terrorism from other kinds of violent political struggle is that it is on the edge, because for achieving political goals still using violence against civilians.

International terrorism is one of the most dangerous and difficult to predict phenomena, which conveys a sense of dynamism and diversity, as well as the ability to adapt and modernization in the context of globalization and Informatization. So, one of the threatening manifestations of international terrorism becomes information terrorism, based on the manipulation of consciousness of the masses, distribution of informational and emotional effect, which is designed for the majority of terrorist acts, attracting supporters among members of the society, the impact on the power structures that make political decisions. Understanding in this respect, the phenomenon of information terrorism is a prerequisite for the formation of a clearer understanding of the essence of modern international terrorism, prevention of threats that can destroy state institutions, foundations stability of the state, as the basis of national security of democratic countries in General.

Information terrorism is the merger of physical violence with criminal misuse of information systems, and intentional misuse of digital information systems, networks and their components in order to facilitate terrorist operations or actions.

Keywords: *information, terrorism, information terrorism, cyber-terrorism, media terrorism, information space, mass media.*

In modern terms the increasingly important role of information. As a result of active processes of globalization and development of information and communication technologies and as a result, changes in social and information sector, changing the tools of state policy, both internal and external, and along with economic and political leverage arising equally important information. In the age of information, in the twentieth century, the traditional conflict of material moved in a fundamentally new space – information (cyberspace) where manipulative technologies are becoming broader use. Thanks to these information wars are being destroyed opponents, have an impact on the masses and many other actions. So much popularity recently acquired information terrorism. Understanding this phenomenon is a prerequisite for a more clear understanding of the nature of modern international terrorism, preventing the destructive effects on public institutions and foundations of national security in general.

The essence of the phenomenon of terrorism information actively studied in the works of both foreign and domestic scientists. Researchers who have studied terrorism in the context of globalization, the development of information and communication technologies and the increasing role of the media in society should be noted D. Bella, Zh. Bodriyara, E. Hidensa, M. Kastelsa, E. Tofflera, F. Fukuyamu, S. Huntington, B. Hofmana, A. Shmida and others.

Please note that there is a considerable number of works of local scientists who have made their contribution to the study of the subject. Among them O. Zernetska, O. Hrytsenko, Victor Ivanov, Ye. Makarenko, M. Ozhevana, T. Petriv, H. Pocheptsov, V. Shklyar, A. Chichanovskyy more. However, these developments do not reflect scientists fully trend of rapid development of this phenomenon, and as a result such new phenomena as media terrorism is poorly understood.

The purpose of this article is to study the concept of terrorism information, basic regulations for the regulation of social policy in the European Union.

For a more clear understanding of the essence of the concept of terrorism information should refer to the actual concept of "terrorism". As for the appearance of this term, the first time he appeared in 1798, when the philosopher Immanuel Kant used it to describe a pessimistic view on the fate of mankind.

Today among scientists there is no universally accepted definition of "terrorism", and moreover among some foreign and domestic researchers developed the idea of the impossibility of this definition. For example, this may be the idea U. Lakkera, which focused on the chance, irrationality and inaccessibility understanding of terrorism. He said: "There should be no illusions about what you can learn about the origin and nature of terrorism. Establishing exposed only to the fact that in some, the administration made more terror than the others, and that under certain circumstances he does not have roots. Overload value term in nature defies all efforts to develop a comprehensive and objective definition of terrorism. This definition does not exist and will not be found in the

near future. "[3]. However, terrorism is still possible to define as the central issue in this case is figuring out how consistently and accurately the term applied to the phenomenon, and that stanovytsya main criterion for determining the nature of the concept.

At the present stage, there are many definitions of terrorism. Broadly speaking, terrorism – a method of influence through the attack to achieve certain goals in which victims of the attack are not subject [13]. Now terrorism has acquired a worldwide scale has become a multi-dimensional and multidimensional phenomenon that recently too rapidly evolving and therefore becomes an international character. International terrorism – is implemented on a global or regional scale terrorist organizations and groups, including the support of the public authorities of individual states in order to achieve certain goals socially dangerous acts of violence associated with theft, seizure, or killing innocent people or threat to their life and health, the destruction or threat of destruction of important economic facilities, life support systems, communications, use or threat of use of nuclear, chemical, biological and other weapons of mass destruction [12].

