Approach to Determining the Parameters of Physical Security Units for a Critical Infrastructure Facility

M.D. Katsman

•

Doctor of Sci., Associate Professor, Security Department of JSC "Ukrainian Railways",
Iezhy Hedroitsa str. 5, 03680, Kyiv, Ukraine, e-mail: katsman@uz.gov.ua

V.K. Myronenko

•

Doctor of Sci., Professor, Head of Department of Railway commercial activities management,
Faculty of Railway transport management, State University of infrastructure and technologies,
04071, Kyiv, Ukraine, e-mail: pupil7591@gmail.com

V.I. Matsiuk

•

Doctor of Sci., Professor, Department of transport technology and traffic process control,
Faculty of Railway Transport Operation, State University of Infrastructure and Technology,
Ivan Ogienko str., 19, Kyiv, 03049, Ukraine, e-mail: vimatsiuk@gmail.com

P.V. Lapin

•

M.D., PhD, MPH, Security Department of JSC "Ukrainian Railways",
Iezhy Hedroitsa str. 5, 03680, Kyiv, Ukraine, e-mail: pavlolapin@gmail.com

Abstract

The article discusses some common mathematical models of counterterrorism and acts of unlawful interference with protected objects. The use of methods of queuing theory of Markov and non-Markov types for modeling the counteraction of security personnel by a malicious group with a random number of criminals in a group and different ways of organizing the actions of such personnel is proposed.

Keywords: security object, queuing system (QS), nonordinary stream of malefactor groups, random number of malefactors in the group, non-Markov type QS, security personnel.

I. Introduction

Many scientific works are currently devoted to the problem of counter-terrorism and acts of illegal interference in the activities of critical infrastructure.

The classification of counter-terrorism models is reflected in [1], which provides an overview of current work on modeling the counter-terrorism system and proposes a classification of terrorism and counter-terrorism models.

According to this paper the conceptual models include models developed by specialists in the subject area, political scientists, psychologists, sociologists. As an example, work is given [2], which provides empirical data on the decision-making patterns of members of terrorist organizations at different levels: strategic, tactical and operational, as well as at the level of the individual terrorist.

Models of analysis and synthesis are usually mathematical or physical models. In the review [3] more such works are characterized. In particular, in [4] the basis for the development of classification of terrorist groups using chemical, biological, radiological and nuclear weapons the heuristic method of pattern recognition, the method of classification trees and discriminant analysis were proposed. With regard to transport safety systems, a number of works are devoted to the analysis of devices to increase the probability of detection and reduce the intensity of false alarms. In [5], using Bayesian analysis, a method of threat ranking and prioritization of security measures for facilities is presented.

The complexity of real-world security situations requires the universality of the mathematical models used.

These requirements inevitably contradict the commonality and validity of the simulation results, so when solving models in the form of hierarchy (usually lower levels of hierarchy corresponds to a higher level of detail of the modeled systems description) or a horizontal chain, each element of which is approximately the same [6].

In [1] the levels of modeling (hierarchy of models) of counteraction to terrorism are considered in detail. Theoretical game models of counter-terrorism are presented in [7,8,9]. In [10], an approach to creating a mathematical model of the physical protection systems functioning of objects as a process of interaction of sets based on the theory of ordinary sets, fuzzy set theory and the analysis of hierarchies.

In [11], a mathematical model of describing the nature of the interaction between the components of the "defender - attacker" system as components of the "predator - victim" system is proposed. The model is a modified classic model of Lotki-Volterra competition, which allows you to assess changes in the level of danger for the object with a change in its security.

The use of fuzzy cognitive modeling to prevent risk situations in conditions of fuzzy source data at critical infrastructure facilities is considered in [12]. It proposes the management structure of NPPs in the form of a fuzzy cognitive model, scenarios of risk situations and their analysis.

In [13] the possibilities of application of models of operations research methods for planning of protection of objects of critical infrastructure are considered. Adaptation of these models includes taking into account the stochastic, informational and behavioral uncertainties of terrorists. In this paper, in particular, the generalizations of the tasks of the antagonistic game of attack and defense and the optimal distribution of protective resources are considered.

An example of the use of complex models with parameters measured on different scales is the game-theoretic model for security at Los Angeles international airport, on the basis of which the automated system "Assistant for randomized route control" (ARMOR) was developed and put into operation. [14]. Security is a very important factor in the protection of this facility, given the terrorist threat. However, limited resources do not allow security forces to monitor all facilities and routes around the clock. Terrorists are able to monitor and select unprotected routes and targets if security forces do not use randomized monitoring and patrol tactics.

