Abramova N.A., Makarenko D.I., Telitsyna T.A.

MODEL AND METHOD FOR DEFINITION OF SUBSYSTEMS MOST EXPOSED TO DISTURBANCES AS PART OF A COMPLEX FACILITY OF PROTECTION

A descriptive model and an expert-formal method have been developed for definition of a risk area – types of facilities most exposed to anthropogenic disturbances, as part of a complex object of protection, for the specified strategy of protection. The explanatory capacities of the model have been demonstrated through the analysis of protection strategies and consequences of their violations exemplified by a threat of terrorist attack.

***Keywords**: security, vulnerability, attractiveness, disturbances, facility of protection, threat of terrorist attack.*

Introduction

Nowadays, a vital task is an analysis of susceptibility of various types of protected objects to disturbances (DB). Such an object can be a specific territory (region, country), a big city with all its infrastructure facilities or a separate airport with its subsystems etc.

However, such task is a complex and complicated one. For instance, development of integrated security systems for a big city can be categorized as advanced poorly structured and formalized interdisciplinary problems. The complexity of the task, according to practically all known criteria, is also related to the subject matter, i.e. the safety of normal life of big cities and to security systems with their multilevel nature when a system incorporates a number of levels ranging from technical facilities of control over a distributed information infrastructure, decision-making system to management systems and regulatory documents governing their application and interaction. At the same time, strict requirements of reliability, resilience, durability and safety are made both for infrastructures of big cities and their control and management systems.

The aim of the analysis of DB susceptibility is to define the weakest spots of the facility (or the territory) to do protection activities under the conditions of DB increased threats or to correct the strategy of facilities protection and choose priority directions of investment (a number of typical problems of the kind has been studied in [1]).

The authors of the paper have developed a descriptive model and an expert-formal method to define a risk zone – types of facilities most exposed to anthropogenic disturbances, as part of a complex object of protection, for the specified strategy of protection. It should be noted that further in the paper we con-

sider DB as a terrorist attack, however the theoretical tools developed are also applicable to other DBs of similar types (i.e. intentional anthropogenic DBs).

The model and method developed are based on the principles of a criterion approach and optimization accepted in the theory of decision making but adapted to the subject matter as to the type of criteria and the specifics of terrorist attacks as intentional anthropogenic DBs [1, 2].

The central place in this adaptation is taken by formalization of the term "susceptibility of an object to terrorist attacks" – its presentation using rough criteria of assessment (offered earlier in [3]) allows us to make a comparative evaluation of facilities. In Section 1 you can find the formalization of the term "susceptibility of an object to terrorist attacks", formalized problem statement, a situation model where the task under consideration belongs to and the method of solution.

Further in Section 2, you can find the exemplified explanatory capabilities of the model for some situations of practical value (analysis of protection strategies and some consequences of their violations, diagnostics of mistaken prediction of a risk zone).

Based on the analysis of narrow places of the model, Section 3 defines the approaches to its further development and statement of new research problems.

1. Model and method for defining subsystems and nodes of a complex object of protection most exposed to terrorist attacks

1.1. Formalization of the term "susceptibility of an object to terrorist attacks"

The main task in defining subsystems and nodes most exposed to DB can be treated from various points of view depending on the context wherein the results of its solution are intended to be used in practice.

In particular, when formalizing the term "susceptibility of an object to terrorist attacks", the property of a facility's susceptibility to terrorist attacks TL, as well as other similar properties, can be considered as

– own **property of an object**, $TL(o)$;

– object-oriented **property of the environment** from where a more or less permanently operating disturbing factor of a terrorist attack possibly accompanied by collateral and counteracting factors arise, $TL(E)$[1];

– property $TL(o,E)$ considering **both constituents**.

In any case, even if for applied objectives, a complex property is required, it seems reasonable to know how to evaluate its constituents separately. And this applies to a criterion approach as well as an approach based on risks.

In formal and logic terms, we can speak about "things" where the investigated property P belongs to.

For example, in the approach based on vulnerability [4], the vulnerability is considered as an infrastructure facility's or territory's own property, $P(o)$. The approach used by a well-know British analytical company Maplecroft [5] who analyzes the susceptibility of countries to risks of terrorist attacks studies a complex index characterizing the property of environment, $P(E)$. However, Maplecroft also does analyses of complex risks taking into account, besides outer threats of terrorism, for example, inner risks for business or human rights, i.e. analyzing a complex property $P(o,E)$.

[1] This property is particularly clear in case of outer terrorism and outer forces that influence its intensity when it is natural to consider the environment as outer environment. However, in case of inner or mixed terrorism as well, it is reasonable to single out factors that are relatively out of control for the terrorized party.

This section offers a model of the term *TL*, wherein susceptibility to terrorist attacks is treated as an infrastructure object's own property, *TL*(*o*), which corresponds to the conditions of a relative stability of the "environment" and in particular to a permanently operating disturbing factor of terrorism. This model is focused on solving the main task within the context of such situations as assessment of an operational situation and decision making about directions of protection measures within a compound object, evaluation of the quality of its protection strategies etc.

1.2. Criteria of susceptibility to terrorist attacks

As a common criterion for assessment of an object *o* as part of a compound object, we accept the criterion *TL*(*o*) that in terms of the interests of security services is interpreted as **a criterion of susceptibility to terrorist attacks** for an object *o*, and in terms of the interests of terrorists as a criterion of relative attractiveness of an object *o* **for making a terrorist attack**. The criterion *TL*(*o*) is understood as a compound criterion comprising a couple of rough criteria defined in [3]:

$$TL(o)=(A(o),V(o)),$$

where $A(o)$ is the attractiveness of o for terrorists,
$V(o)$ is the vulnerability of o.

