


Abramova N.A., Makarenko D.I.

SYSTEMATIZATION OF CRITERIA AND SIGNIFICANT FACTORS FOR EVALUATION OF EXPOSURE OF COMPLEX SYSTEMS TO DISTURBANCES

The paper presents the analysis of domestic and foreign scientific, methodology and normative documents on methods and criteria for identification of critical subsystems and nodes of important economic objects and research in their behavior in abnormal situations. The authors of the paper have studied approaches to evaluation of exposure of various facilities to anthropogenic disturbances and systemized criteria and factors significant for evaluation of impacts of disturbances and step-by-step action factors.

Keywords: *important economic object, vulnerability, disturbance, threat of terrorist attack, protection object, criteria.*

Introduction

To identify nodes of important economic objects (IEO) most susceptible to disturbing influences (DI) is very important in the modern world for various disturbing influences with different objectives, IEO types and task statement types. As IEO, we can have a big city with all its infrastructure facilities, or a single airport with its subsystems, or even a specific territory (region, country), where we consider an aggregate of IEOs as potential objects for DI.

The target of DI exposure analysis is to identify the weakest spots of a given IEO (or territory) to take some operative measures under the conditions of a DI increased threat or to correct the strategy of objects protection and to select priorities for investments[1].

The task of DI exposure of individual objects can be considered as part of a more general task of comparative evaluation of objects, nodes, subsystems within a larger IEO or territory for further categorization or identification of objects mostly exposed to DI, or as a separate task (for example, in case of certification, licensing).

For solving tasks related to evaluation of DI factors and protection against then, types of threats and related DI play a significant role. Usually, natural and anthropogenic threats are identified in this case [1, 2]: the latter are first of all characterized by the fact that they arise due to human activities. Anthropogenic threats are in their turn differentiated as technology-related threats and terrorism.

[1] Some typical tasks of such kind are considered in [1].

While technology-related DI associated with such activity as manufacture, transportation, keeping and exploitation of dangerous materials can be treated (for the convenience of analysis [1]) as accidental, and their consequences can be considered as unintentional, terrorism features purposefulness of disturbing impacts – terrorist attacks, as well as consequences, in the short run and in the long run. Purposefulness can be considered as a general property of different types of terrorism independent of sources, bases, political or social targets stricken, means etc.

It is the presence of active "subjects" – organizations, informal communities, individual people, whose intentions are implemented by means of terrorist attacks (even if they are disguised as unintentional DI types) that should be decisive for choosing theoretical means – models and methods – to solve above mentioned types of tasks.

It is exposure of objects to intentional DI (terrorist attacks) that is studied in this paper.[1]

1. Approaches to evaluation of IEO exposure to disturbing influences

The analysis of domestic and foreign scientific and methodology literature and normative documents shows that there are no more or less generally accepted comprehensive approaches to types of tasks specified above and related to threats of terrorism and terrorist attacks as well as other types of DI.

Thus, a brief overview of literature in [3] that considers a number of characteristics of methods offered for evaluation of infrastructure susceptibility and resilience, and of criteria which are evaluated in such methods makes it possible to come to the following conclusion. Though proposed methodology considers one or two characteristic in more detail, they so far lack integrity and feasibility, as they don't allow including additional criteria (social, administrative, ecological and economical ones).

The insufficient sophistication of a systematic approach to evaluation of critical infrastructure is seen clearly enough in the quality of domestic normative documents. (As an example, Rules "Ensuring of objects safety" of Ministry of Communications of Russian Federation Регламент (2010) and Instruction of Ministry of Transport of Russian Federation "The procedure of evaluating exposure of transport infrastructure and transport fleet objects" (2010) have been analyzed).

Along with development of quality (informal) methods and methodology for evaluating IEO nodes and subsystems, their functional and structural analysis inclusive (for example, [4], the considerable part of methods in [1, 5]), today scientific literature offers a number of **expert and formal methods**. To a greater or lesser degree, such methods include formalized logical and mathematical methods, however their application should be (more or less explicitly) preceded by expert "elaboration" of a complex, poorly structured situation – preliminary structuring and formalizing of knowledge about objects, their structure and significance (criticality), types of threats etc. – and possibly expert estimates.