Today, you can select the components of terrorist actions – that they are generalized classification criteria.

So, if we take the view that terrorism is a deliberate action, it is difficult not to agree that mandatory components of this specific action is:
- Subject (or subjects);
- Object (objects);
- The cause and motive;
- The purpose of implementation;
- Temporal and spatial characteristics;
- Instruments used (tools);
- consequences.

In turn, each group of criteria can be divided into subgroups.

For example, among the subjects should be highlighted: the state (special state service authorized to carry out terrorist activities and terrorist organizations supported by the state), international and national terrorist organizations not supported by the state (nationalist, religious, etc.); lone terrorists.

Objects of terrorism include: direct acts of terrorism objects – objects of private violence and illegal acts (individuals or groups of people – hostages, victims of bombings and other terrorist attacks, buildings, vehicles, etc.) and indirect objects terrorist acts (political party, government, group of people, etc.) – the objects of intimidation and pressure, from which usually depends on achieving the goal of the subject of terrorist activity, performance requirements.

The cause and motive of terrorist activities involve the allocation of the factors that motivate subject to implementation of assassination – separating them from the target of terrorism because the proclaimed goal of terrorists is often not the real reasons. The motives of terrorists are often quite irrational, unconscious – of self, identity,

heroism, etc. or objective character – religious features, results upbringing, the influence of society, economic reasons and so on. In addition, in the case of lone terrorists, the cause of action can be a mental disorder.

Target of terrorist activity – is proclaimed terrorist target; what they seek to achieve as a result of a terrorist act (acts) what they require indirect object. The purpose may be political, religious, economic or other nature.

Temporal and spatial characteristics allow for sharing of terrorism for the duration of terrorism and recurrence of terrorist attacks (short-term and long-term, one-off and recurring), the place of execution (depending on geography – Latin American, Eastern European, etc., or space – water, air, land, etc.) and area of distribution (local (local), state, international, global).

In terms of the instruments used (vehicles) can distinguish different types of terrorism. The difficulty of using this criterion is that the subjects of terrorism usually combine several tools – it may be capturing the strategically important object in which there are people who are caught, and a vehicle with a simultaneous stop the normal functioning of transport etc [14].

Talking about information essence of terrorism, it is different from the general concept, primarily to the fact that the political objectives are achieved indirectly. Violence appears pretext for manipulation. Terrorism always carries informational purposes, regardless of whether it is of global events or events of local character, so that the main task – manipulation (or as intimidating the population to panic origin or in the form of direct threats, etc.). Thus, the fundamental difference of terrorism from other types of violent political struggle, is that it is on the verge, so as to achieve political goals still using violence against civilians.

Information terrorism – merger physical violence from criminal misuse of information systems, and intentional abuse of digital information systems, networks or their components to facilitate terrorist operations or actions [2, p. 98].

Information terrorism is used in various areas covering political, philosophical, legal, religious, aesthetic those other views and ideas, that in the spiritual realm where there is a battle of ideas.

This type of terrorism is characterized not only cybercrime but also the correct manipulation of information, its manipulation, and in some cases deliberately false presentation of facts, which is a result of disinformation to intimidate and implementation paranoid thoughts population. For a long time the total brainwashing and change perspective, this type of terrorism was elevated to the rank of state policy, and is used by ruling elites everywhere. Subjects of information terrorism can be considered:
- Foreign intelligence agencies and institutions;
- Domestic and international media;
- Certain extremist groups.

Modern information terrorism is described as a set of information warfare and special operations involv-

ing national or transnational criminal organizations and special services of foreign states. Availability of information technology significantly increases the risk of information terrorism. Sophistication information infrastructure of society contributes to the creation of additional risks of terrorism information.

In turn, the information is divided into terrorism

- Information and psychological terrorism (control of the media to spread disinformation, rumors, demonstrating the power of terrorist organizations)

- Information Technology Terrorism (damage to individual elements and entire media environment as a whole enemy: the destruction of components, active suppression lines, artificial restart communications nodes, etc.) [4].

Pretty typical example for understanding the nature of media terror mechanisms of evocation, promotion and distribution can serve as a specific media outlet like a postcard. It plays a key role not information as such and propaganda, counter-propaganda, propaganda, advertising. Therefore, the main objective of such means of information terrorism is not information, and manipulation.