The vulnerability V(*o*) is considered as a property additional to protection – the vulnerability is maximum in case of minimum protection, and vice versa.

It is assumed that $A(o)$ characterizes the attractiveness independently of its protection (both natural and intentional), while a compound criterion $TL(o)$ is considered as **relative attractiveness**, since it takes into account both criteria, important for susceptibility to terrorist attacks.

Each of the constituting criteria, $A(o)$ and V(*o*), is a variable which takes on values on a finite order scale.

Generally, rough scales are used for assessment, with a small range of values, very often verbal ones. For example, for assessment of vulnerability-protection, one may accept a four-valued scale:

«maximum vulnerability / minimum protection» (the level of protection is so low that it doesn't decrease the attractiveness for terrorists),

«vulnerability is quite high»,

«vulnerability is quite low»,

«minimum vulnerability / maximum protection» (the level of protection is so high that there is practically no relative attractiveness for terrorists).

It is assumed that intuitive estimations of relative attractiveness for terrorists have the properties of inexact monotony:

$$A(o_1)>A(o_2)\ \&\ V(o_1)=V(o_2) \Rightarrow \neg\ (TL(o_1)< TL(o_2))$$

$$V(o_1)>V(o_2)\ \&\ A(o_1)=A(o_2) \Rightarrow \neg\ (TL(o_1)< T(o_2)).$$

If in its composition, a compound object has facilities indiscriminative as to the criterion $TL(o)$, it is appropriate to speak about homogenous facilities and a type of objects. Further on let us consider the notation o as referring to the type of objects.

Relation of estimations to the state of an object. Estimations of an object of protection as to the criterion $TL(o)$ characterizes its current state. An important difference of constituents consists in the fact that the property of vulnerability (or, on the contrary, protection) is controllable for security services. Also, generally speaking, the state of vulnerability can change due to various factors such as the quality of operational activities of security services. The current estimation as to the criterion of vulnerability $V(o)$ corresponds to the strategy of facilities protection, similar for all the objects of the type.

For solving tasks related to definition of most vulnerable objects in this model, it is assumed that the current state of vulnerability corresponds to estimations.

1.3. Structural model of a compound object of protection

Generally, a compound object of protection is considered as a hierarchy of constituting facilities, including elementary ones, i.e. indivisible ones for the accepted structuring ("nodes") and composite facilities ("subsystems"). In the **T** typology of objects comprising a compound object, the facilities indiscriminative in terms of susceptibility to terrorist attack belong to the same type.

For example, of the same type within a **big city** compound object of protection can be all **international airports** with similar protection / vulnerability, and their constituents can be such facilities as "**green zone**", **arrival areas** etc. (as exemplified by the terrorist attack at the Domodedovo airport in 2011 [6]).

A hierarchy node in the **T** typology of objects is some type of compound objects O comprising a set of types of constituting facilities (elementary or composite ones) belonging to the nearest lower level of the hierarchy.

A hierarchy node of a complex infrastructure object like an airport can be considered as a separate facility of protection if an individual strategy of protection is developed for it.

When solving the main task, as the simplest structural model of a compound object, we study the model $\mathbf{M_0}$ comprising one node of hierarchy. It is attractive in that we can apply to it a model of multicriteria optimization – search of the most attractive types of objects in a set of object types forming the **T** typology of such compound object O.

By the S **strategy** of protection of a compound object O we'll understand a set of more or less heuristic rules to define which types of objects are acceptable (or unacceptable) in the $T(O)$ typology of a protected object O. (Examples of such rules will be given below.)

The method for solving the main task is developed by now for the model $\mathbf{M_0}$.

1.4. Formal statement of the problem

Let there be a compound object O with one level of hierarchy, $O=\{o\}$, and for it there is defined what follows:

- scales S_1, S_2 for assessment of object types as part O as to criteria of attractiveness for terrorists, $A(o)$, and vulnerability, $V(o)$, respectively;
- typology of objects as part of the object O, $\mathbf{T}(O)$ with evaluations on the set scales;
- S strategy of protection of the object O.

It is necessary to define the **risk zone** Z, i.e. the type of objects or, more generally, a set of object types, relatively most attractive for making a terrorist attack, in other words, most exposed to the risk of a terrorist attack.

For the sake of simplification, assume that all the values on each of estimation scales S_1, S_2 are used for assessment of objects as part of O.

1.5. Description of the problem solution method

To make it clear, the method is exemplified by a case where identical scales with scores (0,1,2,3) are accepted for each criterion. In Fig. 1 a full set $\bar{M}$ of object types imaginable for accepted scales of estimation as to a complex criterion $TL(o)$ is presented as a so called Hasse diagram. Each type of facilities is presented by a pair of values:

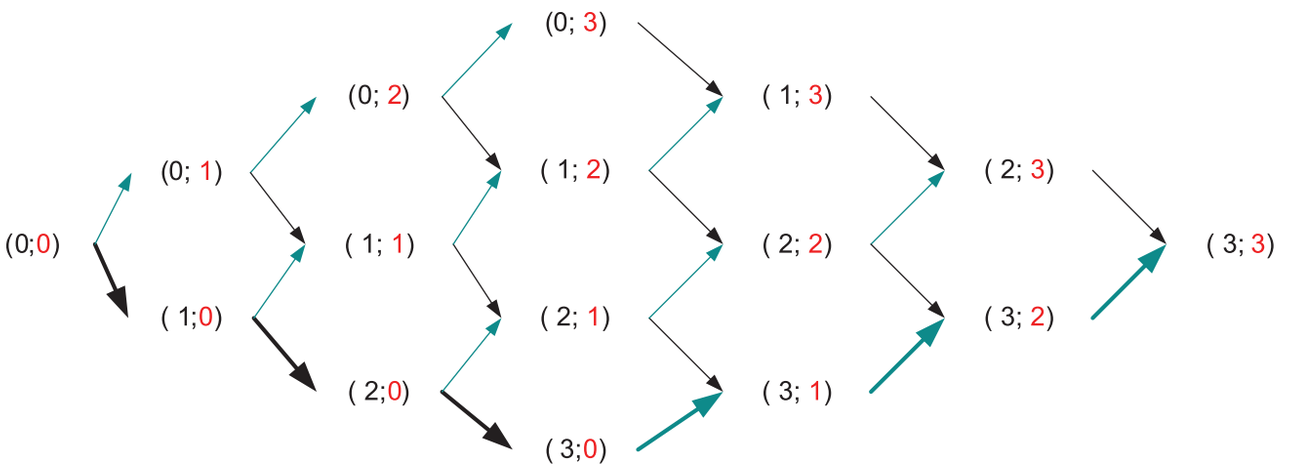

Fig. 1. Full set of types of objects possible for the adopted scales of assessment as to the compounded criterion

For example, pair (1,3) means the type of objects with scores $A(o)$=1, V(o)=3. The arrows show the increase of a score as to one of the criteria with the score remaining the same as to the other criterion.

The set $\bar{M}$ is partially normalized. Thus,

- range (sequence) R1=((3;0), (3;1), (3;2), (3;3)) presents all the types of objects most attractive as to the first criterion, attractiveness, $A(o)$, which are ordered as per increase of the second criterion, vulnerability, V(o);
- range R2=((0;0), (0;1), (0;2), (0;3)), on the contrary, presents all the types of objects least attractive as to the criterion $A(o)$, which are also ordered as per increase of the criterion V(o);
- range R3=((0;0), (1;0), (2;0), (3;0)), presents all the types of objects least attractive as to the second criterion, vulnerability (i.e. assessed as invulnerable), which are ordered as per increase of the first criterion $A(o)$.

Stage 1. Definition of the typology of objects as part of a compound object *O* according to the adopted strategy of protection *S*

When choosing a strategy of protection, one generally relies on intuitive heuristic rules of thumb that are thought rational, and one assumes that the counteracting party is rational (though in its own way).

In terms of selection of a protection strategy, it is obvious that terrorists would find as relatively most attractive as to the complex criterion $TL(o)$ the type of objects with a score (3,3), i.e. most attractive and most vulnerable ones, as well as objects near as per score to (3,3).

On the contrary, it is natural to suppose that the types of objects of range R3 would have a zero attractiveness as to the criterion $A(o)$, independently of their vulnerability.

Let us consider examples of heuristic rules that can be assessed as rational.

General rule 1, R1 ("**objects not attractive for terrorists are not protected**"). According to this rule, objects with score within O protected as to the rule R1 from the potential range of objects R2=((0;~)) where «~» is any vulnerability, in the set M_{R1} of object types accepted by this rule can be only objects of

the type (0;3), i.e. unprotected. (Of course, this rule implies that by default we speak only about protection against terrorists, and natural properties of object protection are not taken into account for the sake of convenience).

In some strategy S` the type of objects (1;0) intuitively close to R2 in terms of attractiveness can also be excluded by an additional **specific rule** R1`.

General rule 2, R2 ("**more attractive objects cannot be more vulnerable**"). According to this rule, if even one of the type of object is protected, this should be the type (3;3). An additional specific rule R2` by means of protection (i.e. reduction of vulnerability) can exclude for example the types of objects (2;3), (3,2), (2;2), (3;1) closer to (3;3) compared to others.

In Fig. 2 you can see in the full set of object types those darkened objects that should not be within a compound object *O* for the adopted strategy of protection *S*={R1, R2, R2`}.