As key indices, domestic and foreign scientific and methodology literature discussing various issues related to terrorist attacks at important economic objects [3, 2, 6, 7 etc.] often uses "vulnerability", "criticality", "risk", "threat", "consequences". Less often such terms as "resilience", "reliability", "hazard" are used.

For the purpose of analysis of a **protected object's properties**, in the context of evaluation of its exposure to terrorist attacks, such terms as **vulnerability**, **criticality** are generally used.

The term "threats" are applied to characterize the properties of environment external to IEO. The term "risk", as a rule, takes into account the properties of an object itself as well as environment.

According to [5], the vulnerability of an object can be evaluated on the basis of two different but complementary approaches.

[1] In some domestic normative documents, threats of terrorist and criminal character differ, though the property of purposefulness holds for the latter as well.

The first approach is based on the assumption that any object has an **inherent vulnerability level** independent of any protection measures applied to it. For example, a football stadium has an inherent vulnerability level, as it hosts a great number of people and therefore it can be a sufficiently attracting target for terrorists in terms of the number of victims of terrorist attacks. In other words, this type of vulnerability characterizes the attractiveness of an object for terrorists in terms of getting public (intimidating people) and political (attracting the attention of international audience) resonance.

The second approach assumes that any object can be protected by means of a wide range of security measures reducing its vulnerability, i.e. increasing its protection against a terrorist attack. For example, if a ventilation system of a protected object is designed in such a way that its elements are hard to access and located in the zone of visibility of CCTV cameras, it will less likely be used by terrorists attempting to administer poisonous gas. To designate vulnerability in terms of protection of an object, the term **tactical vulnerability** is used.

To avoid misunderstanding of terms, we believe it reasonable:

1) To replace a complex term "vulnerability" adopted in [5] with "**exposure to terrorist attacks**";

2) To define vulnerability characterizing the attractiveness of an object for terrorists in terms of getting various types of resonance as "**IEO attractiveness**";

3) To define tactical vulnerability characterizing protection of an object against terrorist attacks as "**vulnerability**".

Therefore, according to [5] and terminology adopted above, IEO exposure to terrorist attacks is defined by its attractiveness for terrorists and its vulnerability (fig. 1).