II. Results and discussion

The authors formulate the basic requirements for ARMOR:

1. The system must take into account the weight of the protected objects. If an attack on the first object leads to economic damage and on the second to human casualties, more weight is given

to the second object. Weights are evaluated by experts and expressed on an ordinal scale.

2. The system must take into account all information about the enemy that is in the security service.

3. The system should not offer a strict service schedule, taking into account additional information, the security service may make adjustments to this schedule. In [15] presented is a description of tests for ARMOR testing, which has been in operation since 2007. Such tests include:

- analysis on the basis of game theory (type of test Mathematic): with known matrices of winnings, the gain of the attacker and the probability of refusal to attempt an offense is calculated;
- resource allocation (test type - Mathematic): game theory helps to find the expected gain of the attacker in different security strategies;
- cost of protection (type of test - Mathematic): game theory helps to find the expected gain of the parties at change of security technologies (due to introduction of new technical means of protection, new technology of check of passengers and luggage);
- simulation of the attack (test type - Simulation): the use of additional simulation models;
- conducting exercises using "educational" criminals;
- Expert assessment (type of test - Qualitative): security specialists are able to assess many factors for their further consideration in the model as their parameters.

Since 2009, ARMOR has been used to plan air patrol services with the task of optimal distribution of 3000-4000 patrols on 29000 daily flights.

Thus, a wide range of mathematical models are used to model the physical security systems of objects.

In our opinion, in order to determine the effectiveness of the actions of the unit of protection of critical infrastructure, it is advisable to use the mathematical tools of the queuing theory.

Consider an object guarded by a security unit of n people as a queuing system. Groups of intruders with an intensity of λ try to enter the object in order to endanger its safe operation. In general, the number of a group of attackers can be random, in other words, with a probability of as, the group can consist of s attackers.

That is, the n-channel queuing system (QS) receives a stream of λ [groups / units of time] of group demands with a random number of demands in the group.

Such QS have found their application in mathematical models of information technology, which is reflected in the works [16-18].

One of the features of the QS under consideration is that the time $\bar{t}_{int}$ of intruders on the object is limited, it is a random variable that is subject to the exponential law with the parameter $\eta = \frac{1}{\bar{t}_{int}}$.

The parameter η is the intensity of demands leaving the QS service channel due to the restriction of their stay in the system.

The parameter μ characterizes the system of counteraction $\mu = \frac{1}{\bar{t}_{ca}}$ [malefactor / unit of time], where $\bar{t}_{ca}$ is the average time of the guard's use of counteraction means to the malefactor.

Counteraction to intruders by the security unit can be organized in different ways, which determines the type of queuing system. The first group of QS includes:

1. M / M / n / m type QS with restriction (η ≠ 0), without mutual assistance (h = n, g = 1), non-ordinary demands and a random number of demands in the group. Here, h is a value equal to the ratio of the total number of n guards (service channels) to the number of g guards, which are combined into a group to counter one attacker, ie n = n / g.

2. M / M / n / m type QS with restriction (η ≠ 0), full mutual assistance (h = 1; g = n), non-ordinary demands and random number of demands in the group.

3. M / M / n / m type QS with restriction (η ≠ 0), with partial mutual assistance (h = n / g), non-ordinary demands and a random number of demands in the group.

The second group includes QSs of the non-Markov type, which simulate the conditions when the forces and means of protection are not on the site, for example, when it is necessary to concentrate additional forces and means. That is, the counteraction process consists of two phases lasting respectively $\bar{t}_1$ - concentration time and $\bar{t}_{gr}$ - time of counteraction means application, where $\overline{t_1}$ has an exponential distribution with the parameter $\mu_1 = \frac{1}{\bar{t}_1}$ [guard / unit time], and $\bar{t}_2$ - with parameter $\mu_2 = \frac{1}{\bar{t}_{gr}}$ [malefactor / unit time].

That is, the total resistance time has a generalized Erlang distribution with parameters μ1 and μ2.

Such QS have limitations $\eta \neq 0$, can be with different characteristics of mutual assistance, there is a queuing system with heterogeneous demands and a random number of demands in the group.

Some aspects of mathematical models of these QS are considered in [19-22].

Consider in more detail the QS of the first group.

1.1 M / M / n / m type QS with restriction ($\eta \neq 0$), without mutual assistance (h = n, g = 1), non-ordinary applications and random number of applications in the group.