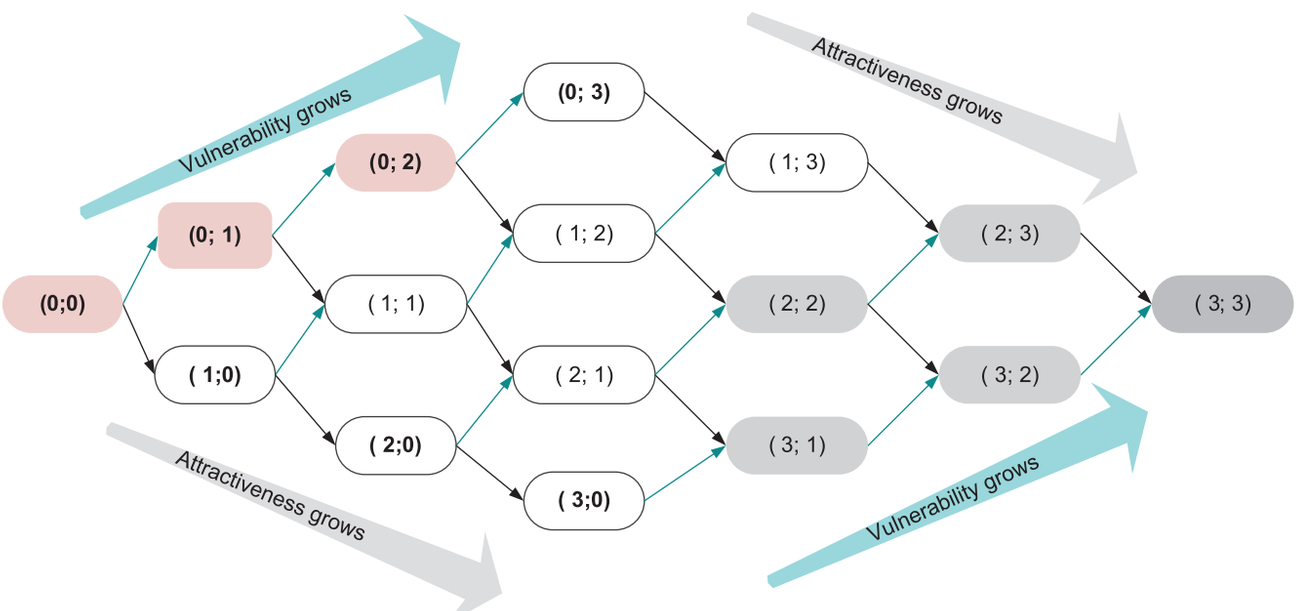

Fig. 2. Set of types of objects when protected using *S* strategy

Generally, according to the general rules of protection R1, R2, when constructing a set of object types M_S which are evaluated as more or less susceptible to a threat, we exclude from the full set $\bar{M}$ the set $M_{\notin}$ of object types that in principle cannot be in the typology O \ in O as to the rule R1 (in the example this is the set $M_{\notin}$ = {(3;3), (2;3), (3,2), (2;2), (3;1)}), on the one hand, and the zone M_u, on the other hand, relatively unattractive due to low attractiveness even in case of protection unavailability (in the example, M_u={(0;0), (0;1), (0;2)}). In comparison to objects from $M_{\notin}$, objects from M_u can be present in the typology *O*, but they are not considered as objects of protection.

The results of application of a protection strategy is received as the set M_S,

$$M_S = \bar{M} \setminus (M_{\notin} \cup M_U)$$

Stage 2. Definition of Pareto set in $\bar{M}$. Rough estimation of the highest susceptibility to terrorist attacks

Fig. 3 shows the division of the set $\bar{M}$ of the example under consideration into 2 classes: Pareto set M_A={(1;3), (2;1), (3,0)} and a set of all other types of objects M_O={(1;0), (2;0), (1;1), (1,2), (0;3)}.

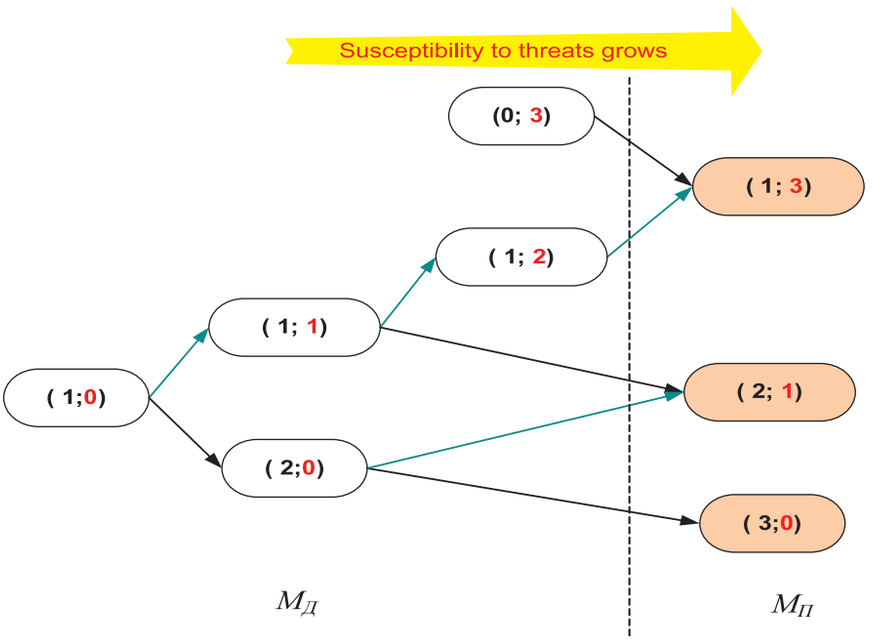

Fig. 3. Types of objects most exposed to terrorist attacks as per Pareto

Compared to a Pareto set of object types, all the objects of the set M_O are **dominated** in $\bar{M}$. Graphically the property of domination of the object type o by the type $o`$ is expressed in that the route from the type $o$ goes to the type $o`$. Thus, for the dominated type (1;0), dominating types as per the criterion of vulnerability are more vulnerable types (1;1), (1;2), (1;3) with their equal attractiveness, and (1;3) $\in M_П$, i.e. it is not dominated by any other objects; the objects of type (1;0) are dominated as per the criterion of attractiveness by the objects of type (2;0), (3;0), with their equal vulnerability, and (3;0)$\in M_П$. For the same type (1;0), the type (2;1) is a dominating one both as per the criterion V(o) and O(o), (2;1)$\in M_П$.