The main tactics of information terrorism is the presence of the dangerous consequences of a terrorist act on disclosure of information and breadth of great public interest. Along with this, information terrorism, or "cyberterrorism", the forms of action in cyberspace has all the characteristic features of political terrorism in general. Recently, the concept of cyber crossed the boundaries of fiction and widely discussed in the media. The threat of terrorism on the Internet was more than expected, scope and functions kiberteroryzmy incredibly increased the total spread across the Internet. Cyberterrorism is a serious social and dangerous threat to mankind than even nuclear, bacteriological and chemical weapons, and the degree of the threat because of its novelty, not yet fully realized and understood. The experience available to the international community in this area, with all the obvious evidence of the vulnerability of any state, especially as the cyberterrorism has no national borders; kiberteroryst able to equally threaten information systems, located virtually anywhere in the world [1].

Distinguish different types of information terrorism, among which the most common is media terrorism and cyberterrorism.

Media terrorism (or "media-killerstvo") refers to a specific kind of information-psychological terror and is part of "the infrastructure of terror." Its essence lies in attempts by organizing special media campaign to destabilize society, create an atmosphere in it civil disobedience, mistrust of society to the actions and intentions of the government and especially – its security forces designed to protect public order [6].

In the case of media terrorism information refers to the kind of information terrorism that is an abuse of information systems, networks and their components for terrorist acts and actions. The means of imple-

mentation of media terrorism are printed media, network, cable and terrestrial media, the Internet, e-mail, various electronic toys and so on.

Note that most modern forms of terrorism can be attributed to media terrorism, the media serve as an effective tool in the rapid dissemination of information, intimidation of the population and terrorists achieving their goal.

Among the consequences of terrorism can be identified economic, social, political and others. It should be noted that the effects of terrorist activity does not always correspond to the purpose of its implementation subjects. Thus, if the proposed use of criteria, you can determine the place of media terrorism typology of terrorism.

Media Terrorism is a special type of terrorist activity, highlighted by the criterion of the use of tools (means) terrorists achieve their goals.

Given the specificity of the media as a tool in the hands of special subjects terrorist activity, which is due to the specifics of the actual fact that one of the main objectives of terrorists – the rapid dissemination of information among the public – actually coincides with the appointment of media and explains their special role in the globalization of terrorism, further study issues requiring specific functioning of media terrorism as a special kind of terrorism in our country and in the world, including subject-object structure of this phenomenon, its methods, tools and functions and more.

The cheapest and most effective tool considered global media and the Internet, which in conjunction form the information field, where the presence of visible reality conceal the true state of affairs. A striking example is media terrorism terrorist use of the media to inform the public about its activities, the involvement of the activity or psychological impact on people. One of the priorities is the classic terrorists in entering the international information space to spread their own ideology. For example, February 5, 2005 the famous British TV channel "Channel 4" aired an interview with well-known international terrorist Shamil Basayev, which provoked outrage from the Russian Federation.

April 17, 2012 Founder "Wikileaks" Julian Assange spoke live from Hassan Nasrallah – leader of the Shiite radical group "Hezbollah", during which discussed a number of important political issues, particularly the Arab-Israeli conflict, the problem of Palestinian civil war in Syrian Arab Republic and other. This interview was broadcast by many international channels, widely spread on the Internet. This helped to familiarize the general population with the ideology of this movement. Another example of terrorism provide information foundation and opportunities to deliver their opinions and ideas to the world there are numerous American journalists interview with the leader of the international terrorist organization "Al Qaeda" Osama bin Laden.

It is important to note that at present terrorism information widely uses various modern means of communication to facilitate the planning of operations, holding meetings, communication, receipt and

transmission of operational information and more. For example, during the civil war in the Syrian Arab Republic in 2011-2012 Syrian militants are widely used multimedia smart phones Iphone, which later caused their prohibition by the government [10].

Under the influence of individual media terrorism itself is unable to navigate the information space unlimited data available, because the media presented today as a tool for designing false reality. The purpose of this reality show is not the truth and hide it there by making a "soft power" that seeks to conquer man improper judgment. Thus, it is not possible to talk about the transition of information in its quality. This applies particularly to the media, including the Internet, as they are the platform for political games that are designed to distort reality.