Kolmogorov differential equations for the probabilities of states of these QS are:

$$\frac{dP_0(t)}{dt} = -\lambda P_0(t) + (\mu + \eta)P_1(t);$$

$$\frac{dP_0(t)}{dt} = -(\lambda + \mu + \eta)P_1(t) + \lambda a_1 P_0(t) + 2(\mu + \eta)P_2(t);$$

$$\frac{dP_2(t)}{dt} = -(\lambda + 2\mu + 2\eta)P_2(t) + \lambda \sum_{s=1}^{2} s a_s\, P_{2-s}(t) + 3(\mu + \eta)P_2(t); \tag{1}$$

……………………………………………………………………………

$$\frac{dP_k(t)}{dt} = -(\lambda + k\mu + k\eta)P_k(t) + \lambda \sum_{s=1}^{k} s a_s\; P_{k-s}(k + 1)(\mu + \eta)P_{k+1}(t);$$

At 1≤ k < n

……………………………………………………………………………

$$\frac{dP_k(t)}{dt} = -(\lambda + n\mu + k\eta)P_k(t) + \lambda \sum_{s=1}^{n} s a_s\; P(t)_{n-s}(t) + [n\mu + (k + 1)\eta]P_{k+1}(t);$$

At k ≥ n.

For stationary conditions the system of linear equations will be:

$$0 = -\lambda P_0 + (\mu + \eta)P_1;$$

$$0 = -(\lambda + \mu + \eta)P_1 + \lambda a_1 P_0 + 2(\mu + \eta)P_2;$$

…………………………………………………

$$0 = -(\lambda + k\mu) + k\eta)P_k + \lambda \sum_{s=1}^{k} s a_s\; P_{k-s} + (k + 1)(\mu + \eta)P_{k+1} \tag{2}$$

At 1≤ k < n;

……………………………………………………………………………

$$0 = -(\lambda + n\mu) + k\eta)P_k + \lambda \sum_{s=1}^{k} s a_s\; P_{k-s} + [n\mu +)k + 1)\eta]P_{k+1}$$

At k ≥ n

Normalizing condition

$$\sum_{k=0}^{\infty} P_k = 1.$$

1.2. M / M / n / m type QS with restriction ($\eta \neq 0$), full interaction ($h = 1$, $g = n$), non-ordinary demands and random number of demands in the group.

The peculiarities of this QMS functioning, and hence the organization of counteraction is:
- the first demand is served by all service channels with intensity $\mu = n\mu + \eta$;
- the next demand is served by part of the service channels, others continue to service the previous demand, if it was not completed;
- after the completion of the service of any demand, the group of channels that has been vacated is connected to the service of demands that are in the system;
- in the Markov (Poisson) QS, the characteristics of the service do not depend on the distribution of channels between demands, only it would be uniform and all channels would participate in the service simultaneously [20];
- if there are already n applications in the system, then (n + 1) application stands in the queue.

The system of differential equations of states probabilities has the form:

$$\frac{dP_0(t)}{dt} = -\lambda P_0(t) + \mu^* P_1(t);$$

$$\frac{dP_1(t)}{dt} = -(\lambda + \mu^*)P_1(t) + \lambda a_1 P_0(t) + 2\mu^* P_2(t);$$

$$\frac{dP_2(t)}{dt} = -(\lambda + 2\mu^*)P_2(t) + \lambda \sum_{s=1}^{2} sa_s\, P_{2-s}(t) + 3\mu^* P_3(t); \qquad (3)$$

……………………………………………………………………………

$$\frac{dP_k(t)}{dt} = -(\lambda + k\mu^*)P_k(t) + \lambda \sum_{s=1}^{k} sa_s\, P_{k-s}(t) + (k+1)\mu^* P_{k+1}(t);$$

При $1 \leq k < n$;

……………………………………………………………………………

$$\frac{dP_k(t)}{dt} = -(\lambda + n\mu^* + k\eta)P_k(t) + \lambda \sum_{s=1}^{n} sa_s\, P_{n-s}(t) + [n\mu^* + (k+1)\eta]P_{k+1}(t);$$

At $k \geq n$.

1.3. M / M / n / m type QS with restriction ($\eta \neq 0$), partial interaction ($h = n / g$), extraordinary applications and random number of applications in the group.