The fact that some type o is dominated as per some or all specific criteria means that it is less susceptible to terrorist attacks than dominating types (in case of real selection based on specific criteria). On the contrary, the fact that the type of objects o belongs to the set M_A means that there are no dominating types for it, and on the basis of separate criteria as part of $TL(o)$= ($A(o)$, V(o)) such types are incomparable, and all of them can be considered as most susceptible to terrorist attacks as per Pareto criterion.

Such solution seems to be natural when we attempt to get higher values if possible as per each of constituting criteria as part of $TL(o)$.

Generally they say that a Pareto set includes a subset of all elements where each of them is “not worse” than others.

Stage 3. Definition of expert preferences in a Pareto set

Despite the intuitive naturalness of defining a set of all objects types most susceptible to terrorist attacks as a Pareto set (for a selected set of constituting criteria, in this case PT_A), it is understandable that in this case by default we imply equivalence of constituting criteria, and there is no aggregation of estimations as per these criteria.

In reference with it, it is necessary to further specify a set of risk zone Z within the limits of Pareto sets,

$$Z \subset M_{UP}$$

The final selection should be done by experts taking into account not only a relative correlation of importance (weights) of criteria $A(o)$ and $V(o)$ in general, but in the first place considering the analysis of a specific Pareto set. In this case experts single out a risk zone Z from a Pareto set. The example of complete solution of the problem is shown in Fig. 4.

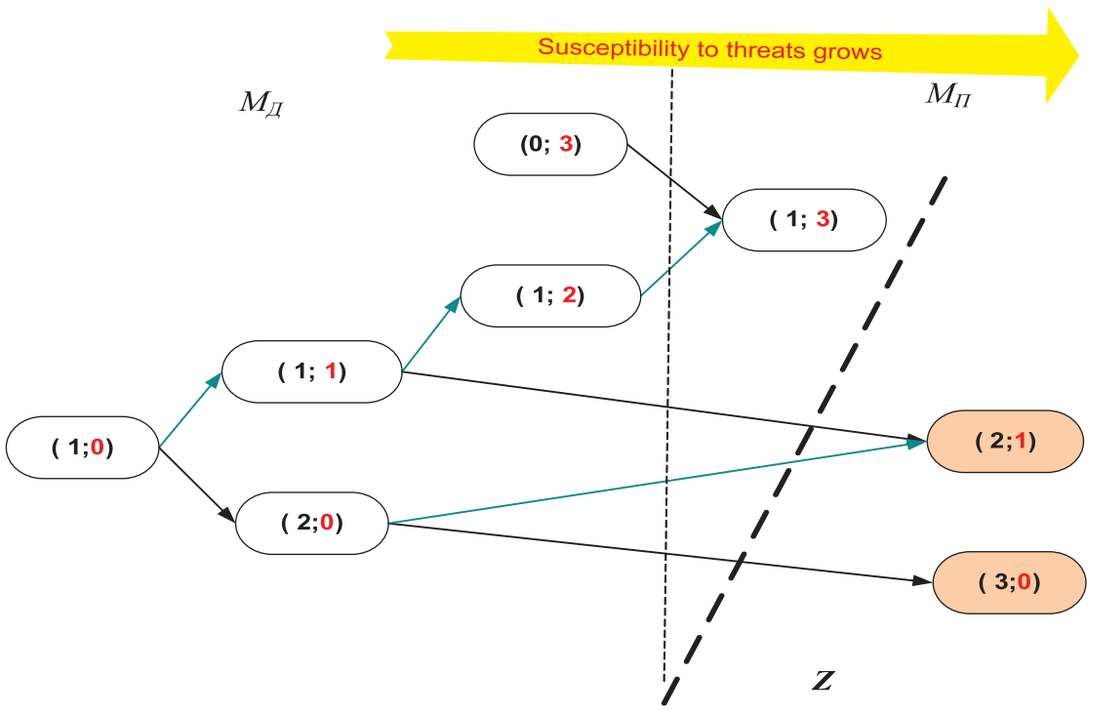

Fig. 4 Preferences within the Pareto set

2. Descriptive capabilities of the model and the method for situations of practical value

The descriptive capabilities of the investigated formalized model M1 of a ситуации where a risk zone Z is defined as part of a compound object O will be exemplified using the previous example in Fig. 1 for two types of situations of practical value.

Operational (in a specific situation) deterioration of protection of some facility in relation to standard protection (i.e. increase of vulnerability). Arrows 1 and 2 in Fig. 5 show two types of deterioration. Transit of an object from the type (1;1) into the more vulnerable type (1;2) and event in (1;3) is not dangerous, as due to low attractiveness it will not be an object of a terrorist attack. (There is some reserve of dominating facilties that are out of a risk zone.)

On the contrary, increase of vulnerability of an object of type (2;0) (transit from type (2;0) into (2;1)) moves it into a risk zone Z.

A fresh example of the situation is increase of vulnerability of the arrival terminal in Domodedovo due to the decrease of protection quality by the transport police securing the airport entries.

To make decisions about responsibility for psychologically explainable reduction of quality in protection of a relatively unimportant facility, e.g. an airport entry, it is necessary to take into account that it is beyond the competence of the police to understand the structure of protection of facilities (such as Fig. 4) as well as the correlation between entry protection and preferences (relative attractiveness) of an arrival terminal as a place of a terrorist attack for terrorists.

