УДК 351.861

J. Sabol, Assoc. Prof., DSc and B. Šesták, Prof., DSc

IMPACT OF TERRORIST CBRN ATTACKS ON THE NATIONAL CRITICAL INFRASTRUCTURE

The use of CBRN substances, agents or material, or weapons which make use of these components, is associated not only with affected persons and the contaminated environment but also with the disruption of some chains and systems of vitally important critical infrastructure. The paper discusses some specific aspects related to possible impacts of CBRN terrorist attacks with special emphasis on the consequences of a radiological dispersive device based on deliberate contamination using high-activity radioactive substances. Further, preventive measures against radiological attacks as well as the response to such acts aimed at the minimization of their impact on health of people and disruption of normal functions of national infrastructure are also outlined. In addition, some initiatives of the EU in fighting international CBRN terrorism are briefly discussed.

Ключові слова: CBRN, radiological terrorism, critical infrastructure, EU, risk mitigation

Дж. Сабол, Доц. Проф., Доктор наук, Б. Шестак, Проф., Доктор наук.

ВПЛИВ ТЕРОРИСТИЧНИХ РХБ АТАК НА НАЦІОНАЛЬНУ КРИТИЧНУ ІНФРАСТРУКТУРУ

Використання РХБ речовин або матеріалів, або зброї з використанням цих компонентів, пов'язано не тільки з зацікавленими сторонами та забрудненням навколишнього середовища, а також з порушенням деяких ланцюгів і систем життєво важливої критичної інфраструктури. У роботі розглянуті деякі конкретні аспекти, пов'язані з можливими наслідками РХБ терактів з особливим акцентом на наслідки радіологічного дисперсійного пристрою на основі навмисного зараження з використанням високорадіоактивних речовин. Крім того, в роботі викладено профілактичні заходи проти радіологічних атак, а також відповідь на такі дії, спрямовані на мінімізацію їх впливу на здоров'я людей і порушення нормальних функцій національної інфраструктури. Також, коротко обговорюються деякі ініціативи ЄС у боротьбі з міжнародним РХБ-тероризмом.

Keywords: РХБ зброя, радіологічний тероризм, критична інфраструктура, ЄС, зниження ризиків

The protection of individual vital sectors of critical infrastructures as well as associated critical activities is now commonly acknowledged as an acute security challenge for many countries and their population. The broad range of CBRN (Chemical, Biological, Radiological and Nuclear) hazards, from man-made, natural, accidental to deliberate, and the wide spectrum of risks, from small disturbances to high damage such as significant contamination with extreme consequences, makes the CBRN threat both insidious and penalizing for the operators in charge of those critical infrastructures.

Many dangerous CBRN components are extensively used in a number of various peaceful applications especially in industry, medicine and science, and can potentially be misused also for terrorist or other malevolent actions. This is why all CBRN materials, which could potentially be used for constructing CBRN weapons, should be strictly kept under appropriate regulatory control. Moreover, there have been developed special CBRN substances for military purpose. Although the access of terrorists to these materials is more difficult, in some countries where there is not sufficient control of dangerous goods, such materials may find their way to terrorists who may use them for attacking large gathering of people and also critical infrastructure.

Therefore, it is important to study the effects of, as well as the preparedness for, a CBRN threat against critical infrastructure. This includes many aspects of CBRN impact, vulnerabilities, response plans and programmes, supporting communications, and the economics involved in preparing for a possible CBRN event. The risk may also involve the sabotage of facilities where CBRN materials are used for peaceful applications, including industrial, medical and research installations.

The national critical infrastructure provides the essential services to the population and the society at large. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the national safety, prosperity, and well-being [1].

The critical infrastructure presents a diverse and complex system which includes distributed networks, varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both the physical space and cyberspace, and governance constructs that involve multi-level authorities, responsibilities, and regulations. Critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient.

Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards including CBRN attacks or sabotage. In order to achieve these objectives, this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery. Important elements of any national system aimed at coping with such emergency situations include the appropriate legislation, competent regulatory authority, support technical services and capabilities for training of professionals in the field.

The critical infrastructure in most developed countries includes the following main sectors (Fig. 1):

• Energy sector – it fuels the economy of the 21st century. Without a stable energy supply, health and welfare are threatened, and the national economy cannot function.

• Healthcare and public health sector protects all sectors of the economy from hazards such as terrorism, infectious disease outbreaks, and natural disasters. This sector is highly dependent on fellow sectors for continuity of operations and service delivery, including: communications, emergency services, energy, food and agriculture, information technology, transportation systems, and water and wastewater systems.

• Chemical sector - an integral component of the economy, relying on and supporting a wide range of other critical infrastructure sectors. The sector can be divided into five main segments, based on the end product produced: basic chemicals, specialty chemicals, agricultural chemicals, pharmaceuticals, and consumer products.

- *Transportation sector* – its main function is to ensure quick, safe, and secure move of people and goods through the country and abroad. The sector consists of several key subsectors, namely aviation (aircraft, air traffic control systems, and airports), roads, highways (including bridges and tunnels) and vehicles), maritime transportation (coastline, ports, waterways), mass transit and passenger rail (buses, rail transit, metros, trams and other vehicles for the transport of people and goods), pipeline systems (transport of oil, gas, various other chemicals), freight rail (railroads, freight cars, locomotives), postal and shipping.
- *Food and agriculture sector* - composed of farms, restaurants, and licensed food manufacturing, processing, transporting and storage facilities.
- *Water and wastewater systems sector* - includes public drinking water systems and wastewater treatment systems. The sector is vulnerable to a variety of attacks, including contamination with deadly agents, physical attacks such as the release of toxic gaseous chemicals. If these attacks were realized, the result could be large numbers of illnesses or casualties and/or a denial of service that would also impact public health and economic vitality. Critical services such as firefighting and healthcare (hospitals), and other dependent

and interdependent sectors, such as energy, food and agriculture, and transportation systems, would also be severely affected due to a denial of service in this sector.

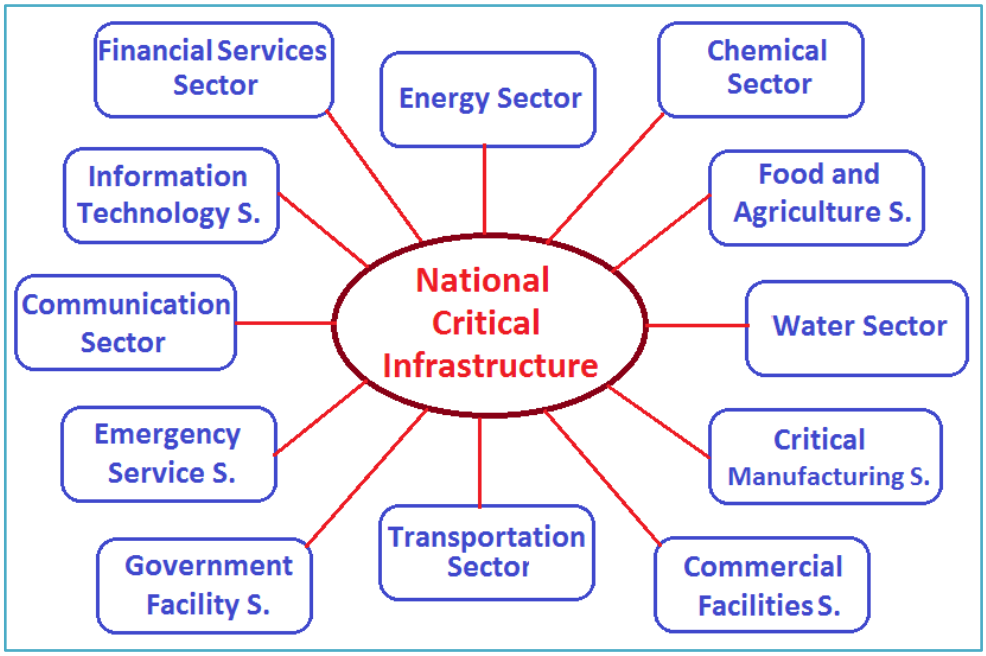

Figure 1. National critical infrastructure main component (in countries operating NPPs, research nuclear reactors or nuclear waste facilities, this has also to be included).

