UDC 343.1

T. P. Iatsyk ,
candidate of juridical sciences (Ph.D.), Associate Professor of Department of criminal process and criminalistics,
University of the State Fiscal Service of Ukraine

MEDIA TERRORISM AND CYBERTERRORISM AS PROBLEM OF INFORMATION SOCIETY (CRIMINAL PROCEDURE ASPECT)

У статті розглядаються види інформаційного тероризму. Характеризується значення ЗМІ як одного із механізмів впливу на сучасне суспільство. Окреслюються проблеми та напрями вдосконалення ефективної боротьби із медіа-тероризмом та кібертероризмом.

Ключові слова: *засоби масової інформації, інформаційний тероризм, медіа-тероризм, кібертероризм, інформаційне суспільство, кібератаки.*

В статье рассматриваются виды информационного терроризма. Характеризуется значение СМИ как одного из механизмов влияния на современное общество. Определяются проблемы и направления совершенствования эффективной борьбы с медиа-терроризмом и кибертерроризмом.

Ключевые слова: *средства массовой информации, информационный терроризм, медиа-терроризм, кибертерроризм, информационное общество, кибератаки.*

In the article types of information terrorism are considered. Value of media as one of mechanisms of influence on modern society is characterized. Problems and the directions of enhancement of effective fight against media terrorism and a kibertirorizm are determined.

Keywords: *mass media, information terrorism, media terrorism, kibertirorizm, information society, cyber attacks.*

Transition to methods of electronic control by technological processes gives the grounds for emergence of essentially new type of terrorism – cyber terrorism: intervention in work of components of the telecommunication networks functioning in the environment of computer programs or unauthorized modification of computer data causes disorganization of work of crucial elements of infrastructure of the state and creates danger of death of people, causes approaches of significant property damage or other socially dangerous consequences.

Phenomenon of information terrorism works of both foreign, and domestic scientists are devoted. Among theorists and practitioners, researched information terrorism as means of conducting information war in the conditions of the cross-border globalized processes and development of information cyberspace, it should be noted D. Bell, J. Baudrillard, A. Giddens, M. Castells, A. Toffler, F. Fukuyama, S. Huntington, B. Hoffman, A. Schmid.

Cyberterrorism problems are also considered in scientific works of A.I. Primakin, V.E. Kadylin, Yu.I. Zhukov, E.P. Kozhushko and others.

Let's note that despite a large number of works on this perspective, the matter demands further scientific development, and also consideration of a problem of interference of modern terrorism as integral part of information structure and mass media.

Technical progress develops so promptly that some of his consequences are realized by society too late when for correction of a situation already considerable efforts are required. There is even an opinion that upon transition of some critical point progress begins to work already for extermination of mankind. Such situation has developed, for example, with ecology and, unfortunately, it develops also in the field of information technologies.

Terrorists can block work of the subway; to paralyze work of rail and air transport for the purpose of causing an economic damage to the state; to get into local networks of government institutions (the Ministry of Internal Affairs, financial institutions) for the purpose of change or destruction of information, to block operation of computers, to abduct means and so forth.

Information revolution concerned practically all industries of the national economy, all society. The problem of information security was inseparably linked with all other aspects of safety, in particular, personal security, safety of the state and society. Information weapon which now only appears and develops can become very dangerous. It can selectively work, be applied through cross-border linkages that will make impossible identification of a source of the attack. Therefore information weapon becomes ideal means for terrorists, and information terrorism - threat of existence of the whole states that does a question of information security by important aspect of the homeland and international security.

Implementation of modern information technologies, brought, unfortunately, before emergence of new types of crimes, such as computer crime and computer terrorism – illegal intervention in operation of electronic computers, systems and computer networks, stealing, assignment, a racketing of computer information. Cyber terrorism is a new form of terrorism which for achievement of the terrorist purposes uses computers and electronic networks, modern information technologies. On the mechanism, methods of implementation and concealment computer crimes have certain specifics, are characterized by the high level of latency and low level of solvability of crimes [1].

To reveal and neutralize the virtual terrorist very difficult because of too small quantity of the marks left by them, unlike the real world where traces of deeds remains nevertheless more. This property – anonymity. Neither personal meetings, nor names, nor binding to the specific place. To predict or monitor terrorist attack preparations impracticably.

Rapid growth of quantity of the crimes committed in a cyberspace in proportion to number of users of computer networks (by estimates of the Interpol, growth rates of crime on the wide area network the Internet, are the most bystry on the planet). It once again emphasizes a danger status from information and cyber terrorism.

Information terrorism – merge of physical abuse and criminal use of information systems, and also intended abuse of digital information systems, networks or their components, for the purpose of the help of implementation of terrorist transactions or actions [2, P. 101].

Modern information terrorism is characterized as a set of the information wars and special operations connected with national or transnational criminal structures and intelligence agencies of foreign states. Availability of information technologies considerably increases risks of information terrorism [3, P. 56].

Information terrorism shares on:

1) information and psychological terrorism (control over media for the purpose of distribution of misinformation, rumors, demonstration of power of the terrorist organizations):

a) media terrorism or «media killer» " abuse of information systems, networks and their components for implementation of terrorist actions and shares;

2) information and technical terrorism (causing damage to separate elements and to all to the information circle of the opponent in general: destruction of element base, active suppression of communication lines, artificial resets of nodes of communication, etc.):

a) cyber terrorism – set of the actions including the information attack to computer information, computing systems, the data transmission equipment, other components of information infrastructure which is performed by criminal groups or individuals [4, P. 231].