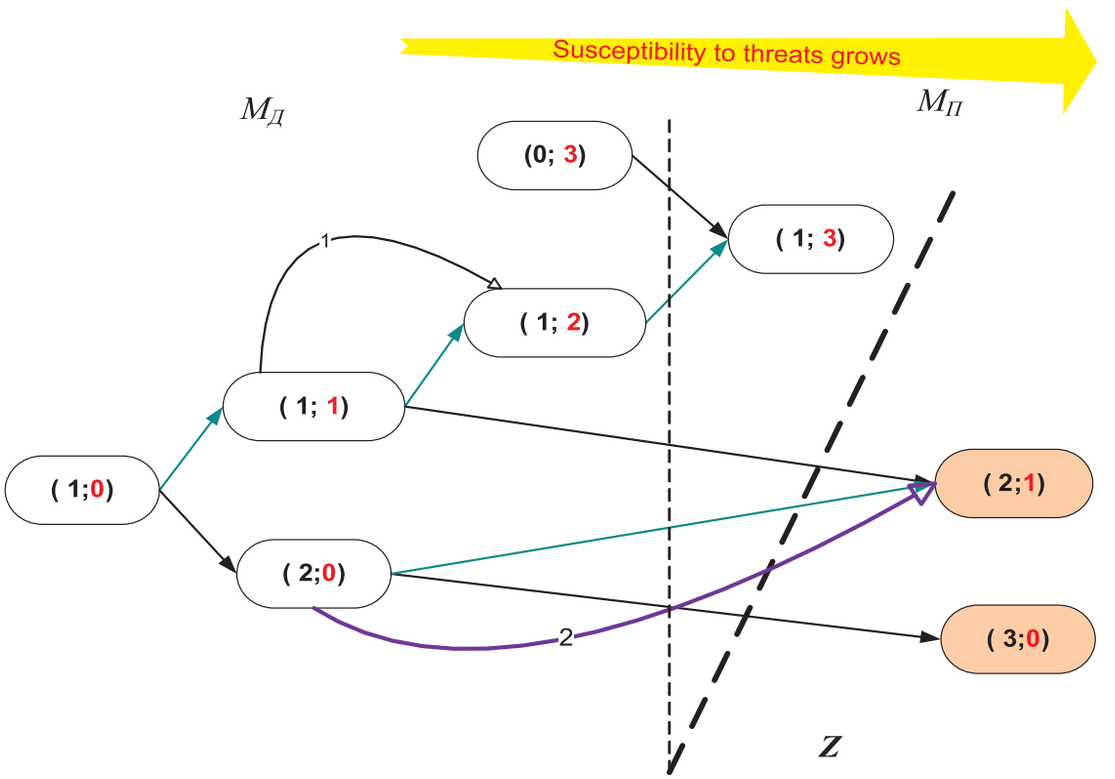

Fig. 5. Operational violations

Measures of ensuring and supervision over ensuring a required quality of protection strategy implementation as well as a strategy of protection itself should be in charge of security services protecting a compound object, an airport, due to their awareness as to the logics of management. It should not be ruled out that the quality of security could be influenced by simply briefing the guards that penalties for poor quality of protection of specific nodes were defined according to a (specified0 level of risk.

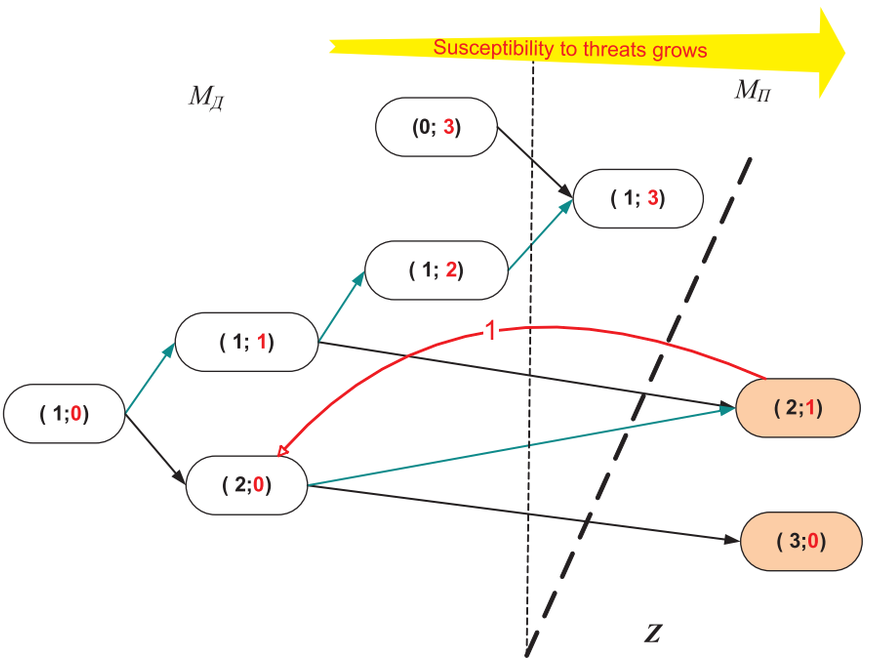

Fig. 6. Improvement of protection

Estimation of effect from a protection strategy change. The strategy "increase of protection level" that they start to promote in many countries after terrorist attacks should be naturally applied in the first place to a risk zone (or at least to a Pareto set), since otherwise a set of object types most exposed to terrorist attacks will not change.