- *Emergency services sector* - includes a system of prevention, preparedness, response, and recovery elements, and represents the nation's first line of defence in the prevention and mitigation of risk from both intentional and unintentional manmade incidents/accidents and natural disasters. The sector also serves as the primary protector for the other critical infrastructure sectors.
- *Communication sector* - an integral component of any economy, underlying the operations of all businesses, public safety organizations, and government. It provides an "enabling function" across all critical infrastructure sectors. The transmission of these services has become interconnected; satellite, wireless, and wireline providers depend on each other to carry and terminate their traffic and companies routinely share facilities and technology to ensure interoperability.
- *Information technology sector* – represents a main element of the nation's security, economy, and public health and safety. Businesses, governments, academia, and private citizens are increasingly dependent upon this sector functions. These virtual and distributed functions produce and provide hardware, software, and information technology systems and services, and - in collaboration with the Communications Sector - the Internet.
- *Financial services sector* – constitutes a vital component of any nation's critical infrastructure. Large-scale power outages, recent natural disasters, and an increase in the number and sophistication of cyber-attacks demonstrate the wide range of potential risks facing the sector. Financial institutions provide a broad array of products from the largest institutions to the smallest community banks and credit unions. Whether an individual savings account, financial derivatives, credit extended to a large organization, or investments made to a foreign country, these products allow customers to: deposit funds and make payments to other parties; provide credit and liquidity to customers; invest funds for both long and short periods; and transfer financial risks between customers.
- *Government facilities sector* - includes a wide variety of buildings, located in the country and overseas. Many government facilities are open to the public for business activities,

commercial transactions, or recreational activities while others that are not open to the public contain highly sensitive information, materials, processes, and equipment. These facilities include general-use office buildings and special-use military installations, embassies, courthouses, national laboratories, and structures that may house critical equipment, systems, networks, and functions.

- *Critical manufacturing sector* – a crucial sector to the economic prosperity and continuity of any advanced country. A direct attack on or disruption of certain elements of the manufacturing industry could disrupt essential functions at the national level and across multiple critical infrastructure sectors. The sector identifies the following industries to serve as the core of the sector: primary metal manufacturing ; machinery manufacturing; electrical equipment; appliances and component manufacturing; and transportation equipment manufacturing.
- *Commercial facilities sector* - operates on the principle of open public access, meaning that the general public can move freely throughout these facilities without the deterrent of highly visible security barriers. It include a number of facilities such as public assembly (arenas, stadiums, aquariums, zoos, museums, convention centres), gaming (casinos), lodging (hotels, motels, conference centres), outdoor events (amusement parks, fairs, campgrounds, parades), entertainment and media, real estate (office and apartment buildings, condominiums, mixed use facilities), retail (retail centres and districts, shopping malls).
- *Nuclear reactors, materials and waste sector* - accounts in the Czech Republic for more than 30 percent of nation's electrical generation, provided by two nuclear power plants. The sector may also include non-power nuclear reactors used for research, testing, and training; manufacturers of nuclear reactors or components; radioactive materials used primarily in medical, industrial, and academic settings, nuclear fuel cycle facilities; decommissioned nuclear power reactors; and transportation, storage, and disposal of nuclear and radioactive waste.

CBRN-threats are defined as the protection against the impact of chemical (C), biological (B) as well as radiological (R) and nuclear (N) threats. Each of these components has some specific characteristic as to the time to effects, potential impacts and availability (Fig. 2).