In case of media terrorism it is told about a kind of information terrorism, is abuse of information systems, networks and their components for implementation of terrorist actions and shares. Media terrorism policy tools printed media, networks of radio and cable mass media, Internet, e-mail, spam to that similar.

Media terrorism represents the special type of terrorist activities allocated by criterion of use of tools (means) of achievement of the purposes by terrorists. K.S. Gerasimenko claims that his essence consists in attempts by the organization of special media campaigns to destabilize society, to create in it the atmosphere of civil disobedience, mistrust of society to actions and intentions of the power and especially – its law enforcement agencies designed to protect public order [5].

Media and the Internet reckon that in correlative interrelations create information resource which is capable to hide the reliable, exact and complete information behind abstract reality with instruments of media terrorism as the most effective. A striking example of use by terrorists of media and the Internet is the manipulation public opinion, distribution misinforming influences on society, discredit of official organs of public administration for the purpose of psychological combing of society and distribution of one-vector information, as a result creates ideology acceptable for terrorists.

According to specialists of counterintelligence services, «terrorists» by e-mail transfer in encrypted form of the instruction, card, scheme, passwords and other important information which disclosure can cause damage to a homeland security of the state [5].

And under the influence of media terrorism the individual isn't capable to be guided independently in unrestricted information space of available data as by media it is presented in the form of tools for designing of doubtful reality today. A task of this reality is not reproduction and distribution of reliable information, but conquest of the personality judgment unusual for it. Thus, today it is impossible to speak about transition of amount of information in its quality. Especially it concerns media and the Internet as they act as object of political impact, which purpose to distort the real situation.

So, it is possible to state that the threat of media terrorism and cyber terrorism is rather complex and urgent problem now, and it will become complicated in process of development and distribution of information technologies [6, S. 15].

Now computer crime of Ukraine is at the level of the USA the beginnings of the 80th years. But rates and development can't but guard. Estimating cyber terrorism threat, it is necessary to consider some features of our country. It is, first, the high potential and professional level of programmers which services even such leaders of the program industry as Microsoft willingly use. Secondly, a

youth capability quickly to master technical innovations of which still yesterday they had no idea. Considering the fact that the computer facilities constantly become cheaper, it is possible to expect that also the number of Internet users will grow in our country. Thirdly, though still weak, but already noticeable economic recovery without fail will cause growth of a computerization and on one-two steps will bring closer us to the countries with the developed infrastructure, will make threat of cyber terrorism quite real.

Summing up, it is necessary to tell that the problem of counteraction to acts of information terrorism is a complex problem. Today problem of counteraction to acts of information terrorism. Therefore the main task for Ukraine – purposeful work on harmonization and enhancement of the legislation in the sphere of information security of the state. Implementation of effective information policy and informing citizens through media (a capability to resist to attempts of manipulation by means of information flows) about the terrorism reasons, negative its influence and trust to the state which will help to construct system on protection of each person [7, . 308].

As the recommendations submitted on counteraction to dangerous tendencies and increase in efficiency of fight against media terrorism and cyber terrorism we offer the following directions of enhancement: 1) the organization of an effective cooperation with foreign states, their law enforcement agencies and special services, and also the international organizations which task includes fight against cyber terrorism and transnational computer crime; 2) creation of the international contact point on assistance in case of response to transnational computer incidents; 3) expansion of a cross-border cooperation in the sphere of a legal assistance in fight against computer crime media terrorism and cyber terrorism; 4) to create programs for overcoming problems of cyber terrorism for forecasting and modeling of crisis situations and development of optimum responses to «cyber attacks»; 5) to create special structures on tracking and neutralization of the hidden cyber threats with involvement to it of specialists of high level; 6) development of reliable system of protection of the vital government institutions with the maximum isolation of the people responsible for separate links of protection; 7) adoption of laws on electronic safety according to the existing international standards and the Convention of the Council of Europe on fight against cybercrime; 8) to add the Criminal code of Ukraine with concepts of all types of information terrorism and to establish specific measures of responsibility for them.

THE LIST OF REFERENCES

1. Травников Ю. Преступления в Паутине: Границы без замков [Электронный ресурс] / Ю. Травников. – Режим доступа: http://www.pl-computers.ru/article.cfm?Id=742&Page=3.

2. 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.

3. Яцик Т. П. Особливості інформаційного тероризму як одного із способів інформаційної війни / Т. П. Яцик // Науковий вісник Національного університету ДПС України (економіка, право). – 2014. – № 2 (65) – С. 55–60.

4. Бойченко О. В. Медіа-тероризм: особливості сучасних ознак інформаційній безпеці / О. В. Бойченко // Друга міжнародна наук.-практ. конф. [«Інтегровані інтелектуальні робототехнічні комплекси (ПРТК-2009)»], (25–28 травня 2009 р.). – К.: НАУ, 2009. – С. 230–232.

5. Герасименко К. С. Сучасні ознаки загроз «інформаційного тероризму» [Електронний ресурс] / К. С. Герасименко // Форум права. – 2009. – № 3. – С. 162–166. – Режим доступу : file:///C:/Users/User/Downloads/FP_index.htm_ 2009_3_26%20(12).pdf.

6. Катренко А. Особливості інформаційної безпеки за міжнародними стандартами / А. Катренко // Альманах економічної безпеки. – 1999. – № 2. – С. 15–17.

7. Yatsyk T. P. Information terrorism as threat of national and international safety / T. P. Yatsyk, Z. A. Gasimov // 2-nd International Academic Congress «Fundamental and Applied Studies in America, Europe, Asia and Africa». – New York, USA. – 27 September 2014. – P. 306–309.