Arrow 1 in Fig. 6 shows the effect from increase of a protection level for the objects of type (2;1) from the risk zone *Z,* i.e. their transit into a less vulnerable type (2;0).

As a result, the number of objects in a risk zone has decreased; however, in cases when a risk zone still contains only the objects with maximum protection (in this example (3;0)), further efforts in increasing protection of a compound object *O* will not change the set *M* of objects most exposed to threats.

Diagnostics of a mistakenly predicted risk zone. Prediction of a risk zone in a set of objects with varying degrees of protection and attractiveness by using the presented method or otherwise is based on a number of human assumptions. Such assumptions are among the risks for reliability caused by human factor [7]. Detection of erroneous prediction and in our case a fact of a terrorist attack at an object not being in a risk zone requires further diagnosis and correction of the model adopted for prediction. Reasons of forecast inaccuracy can be very different including violations of the protection strategy. Special role among these reasons is taken by mistakes of the model of attractiveness for terrorists, which is laid in the typology of objects to be protected through the evaluation of object types as per A(*o*). (In theoretical terms, this is a false hypothesis of general knowledge.) At least one type of such errors consists in that from the viewpoint of terrorists, objects do not in fact belong to the type of attractiveness, as it is viewed by the protecting side.

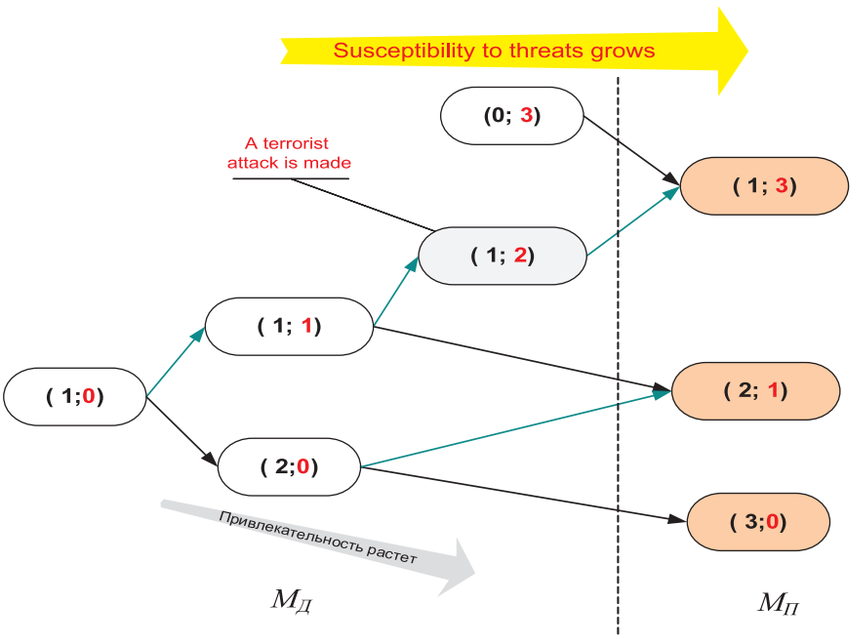

Fig. 7. Errors of the attractiveness model

The possibility of diagnosing such errors, i.e. forming hypotheses about the causes of errors, is shown for our example in Fig. 7 and Fig. 8. In Fig. 7 we have marked the object type (1;2), to which the object of a terrorist attack was attributed; this object does not belong to a risk zone, according to the accepted model of attractiveness for terrorists. One of the reasons that the terrorists did not follow this model, remaining within the framework of rationality hypotheses, could be that the protection of the object *O* is in general high and the pressure (intensity) of the destabilizing factor of terrorism is also high. The result may be a shift of the attractiveness model, not considered in predicting a risk zone (Fig. 8).