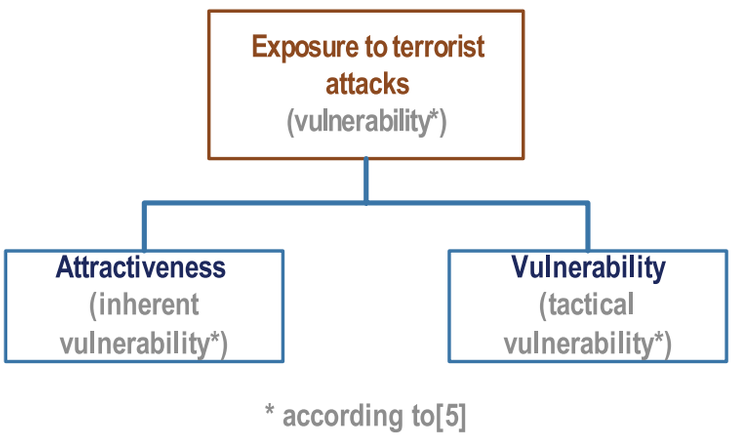

Fig. 1. Approaches to assessment of vulnerability

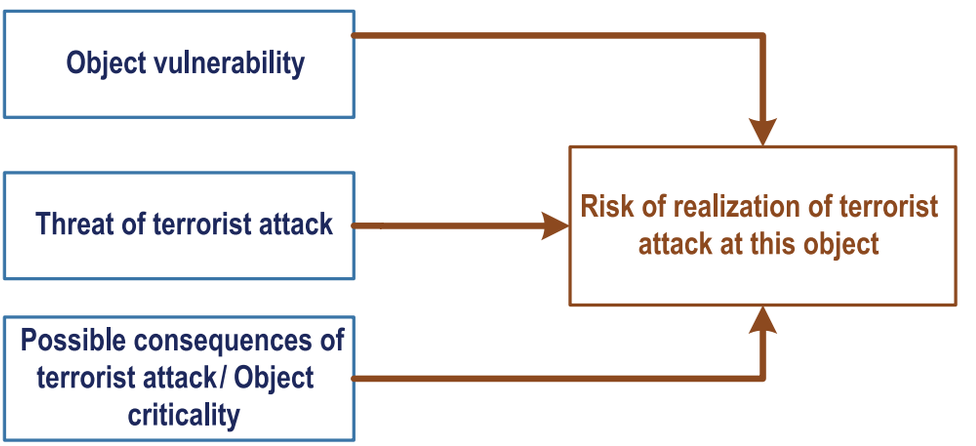

Fig. 2. Criteria taken into account for evaluation of risk of realization of terrorist attack to solve some tasks

Depending on the task to be solved, the task of evaluation of vulnerability of a protected object can be specific in relation to more general tasks, such as, for example, the task of development and correction of the strategy of risk management of a terrorist attack regarding this IEO, or the task of splitting of resources among IEOs located on the territory of a single administrative unit. In these cases the risk is considered as a function of vulnerability, threat and criticality of an object's nodes and subsystems (for the first task [1]) or consequences of terrorist attacks (for the second task [6]) (fig. 2).

Below we shall study criteria and factors defining IEO exposure to terrorist attacks and some other indices specified above, important for solving the tasks of an investigated family.

2. Criteria and factors significant for evaluation of IEO exposure to disturbing influences and their systematization

According to [5] and terminology adopted above, IEO exposure to terrorist attacks is defined by its attractiveness for terrorists and its vulnerability. IEO attractiveness for terrorists is defined by the following criteria or factors:

– openness of an object: an object can be secret and its existence can be known to a very limited circle of people;

– usefulness of an object in terms of its suitability or value for hitting their targets by terrorists;

– availability of an object for population;

– mobility: an object can be stationary or mobile;

– availability of dangerous substances and materials at an object;

– possible concurrent damage: damage for public or related objects and environment due to an attack at an object;

– population of an object: the number of people present at an object at one and the same time.

IEO vulnerability for terrorists is defined by the following factors [5] (fig. 3):

Perimeter of an object

– security aspects taken into account at the stage of planning area and landscape around an object**;**

– parking lot security: detachment of a road and parking lot from an object.

Building fencing

– capability of building fencing **to prevent DI or mitigate consequences.**

Inside space of an object

– planning and architecture of inside space: visibility of public and closed areas. Detachment of public and closed areas. Detachment of critical systems and processes;

– protection and/or availability of backup public water system and heating, ventilation and conditioning system**;**

– electrotechnical systems: availability of backup power and communications systems; functioning alarm system; sufficient illumination;

– fire protection system: sufficiency and protection of fire systems and water supplies; staff qualification; local rescue service awareness of an object's nature;

– object's security system: availability and sufficiency of CCTV equipment and security and staff.

A similar (in a substantial way) structure of criteria and factors described above is used in other sources as well [7].

It should be highlighted that an object's vulnerability is always evaluated in relation to predefined disturbing influences, or to be more precise, to predefined methods of terrorist attacks, i.e. means of destruction and ways of their application used by terrorists [2, 8]. A detailed description of terrorist methods is available in [9].