AGENTS	SUMMARY CHARACTERISTICS		
	Time To Effects	Potential Impact	Availability
BIOLOGICAL	Days to Weeks	Local to Global	Low
RADIOLOGICAL	Minutes to Hours	City to Region	Medium
CHEMICAL	Seconds to Hours	City Blocks	High

Figure 2 – Illustration of some differences between some individual components of CBRN weapons.

Terrorists have considered a wide range of toxic *chemicals* for attacks. Typical plots focus on poisoning foods or spreading the agent on surfaces to poison via skin contact, but some also include broader dissemination techniques. Dangerous chemical include such substances as cyanides,

mustard agents, nerve agents, toxic industrial chemical as well as specifically developed toxic substance for military purpose [2,3].

For historical reasons, the term "*biological agents*" combines infectious pathogens (bacteria, viruses) and poisons of natural origin (toxins), so that questions of microbiology, infection prevention and toxicology are all involved here. This area deals with the medical aspects of biological protection, meaning protection against biological hazards. Such tasks require expertise providing supports and the development of suitable concepts and recommendations.

Radioactive contamination can occur for instance after accidents in nuclear power plants, accidents in research laboratories or through so-called "dirty bombs" (use of radioactive material for criminal purposes). Nuclear hazards can be brought about by the use of atomic weapons. Following acute ionizing radiation exposure to the human organism, specific symptoms may occur, which are referred to as radiation sickness. Depending on the dose and nature of the radiation, the acute symptoms and their progression can vary. They range from influenza-like symptoms (with or without fever), sickness, vomiting, diarrhoea, lack of appetite and loss of fluid, through to cramps, apathy, paralysis, neurogenic shock, coma and death. The long-term consequences may include cancer and genetic damage. They may occur with the probability proportional to the dose.

Nuclear materials can be used to construct an atomic (nuclear) or thermonuclear bomb which has the most devastating consequences including exposure to ionizing radiation and radioactive contamination of vast territory. For the time being, it is not probable that terrorist could acquire this weapon of mass destruction.

Various CBRN weapons show also different level of probability of the risk which is associated with their potential use for terrorist attacks. In the case of radiological weapons, this risk probability is shown in Fig. 3 (based on [4]).

Probability / Severity	Frequent	Likely	Occasional	Seldom	Unlikely
Catastrophic	Extremely High	Extremely High	High	High	Moderate
Critical	Extremely High	High	High	Moderate	Low
Marginal	High	Moderate	Moderate	Low	Low
Negligible	Moderate	Low	Low	Low	Low

Figure 3 – Level of radiological risk.

In the case of *chemical threats* victims should be evacuated from the danger zone immediately, inhalation of the poison must be avoided, for instance as a result of evaporation from clothing. Since some substances can also enter the body via the skin, quickly removing the contaminated clothing is one of the most important initial self-help measures. Decontamination (as a rule extensive showering) can then take place. If a large number of contaminated individuals are also injured, the personnel of the fire services and rescue services must provide help. This may indicate safeguarding the vital factors (consciousness, respiration, and circulation), symptomatic treatment and where appropriate administration of antidotes (medicines which alleviate or cancel out the effect of the poison). Rescuers must wear chemical protection suits, and where appropriate a self-contained breathing apparatus. A large number of people could be injured and contaminated in the event of a release of dangerous chemicals, for instance as the result of a terror scenario or of an accident in a chemical plant. In order to deal with such an incident, extensive medical measures and

appropriate knowledge of the chemical and toxicological properties of the released substances, taking account of medical and occupational health aspects, are necessary. Some examples how to ensure the protection against chemical dangerous substances is shown in Fig. 4.

Figure 4 – Measures to be taken in case of a chemical attack or sever accident.