Another type of information terrorism is cyberterrorism, which is defined as a set of actions that include information attack on computer information, computer systems, data transmission equipment, and other components of the information infrastructure, carried out by criminal groups or individuals. Cyberterrorism aimed at penetration of information and telecommunications system, the interception management means suppression network of information exchange and implementation of other destructive actions. The danger of this type of information terrorism is that it has no national boundaries (terrorist attacks can be carried out anywhere in the world) and to identify problematic terrorists in cyberspace, because hackers carry out terrorist activities in several front of computers, making it difficult its identification and location [4]. Weapon "kiberterorystiv" constantly improved depending on the remedies used by users of computer networks.

Thus, at the moment cyberterrorism is one of the most dangerous types of crime. Cyber attacks can cause huge damage on the local, national and even international level. Indeed, external cyber attacks can pursue more serious purpose than passive data collection, and objects can be cyber money and confidential information, equipment control devices space, nuclear power, military complexes main computer components and so on.

According to the views of some foreign experts to paralyze the vital point established infrastructure, enough to strike for only a few dozen objects. For example, turn off the computer systems will lead to ruin 20% of medium-sized companies for a few hours, 48% fail within a few days. About 33% of banks will be ruined within a few hours after this disaster, and 50% of them go bankrupt in a few days.

A striking example of cyber attacks on computer node is an explosion of homemade bomb in the electronic underground garage of the international business center in New York, made in the mid-1990s. The explosion injured no one and techniques offices remained intact. However, the main damage was the loss of content databases – software (often unique) and the actual information that was stored.

An example of Internet attack is terrorist action performed 7-9 January 2000, when nine sites leading trading companies underwent massive Internet attack criminals. So, in the morning on the main website Yahoo received nearly a billion downloads. Computers were unable to cope with the amount of information (number of applications typically less than 200 million. Daily) and were shut down one after another. Half an hour later the site Yahoo disconnected from the network. Exactly the same sites were subjected to attacks by other major trading and media companies [17].

It should be noted that due to the globalization of information terrorism and its international character appeared an objective need for legal regulation of the phenomenon at the international level and therefore measures to combat information terrorism must be based on common law, developed by the international community. Needless to say that the policy of "double standards" when the evaluation of certain actions informational nature often depends on political views, religious beliefs or national origin, does not contribute to the destruction of one of the global problems of mankind. Therefore, the information should oppose terrorism united power of the world community, as this phenomenon and has threatened the security of all countries. An example of such a regulation can be considered a single source contract to resolve the problems of cybercrime – Council of Europe Convention of cybercrime concluded November 23, 2001, which states four types of computer crimes, namely:

- Illegal access;
- Illegal interception;
- Interference with the data;
- Interference in system [11].

According to this document cyber tools are: computer system, computer data, ICT services and data traffic. This is the first document signed by 29 states, including Ukraine. [12]

Today, there are two great organizations that are willing to take a leading role in the fight against cybercrime internationally. This division against terrorism OSCE – an organization that operates under the auspices of the UN and Interpol. In addition, the European Union since the new year began work center to combat cyber Crime (European CyberCrime Centre). Member States and European institutions intend to support the Center for Combating cybercrime to create operational and analytical capacity of its investigations and cooperation with international partners [11].

Analyzing and exploring combating cyber development in Ukraine, it is impossible to ascertain the trend of States aimed at joint efforts to counter this phenomenon. Ukraine has risen in the world ranking for the highest number of cyber threats and the first among the ten countries with the most spam and network attacks. Another legal document regulating this sphere is the Information Security Doctrine of Ukraine,

in which one of the key issues is ensuring technological safety, including in the field of information issues and the fight against terrorism technology. However, it is not an effective regulator in their field. Also, never passed the Law on Principles of the State Information Policy. Also in Ukraine has not created combating cyber, which could quickly respond to the challenges in the field of information security.