According to [9], one of the key factors that has to be taken into account when evaluating the vulnerability of objects is **redundancy, or availability of backup systems and resources that can ensure**

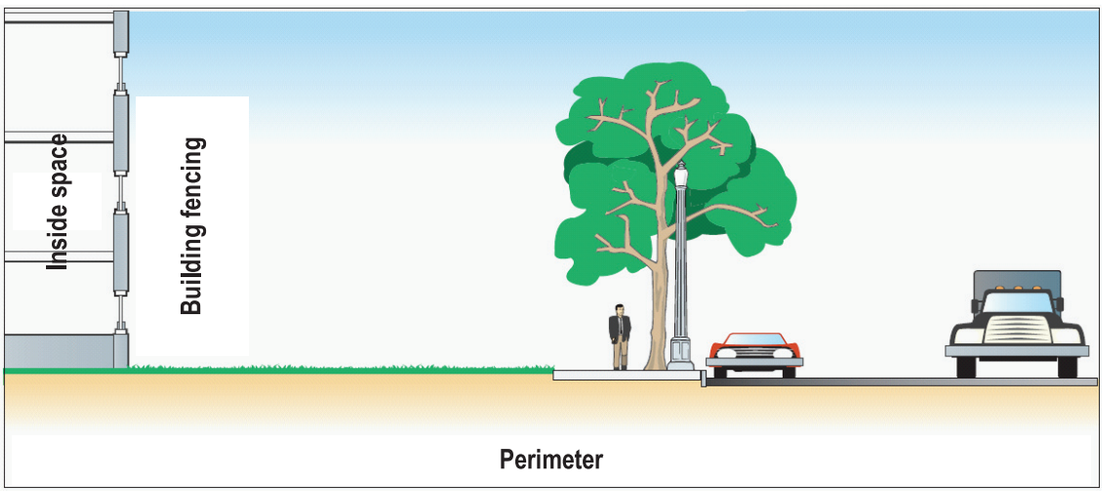

Fig. 3. Factors taken into account for evaluation of an object's vulnerability

IEO functioning in case of failure of primary systems and after a terrorist attack. IEO typical vulnerabilities related to this factor are:

– absence of redundancy;

– use of the same nodes and subsystems by primary and backup systems;

– collocation of primary and backup systems;

– absence of sufficient reserve of resources for IEO autonomous functioning immediately after a terrorist attack.

However scientifically and technically complex an object may be, no system can be purely technical as all technical processes and factors defining an object's functioning are closely intertwined with administrative, psychological, political and other human and social factors (fig. 4).

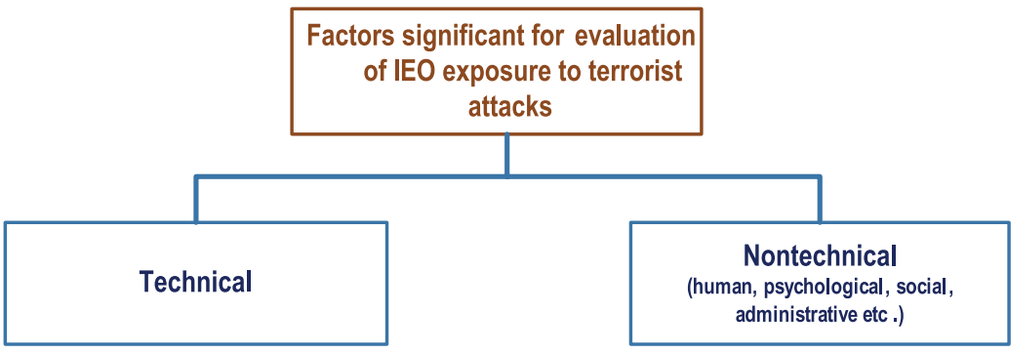

Fig. 4. Variant of classification of factors

The significance of these factors is confirmed by the results of analysis of a particular emergency – the accident happened at the drilling rig in the North Sea, made in [10]. The authors made a conclusion that 80% of equipment failures were due to nontechnical factors (human, psychological, social, administrative ones).

The high importance of these factors was also confirmed by a terrorist attack at the Domodedovo airport in January 2011. In opinions of recognized experts, one of the causes that terrorist managed to bring an explosive device into the airport building is the absence of "any teamwork on the part of several bodies in charge of transport security" [11].

Human and social factors can be identified as follows:

– level of staff qualification;

– staff reliability (motivation);

– coordination of activities of different bodies in charge of security;
– efficiency of protection measures etc.