As to response to *biological agents*, depending on the causes, specific medical measures with epidemic emergency management (for example sequestration) as well as targeted therapy (for example administration of antibiotics) ranging to preventive measures (for example vaccination) are to be implemented. Development of so-called resistance (resistant bacteria strains) against drugs however presents a concern, and leads more and more frequently to antibiotics no longer being effective.

The use of a radiological weapon may result in the exposure to *ionizing radiation* of persons affected by external penetrating radiation and internal contamination. The most important life-saving measure for victims is to remove them from the hazard zone as quickly as possible in order to put the greatest possible distance between them and the source of the radiation. In order to avoid damage to the body through radioactive material affixed to the skin, the victim must be decontaminated. Specific medical measures can accelerate the elimination of accumulated radioactive substances from the body, or they can be prevented from being deposited in the body.

There have been proposed a number of recommendations aimed at the protection of critical infrastructure against the CBRN threats including:

- Timely, accurate information is critical to life saving efforts as well as to manage fear;
- Advanced, automated surveillance and detection devices for indoor and outdoor use must be put in place;
- Systems must be able to assess and prioritize threats and vulnerabilities;
- Communications operability and interoperability must be continuously improved; and
- Systems must also prevent disruption, mitigate results and build in resiliency.

For protection against CBRN threats, it is important to use relevant means of monitoring the presence of even minor amount or concentrations of chemical and biological agents as well as radiation levels and radioactivity in the air and on surfaces of soil and the structures of buildings. The present monitors developed for this purpose can be characterized as follows:

- *Chemical monitors* should rapidly detect pre-defined chemical contaminants present as vapours with response times from seconds to less than one minute. As new chemical threats are identified, they may be added to the library. Such systems are usually based on direct sampling mass spectrometry, and as a result, are not as susceptible to false alarms as traditional monitoring systems.

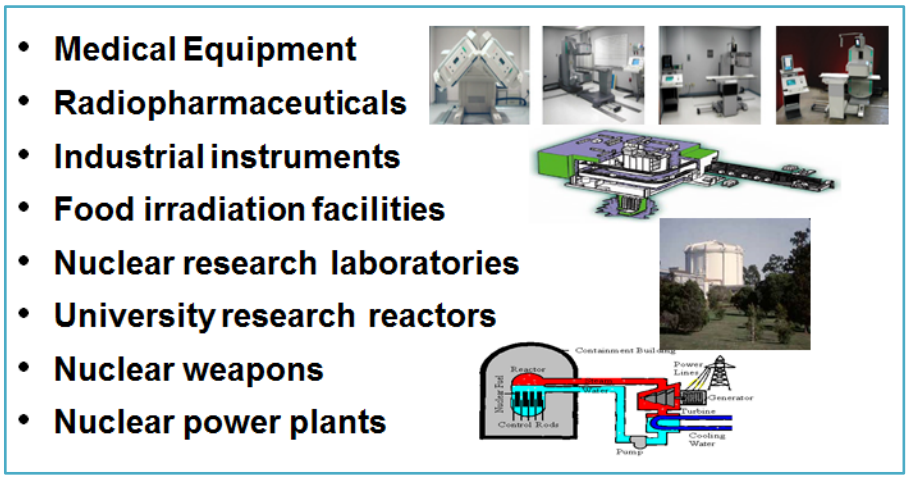

Figure 5 – Applications where high-activity radioactive sources or materials are used.

- *Biological monitors* are preferably to be designed as biological “smoke alarms” for near-real time detection, which implement threat algorithms based on a combination of particle counting, sizing and fluorescence. Both systems support a tiered detection architecture: once a bio-aerosol threat is detected, the aerosol sampler is triggered. The monitor collects samples which allow multiple assays to be performed. These samples can then be directly transferred on-site to a pathogen identification system.
- *Radiation monitors* can ensure radionuclide detection and identification in order to obtain reliable information about the nature and movement of radioactive materials. Stride systems can be openly or covertly installed in any high traffic area or portals as well as along parcel or freight conveyor systems. Within just a few seconds, a detection unit will classify the type of material detected (medical, industrial, naturally occurring or special nuclear material). In addition, the system will also categorize it as innocent, suspicious or threatening and identify the specific isotope detected.