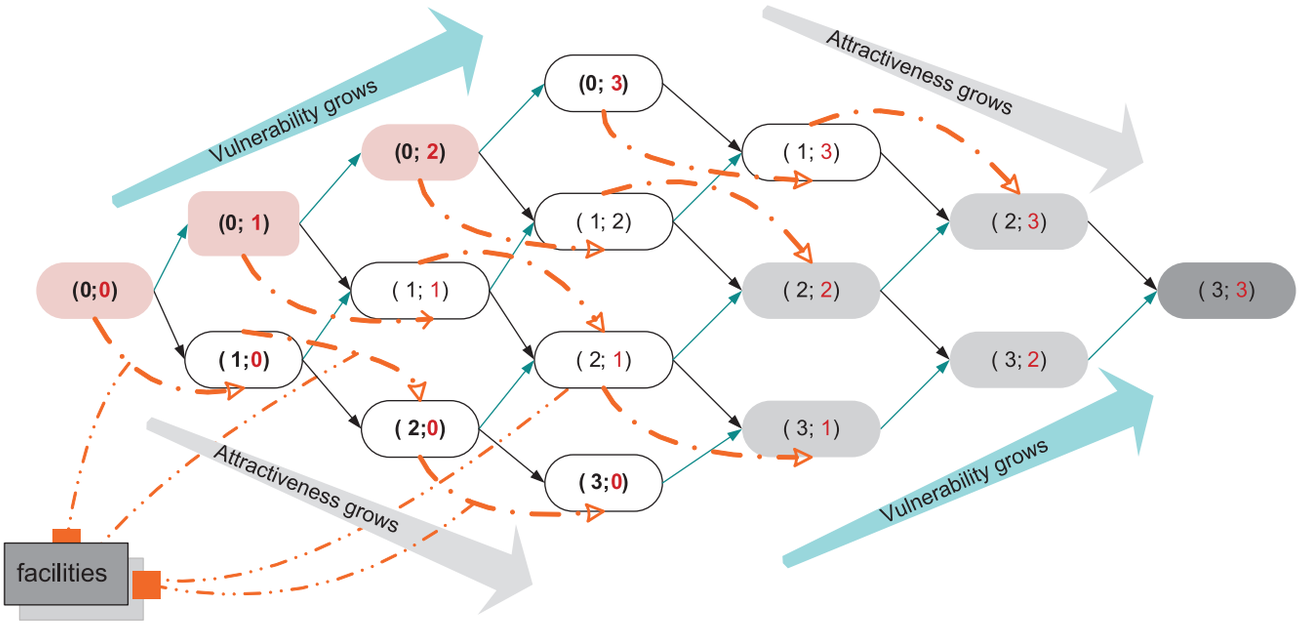

Fig. 8. Shift of the attractiveness model

3. Analysis of bottlenecks and limitations of a situation model forming the basis of the method. Further development

In accordance with the principle of development and cross-cutting application of verification methods to protect against risks to ensure the reliability of methods put in the basis of security systems, the proposed method of estimating objects most prone to terrorist attacks and a model of evaluation situations in which it can be applied should undergo analysis. The purpose of this analysis is to identify bottlenecks, constraints, risks due to a human factor.

To demonstrate the content and features of this analysis, let us present a fragment of such an analysis. It is based on the restriction of the proposed model consisting in the fact that the proposed criteria of attractiveness, A(o), and vulnerability, V(o) to assess certain types of objects as part of an object of protection are very generalized. To obtain estimates for these criteria, it is necessary to move from estimates as to specific criteria to integrated estimates as to criteria A(o) and V(o), and in this case these criteria may be interdependent.

Accounting of the dependence of A(o) and V(o) **on general factors.** It is not obvious how to take into account various specific criteria and factors in the composition of the main criteria: attractiveness, A(o), and vulnerability-protection, V(o), when assessing objects as to these two criteria.

First of all, we deal with such indices as criticality (importance) of an object, which can be attributed to A(o) as well as to V(o). Since a more critical object, on the one hand, is more attractive for terrorists, and on the other hand, it is usually more protected in accordance with typical security strategies of protection.

In the case of a criticality factor, C(o), it is certainly among the main factors for evaluation of attractiveness, A(o). However, in the model an estimation is made for the current state of affairs for a fixed protection strategy, C(o), so the dependence of C(o) on criticality is already included in the strategy, and its inclusion in the V(o) is no longer required.

If it is necessary to review and compare different protection strategies, evaluate sensitivity to modifications of the strategy (or different knowledge of counteracting parties about it), it is required to consider

different models of the situation. It is recommended to do such activities related to modification of strategies using some software support (animation like in Fig. 6, Fig. 7) for clarity.

In all cases, an individual analysis is required for each criterion (or factor) to avoid duplication of accounting of the same factor via A(o) and V(o): in the proposed model the criteria A(o) and V(o) are treated as independent. (For this purpose, cognitive maps describing the interaction of various factors and their impact on selected generalized criteria may be useful. The example of such card is presented in [3].)

Further development in this direction consists in moving to reflexive models taking into account the estimations of the parties of others' knowledge. It is assumed that the further development of models and methods of its analysis should allow for not only taking into account the different knowledge of the opposing sides, but also the "reflexive games": mimicry in the case of terrorist attacks, creating traps for terrorists, etc.

When analyzing the influence of an external threat of a terrorist attack on a security system using the proposed method (or possibly other methods of the same kind), the focus is on the current state of vulnerability / security of a complex object and its current assessment by terrorists. However, in reality, for reliability of short-term predictions, it is also important to take into account the long-term dynamics of the interaction of an external destabilizing factor of terrorism and its attendant factors with internal strategic decisions on such interaction.

Conclusion

The offered model with the method of defining a risk zone in the situation when susceptibility of separate facilities of a complex object of protection is conditioned by two criteria, i.e. the attractiveness of separate facilities and their vulnerability (for the specified strategy of protection of a complex object), though simple, has shown its real value for various practical situations.

However, due to limitations related to the model, it is required that there will be the further development of the model and the method, from the one hand, and the development of the approach centered on the analysis of long-term dynamics of interaction of security systems with continuous disturbances made by the terrorism factor.

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 a big city: assessment of threats and protection/Ed. Dvorkin V.Z. M.: Human Rights Publishing House, 2002. – 113 p.

3. **Makarenko D.I.** Systematization of criteria and critical factors for assessment of complex systems exposure to disturbances / Dependability, 2013, #4.

4. **D. Sarewitz, R. Pielke, M. Keykhah** Vulnerability and Risk: Some Thoughts From A Political and Policy Perspective, Risk Analysis, Vol. 23, No. 4. (2003), 805-810.

5. Review of Maplecroft's "Terrorism Risk Index 2011", Link: http://foreignpolicyblogs.com/2010/12/04/review-of-maplecrofts-%E2%80%9Cterrorism-risk-index-2011%E2%80%9D/ (request data: 08.08.2013)

6. Terrorist attack at the Domodedovo airport. Wikipedia [Web resource] Link: https://ru.wikipedia.org/wiki/ (request data: 01.08.2013)

7. **Abramova N.A.** About human factor risks in expert methods and information technology // Management issues– 2007, #2, p.11-17.