Depending on the task in question and the type and level of a protected object, the structure and composition of criteria applied to evaluate its exposure to DI will change. When evaluating exposure to DI for objects of different levels, the same factors and criteria can be taken into account for evaluating the properties if IEO itself, i.e. IEO exposure to terrorist attacks, as well as its environment, i.e. topicality of a terrorist threat.

Thus, for example, if there is a task of evaluating exposure of different country regions to terrorist attacks, then one should consider geographical factors and those that influence a terrorist threat and typical for each specified territory, for example, such factors as:

– accessibility of a region for terrorists, i.e. its remoteness from sources of terrorism and terroristic bases;
– accessibility for making a terrorist attack or availability of allies – those are present in a greater number on a territory with a higher crime rate [7].

At the same time these factors will characterize the properties of the environment if an evaluated object is IEO located on this territory. The task of identification and structuring of criteria and factors significant for evaluation of a terrorist threat requires a more profound study and is not the objective of this paper, however we think it reasonable to mention some groups of factors characterizing a terrorist threat and found in sources considered in this paper.

In [12] threats as to the time of action are divided into two types – threats of permanent action and of temporary action.

According to [1], factors characterizing the level of a terrorist threat can belong to presence of a threat (causes, reasons for terroristic activities), possibility to commit a terrorist attack, activity of terrorists (availability of cases of committing terrorist attacks), expressed intentions to commit a terrorist attack, identified target of terrorist activities.