In the case of radiation hazards, one has to consider two components: exposure due to the external radiation and exposure due to the internal contamination by radioactive substances entering the human body via ingestion or inhalation. Some basic protection methods against the exposure of external radiation are presented in Fig. 6.

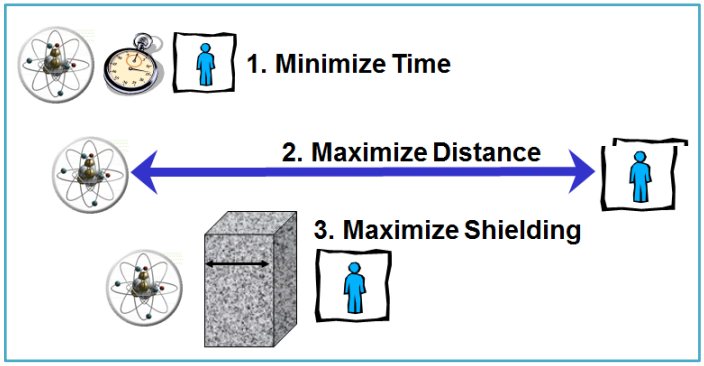

Figure 6 – Main protection measures to minimize the exposure due to external penetrating radiation.

For protecting any critical infrastructure sectors, the threat and vulnerability assessment of the structure is of paramount importance. The process of securing a building begins with a risk-based threat and vulnerability assessment. This is based on the facility design information,

threat modelling and/or *in situ* test aerosol dispersion capabilities. The analysis results enable to identify how best to apply the available resources to produce to highest level of protection possible for a specific building or structure. The approach has to include all stakeholders in order to create an integrated system, aimed at maximizing the value of the networked threat detection technologies, existing building operations, security and personnel resources.

Critical to the mitigation of an airborne agent is the control of the building automation system. By active control of the building's ventilation and access control systems, it is possible to significantly reduce the spread of the agent and limit exposures to the aerosol or vapour threat. Special systems can be installed in both indoor and outdoor environments. Through a layered approach and careful tailoring of the design for the facility, the system can provide early warning of potential CBRN threats, confirm their presence and identify specific agents.

The CBRN-substances can enter the environment in two ways: this is either caused by deliberate acts, or due to an accident, for example, during transport, or thus become a danger to the population. As the impact on those affected is concerned, it is of no real importance which of the reasons is responsible for the release of hazardous CBRN-substances.

In order to be protected against CBRN threats after the release of a dangerous substance, three aspects are of vital importance:

- Protection of people in the danger zone by means of appropriate measures, for example protective clothing, rules of conduct
- Quick detection and identification of the specific danger;
- Counteractions if exposed to a hazardous substance, for example decontamination, rules of conduct; and
- As these three aspects are concerned, relevant national specialized authorities and technical support organizations provide professional and scientific advice as well as technical support.

The European Union (EU) CBRN Centres of Excellence (CoE) Initiative was launched in May 2010 in response to the need to strengthen the institutional capacity of countries outside Europe to mitigate CBRN risks, including criminal activities (e.g. CBRN proliferation or terrorism), natural disasters and accidental disasters (e.g. Bhopal or Fukushima) [6]. The objective of the CoE Initiative is to develop a structural, all-hazards CBRN policy at the national, regional and international levels to anticipate and respond to these risks, and to reduce the vulnerability of countries to CBRN events. In this respect, the initiative is in the reciprocal interests of regional and EU security.

The EU CBRN CoE programme is supported by EU Member States and presents an innovative and broad-ranging approach, in alignment with European security objectives, aiming to help partner countries build institutional capacities and implement a coherent and coordinated strategy for CBRN risk mitigation. It has been welcomed at the international level and represents an opportunity to show the visibility of the EU actions [5,6].