So now in front of each state, including Ukraine, there is an objective need for effective measures to counter information terrorism. As noted above, an important role in this process is a legal framework that is the basis for the implementation of counter-terrorism. Quite effective is the presence in the Security Service and Interior Ministry joint interactive database of terrorists and persons sympathetic to them, indicating the strong potential rather informative interactions between data structures and can quickly solve the problem on the prevention of terrorism. To successfully address threats cyber terrorism actions necessary to point out a number of key areas such struggle:

- Unification and harmonization of national legislation and international instruments;

- Carrying out scientific research in the field of modern technologies to detect and prevent criminal and terrorist influences on information resources;

- The creation of specialized units in the fight against computer crime and computer terrorism;

- Improvement of the legal international cooperation on combating computer crime and computer terrorism;

- Improvement of multi-level training in information security [5].

Based on the above it can be argued that the fight against kiberzlochynstvom should be based on an integrated approach, combining power, political, diplomatic, economic and humanitarian countermeasures.

If we consider the information measures address threats of terrorism in Ukraine, then in this case it should be noted a number of important issues that must be resolved in order to optimize this response. First of all, we should implement effective information technology, intended to help prevent terrorist and extremist acts in Ukraine.

An important objective is the recognition of the media as independent actors can play an active part in maintaining information security in general and against terrorism in particular. Therefore, it is necessary to provide strengthening the responsibility of the media for possible intensification in society due to inadequate coverage of terrorist acts or vice versa pumping the atmosphere before its implementation.

It is necessary to develop a national information system to counter terrorism by clearly defining the functions and powers of state bodies, NGOs, the media in a complex of measures on information blockade any acts of terrorists.

Equally important is the formation via the mass media complex scientific and educational programs to promote the ideology of non-violence, tolerant behavior, the formation of "anti-terrorist mind" in society, respect for cultural diversity. Intercultural dialogue, which should be implemented by means of mass media, can help avoid various kinds of extremism, violence, xenophobia, religious intolerance in the country [15].

One of the most effective means to combat information terrorism is to create some special institutions designed primarily to develop a new doctrine of information security involving experts and together with the media to implement it as soon as possible. An example of such an institution could be British central office of information that existed before 2011. However, at this point in Ukraine is not an institution set up, but the only establishment of the Information Centre information counter terrorism at the National Security Council and Defense of Ukraine is necessary. This center should have its own functions and perform a number of tasks assigned to it by countering the propaganda of terrorism. Among them are major include:

• information gathering and analysis of terrorist propaganda reasoned elaboration of appropriate responses

• work with the public sector, the formation of an expert pool, including experts from the East Ukraine

• implementation of PR work of state bodies

• Organization of a centralized mass media.

creating the concept of information confrontation of terrorism, in accordance with the above threats:

a) clearly indicate the blame in the events;

b) appeal to law;

c) to calm the population and to offer effective ways of protection;

d) to disseminate information about terrorist crimes against the civilian population and the protection of the public authorities;

e) ensure a dialogue with the authorities, display confidence and success of operations, and so on.

• control closing esters for terrorists, their non-admission to the media etc. [7].

Thus, information terrorism – a phenomenon that developed and spread, making the threat of almost the entire world community. Due to the rapid development of ICT it takes new forms, so that the study of this phenomenon is insufficient and thus the properties of modern information terrorism are the subject of close attention of scientific researchers of the complex socio-political phenomenon, which requires more detailed consideration.

Information as a modern phenomenon of terrorism is a serious threat to security and vital interests as individuals, as a society and state. Obviously, the terrorist use of advanced science and technology greatly expands their destructive capabilities, can attract everyone's attention and keep people in constant

fear. Currently easily vulnerable to terrorists virtually all computer equipment handling and storage.

In summary, to say that the problem of counteraction to acts of terrorism information – is a complex problem. Today's laws must meet the requirements of modern development. To this end, the government of our country should be carried out purposeful work on harmonization and improvement of legislation in the field of information security.

Today there is a problem of information counteraction to acts of terrorism. Therefore, a top priority for Ukraine is purposeful work on harmonization and improvement of legislation in the field of information security. Implementation of effective information policy aimed to inform citizens and ensure their understanding of what are the causes of terrorism, increase media literacy (the ability to resist attempts to manipulate them by means of information flow) and confidence in the state and other components that help build a system to protect every person from negative impact of information terrorism. Regulation and countering terrorism information as one of the components of the civilizing process at the international level should have a cooperative anti-terrorist activities as a subsystem of national and international security systems.

You can identify several main objectives, the implementation of which requires an integrated approach and presents the state of information in the avoidance of threats:

1) Systematic study, data collection and exploration of potential threats kiberterorystychni.