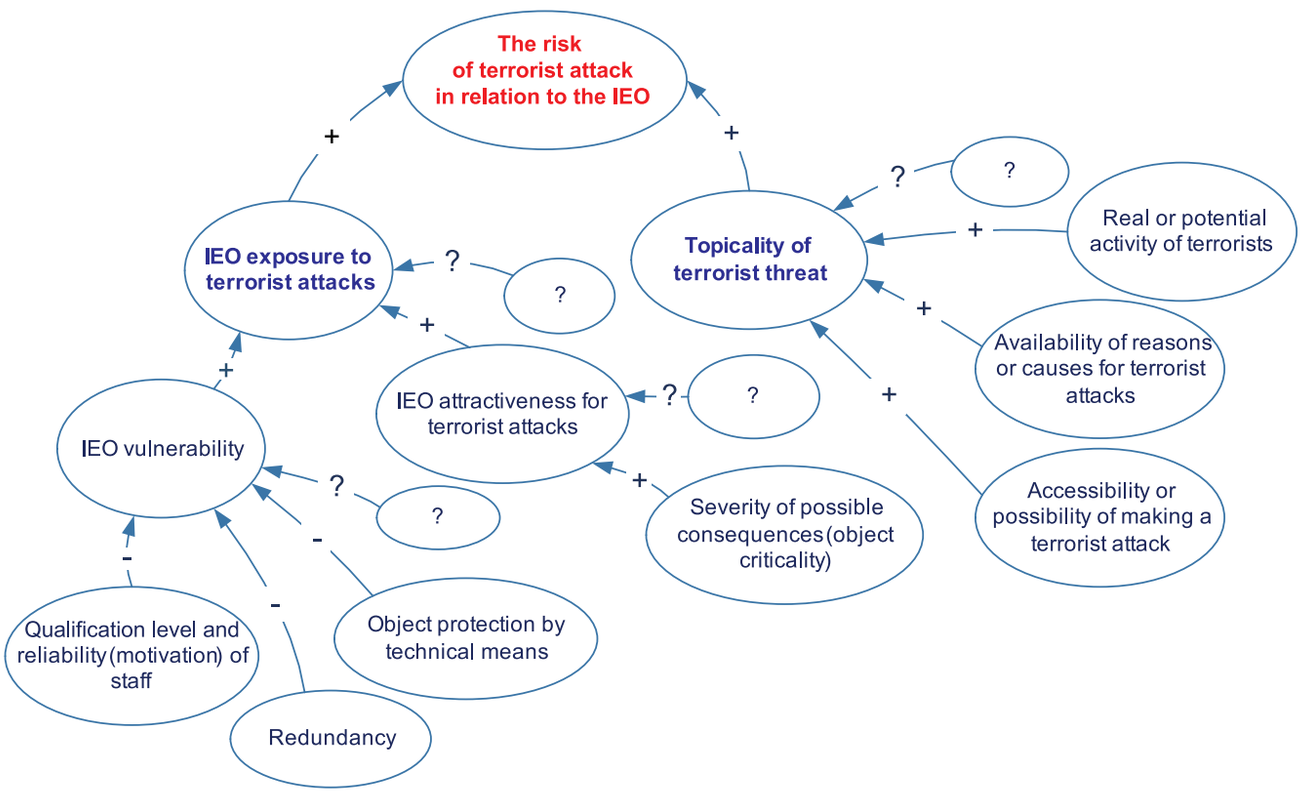

Fig. 5. Example of a cognitive map of factors and criteria significant for IEO exposure to terrorist attacks

The structure of criteria and factors determining IEO exposure to terrorist attacks is conveniently represented and analyzed in the form of a cognitive map. The example of such cognitive map for a hypothetical IEO is presented in fig. 5.

Conclusion

Therefore, the analysis of domestic and foreign scientific and methodology literature related to evaluation of IEO exposure to terrorist attacks allows us to state the following conclusions:

1. The evaluation of IEO exposure to terrorist attacks is reasonable to be made in a complex way, with the following indices taken into account:

– IEO attractiveness for terrorist in terms of getting public (intimidating population) and political (drawing the attention of international audience) resonance as well as possible economical consequences;

– IEO vulnerability, i.e. protection of an object against a terrorist attack.

2. To increase the reliability of results of evaluation of IEO exposure in relation to terrorist attacks, it is necessary to consider administrative, social, psychological and other human factors, along with traditionally considered – technical – ones.

3. Depending on the task in question and the type and level of a protected object, the structure and composition of criteria applied to evaluate its exposure to DI will change. When evaluating exposure to DI for objects of different levels, the same factors and criteria can be taken into account for evaluating the properties if IEO itself, i.e. IEO exposure to terrorist attacks, as well as its environment, i.e. topicality of a terrorist threat.

References

1. Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426). – Hyattsville, MD: U.S. Federal Emergency Management Agency, 2003. – 420 p.

2. National and global security. Terrorism in big city: evaluation of threats and protection/ Ed. **V.Z. Zvorykin**. – M.: Publishing house “Human rights”, 2002. – 113 p.

3. **Solano E.** Methods for Assessing Vulnerability of Critical Infrastructure. Institute for Homeland Security Solutions (IHSS), 2010.

4. **Baker G. A.** vulnerability assessment methodology for critical infrastructure sites. Department of Homeland Security symposium: R&D partnerships in homeland security. – Boston, Massachusetts, 2005. http://works.bepress.com/george_h_baker/2.

5. State and Local Mitigation Planning How-to Guide: Integrating Manmade Hazards into Mitigation Planning (FEMA 386-7). – Hyattsville, MD: U.S. Federal Emergency Management Agency, 2003. – 78 p.

6. **Willis H., Morral A., Kelly T., Medby J.** Estimating Terrorism Risk. – Santa Monica, CA: RAND Corporation, 2005. – 94 p.

7. **Radaev N., Bochkov A.** Evaluation of terrorist threat for an object/ BDI (Security. Reliability. Information). – 2008. – № 2. – P. 16-19.

8. DHS Risk Lexicon. – Wash.: U.S. Department of Homeland Security, 2010. – 72 p.

9. A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 452). – Hyattsville, MD: U.S. Federal Emergency Management Agency, 2005. – 248 p.

10. **Bea R., Mitroff I., Farber D.,** et al. A new approach to risk // Risk Management. – 2009. – Vol. 11, 1. – 30-43 pp.

11. **Kuvaldin S., Silaev N.** Terror with Russian money // Expert. – 2011. – № 4 (738). – P. 17-21.

12. **Brooks N.** Vulnerability, Risk and Adaptation: A Conceptual Framework. – Norwich: Centre for Social and Economic Research on the Global Environment (CSERGE). School of Environmental Sciences. University of East Anglia, 2003. – 20 p.