The set-up of Regional Secretariats in different geographical areas (Fig. 7) and the designation of NFPs in partner countries has helped create a flexible structure that should guarantee ownership and sustainability of the initiative. Altogether eight Regional Secretariats have already been established covering most of the regions.

Figure 7 – The EU CBRN Centres of Excellence in individual regions: Tashkent – Central Asia (Kyrgyzstan, Tajikistan, Uzbekistan), Manila – South-East Asia (Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, Vietnam), Tbilisi - South-East Europe, southern Caucasus, Moldova and Ukraine (Albania, Armenia, Bosnia and Herzegovina, Former Yugoslav Republic of Macedonia, Georgia, Moldova, Montenegro, Serbia, Ukraine), Amman – Middle East (Iraq, Jordan, Lebanon), Nairobi – Eastern and Central Africa (Burundi, Democratic Republic of Congo, Ghana, Kenya, Rwanda, Seychelles, Uganda, Zambia), Rabat – African Atlantic Façade (Côte d'Ivoire, Gabon, Liberia, Mauritania, Morocco, Senegal, Togo), Algiers – North Africa (Algeria, Libya, Morocco, Tunisia) [6].

However, some general aspects of the EU CBRN CoE initiative need to be carefully addressed, including setting clear geographic and thematic priorities; carrying out systematic, comprehensive and accurate needs assessments at the country level; assuring a greater involvement of member states in the different phases of project definition and implementation; and establishing a verification regime to monitor performance and long-term impact of the projects on CBRN risk mitigation.

Finally, the accomplishments of the CoEs should be communicated to a wider public, highlighting the EU's contribution to security and development. In this respect, EU Member States' support for the initiative and the appreciation demonstrated by international organizations and other interested stakeholders should help ensure the continuity of the actions currently being undertaken by the EU to control the proliferation of CBRN materials.

Conclusion

The threats of the potential use of such dangerous materials like CBRN are considered to be present a real risk which should be eliminated or minimize to the lowest possible level. The weapons based on CBRN materials can affect not only people and the environment but also disrupt important systems of national critical infrastructure. This is why every effort should be made to prevent any use CBRN weapons or materials for terrorist or other malevolent actions. The EU initiated several programmes aimed at the reduction of the CBRN threat not only in Europe but also in other regions worldwide where EU CBRN Centres of Excellence have been established in order to assist third countries to introduce relevant and efficient preventive measures to fight international terrorism. These measures are aimed especially at introducing strict control of these materials including their illicit trafficking and to adopt appropriate legislative tools for this purpose.

СПИСОК ЛІТЕРАТУРИ

1. Critical Infrastructure Security, Homeland Security. On line (10 April 2015): http://www.dhs.gov/topic/critical-infrastructure-security.
2. Mika, O., Polívka, V., Sabol, J.: Weapons of mass destruction and the protection against them, Textbook, Police Academy of the Czech Republic in Prague, Prague, 2009.
3. Sabol, J., Šesták, B., Polívka, L.: Current Activities of the European Union in Fighting CBRN Terrorism Worldwide, NATO Advanced Research Workshop "Preparedness for Nuclear and Radiological Threats", Los Angeles, 18-20 Nov. 2014 (invited paper).
4. Joint Publication 3-11: Operations in chemical, biological, radiological, and nuclear environments, Joint Chief of Staff US DoAF, 2013.
5. Mignone, A.: The European Union's Chemical, Biological, Radiological and Nuclear Centres of Excellence Initiative. EU Non-Proliferation Consortium, Non-Proliferation Papers, No. 28, June 2013.
6. Can the EU's Centres of Excellence initiative contribute effectively to mitigating chemical, biological, radiological and nuclear risks from outside the EU?, European Court of auditors, Luxembourg, 2014.

❖ ❖ ❖