2) Ensure the protection of critical national infrastructure.

3) Development of qualitatively new technologies to protect against cyber attacks. This problem also causes the cooperation with academic and research institutions and organizations.

4) Reduce the number of gaps in national legislation.

5) Reducing latency of computer crimes, as of today, approximately 80% of computer attacks do not entail recourse to law enforcement.

6) Stop mass use in different areas are not properly protected software.

7) Establishment of information security.

8) Revitalization of public opinion in the spirit of rejection analyzed the phenomenon and actively opposed to it.

Without a doubt, the best way to fight against terrorism is just an information support high information technologies and spur technological progress that should serve to counter cybercrime. Financing of high technology in the fight against cybercrime has become a national priority today.

REFERENCES:

1. Boychenko O. Media terrorism: features advanced features information security / AV Boychenko // Integrated intelligent robotic systems (PRTK 2009): second international scientific-practic. Conf. (25-28 May 2009). – K .: NAU, 2009. – P. 230-232.

2. SB Gavrish Computer Terrorism: current status, development forecasts and ways to counter // The fight against organized crime and corruption (theory and practice). – 2009. – № 20.

3. Gerasimenko KS features modern threats "information terrorism" / KS Gerasimenko // Forum law. – 2009. – № 3. – P. 162-166 [electronic resource]. – Access: http://www.nbuv.gov.ua/e-journals/FP/2009-3/09gkczit.pdf4

4. Information Security Doctrine for Ukraine / Ukrainian Artem Bidenko Pravda // 04.18.2014 [electronic resource]. – Access mode: http://www.pravda.com.ua/articles/2014/04/18/7022849/?attempt=1

5. The EU opened a center to combat cyber crime January 3, 2013. [Electronic resource] // newspaper "Mirror of the week. Ukraine". – Access mode: http://dt.ua/TECHNOLOGIES/evrosoyuz_vidkriv_tsentr_po_borotbi_z_kiberzlochinnistyu.html

6. Law of Ukraine "On Combating Terrorism" 638-IV of March 20, 2003.

7. Information aspect terrorism and negotiations with terrorists / Eli Kusa – 02.15.2014 [electronic resource]. – Access: http://mskod.com/informatsiyniy-aspekt-terorizmu-ta-peregovorniy-protses-iz-teroristami/

8. Cyberterrorism as a part of the modern National Security [Electronic resource] – Mode Access: www.nbuv.gov.ua/Portal/soc_gum/bozk/2007/17text/g17_30.htm

9. Convention on Cybercrime: as of 7 September 2009 [electronic resource] // Official Web Portal Verkhovna Rada of Ukraine. – Access mode: http://zakon4.rada.gov.ua/laws/show/994_575

10. Markov MM Terrorism-1997 Duel number 14 (36) [electronic resource]. – Access mode: http://www.agentura.ru/text/biblio/globalmenace.txt

11. Media-terrorism among other types of terrorism: an attempt typological analysis / Tatiana Erokhin [electronic resource]. – Access: http://www.social-science.com.ua/article/1002

12. Sventytska A.V. Information terrorism as a phenomenon of contemporary international politics [Text]: Thesis. Thesis ... candidate. flight. Sciences: 23.00.03 / Sventytska Olesya Vladimirovna; Kyiv National University them. Taras Shevchenko. – K., 2007. – 19 p.

13. Tsyganov VV Media terrorism. Terrorism and the media / V.V. Tsyganov. – K. : Nika-Centre – 2004, 124, p. 15.

14. Shabelnikova NA Information terrorism: the main manifestations and implications // Informatization and information security police. Proceedings of the XV International Scientific Conference, May 23-24, 2006. – M .: Publishing House of Acad. Department of Internal Affairs of Russia, 2006. – P. 167-171.

15. Chambet P. Le cyber-terrorisme / P. Chambet // [Electronic source]. – Régime d'accès: http://www.chambet.com/publications/Cyberterrorisme.pdf

16. Jerrold M. From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism / M. Jerrold // NATO Library at: TERRORISM_AND_POLITICAL_VIOLENCE, vol. 12, no. 2, Summer 2000. –P. 97-122.

17. Laqueur W. New terrorism / NY., Oxford: Oxford University Press, 1977. – 290 p.