The system of differential equations of probabilities of states of the system will be as follows:

$$\frac{dP_0(t)}{dt} = -\lambda P_0(t) + \mu_g^* P_1(t);$$

$$\mu_g^* = g\mu + \eta;$$

$$\frac{dP_1(t)}{dt} = -(\lambda + \mu_g^*)P_1(t) + \lambda a_1 P_0(t) + 2\mu_g^* P_2(t);$$

$$\frac{dP_2(t)}{dt} = -(\lambda + 2\mu_g^*)P_2(t) + \lambda \sum_{s=1}^{2} sa_s\, P_{2-s}(t) + 3\mu_g^* P_3(t);$$

……………………………………………………………………………

$$\frac{dP_i(t)}{dt} = -(\lambda + i\mu_g^*)P_i(t) + \lambda \sum_{s=1}^{i} sa_s\, P_{i-s}(t) + (i+1)\mu_g^* P_{i+1}(t); \qquad (4)$$

At $0 < i < h$

……………………………………………………………………………

$$\frac{dP_h(t)}{dt} = -(\lambda + n\mu_g^*)P_h(t) + \lambda \sum_{s=1}^{h} sa_s\, P_{h-s}(t) + (n\mu + (h+1)\eta)P_{h+1}(t);$$

……………………………………………………………………………………

$$\frac{dP_{h+1}(t)}{dt} = -(\lambda + h\mu_g^* + \eta)P_{h+1}(t) + \lambda \sum_{s=1}^{h+1} sa_s\, P_{(h+1)-s}(t) + (h\mu_g^* + 2\eta)P_{h+2}(t)$$

……….……………………………………………………………………………

$$\frac{dP_j(t)}{dt} = -(\lambda + h\mu_g^*(j-h)\eta)P_j(t) + \lambda\sum_{s=1}^{j} sa_s\, P_{j-s}(t) + (h\mu_g^* + (j-h+1)\eta)P_{j+1}(t)$$

At h < j < n

……….……………………………………………………………………………

$$\frac{dP_k(t)}{dt} = -(\lambda + n\mu_g^*)P_n(t) + \lambda\sum_{s=1}^{k} sa_s\, P_{n-s}(t) + (n\mu_g^* + \eta)P_{n+1}(t)$$

At k ≥ n.

The probability of intruders entering the object due to the fact that the guards do not have time to counter intruders can be calculated from the formula:

$$P_{int} = \frac{\eta\sum_{k=1}^{\infty} kP_k}{\lambda\sum_{k=1}^{\infty} ka_k} \tag{5}$$

The probability that the intruders will be neutralized will be:

$$P_{neut} = 1 - P_{int}. \tag{6}$$

We will consider the QS of the second type on the example of the queuing system M / E2 / n / m with restriction (η ≠ 0), without mutual assistance, with non-ordinary demands and a random number of demands in the group.

The system of differential equations of probabilities of states of these QS has the form:

$$\frac{dP_{00}(t)}{dt} = -\lambda P_{00}(t) + \mu_2^* P_{21}(t);$$

$$\frac{dP_{11}(t)}{dt} = -(\lambda + \mu_1^*)P_{11}(t) + \lambda a_1 P_{00}(t) + 2\mu_2^* P_{22}(t);$$

$$\frac{dP_{21}(t)}{dt} = -(\lambda + \mu_2^*)P_{21}(t) + \mu_1^* P_{11}(t);$$

$$\frac{dP_{12}(t)}{dt} = -(\lambda + 2\mu_1^*)P_{12}(t) + \lambda a_1 P_{11}(t) + 2\lambda a_2 P_{00}(t) + 3\mu_2^* P_{23}(t) + \lambda P_{21}(t);$$

$$\frac{dP_{22}(t)}{dt} = -(\lambda + 2\mu_2^*)P_{22}(t) + 2\mu_1^* P_{12}(t); \tag{7}$$

……….……………………………..…………………………………………

$$\frac{dP_{1k}(t)}{dt} = -(\lambda + k\mu_1^*)P_{1k}(t) + \lambda\sum_{s=1}^{k} sa_s P_{1(k-s)}(t) +$$

$$+[(k+1)\mu_2^* + \eta]P_{2(k+1)}(t) + \lambda P_{2(k-1)}(t)$$

$$\frac{dP_{2k}(t)}{dt} = -(\lambda + k\mu_2^*)P_{2k}(t) + k\mu_1^* P_{1k}(t);$$

At k = n

…………..……………………………………………………………...…

$$\frac{dP_{1k}(t)}{dt} = -(\lambda + \eta\mu_1^* + k\eta)P_{1k}(t) + \lambda\sum_{s=1}^{k} sa_s P_{1(k-s)}(t) + \lambda P_{2(k-1)}(t) +$$

$$+(\eta\mu_2^* + k\eta)P_{2(k+1)}$$

$$\frac{dP_{2k}(t)}{dt} = -(\lambda + n\mu_2^* + k\eta)P_{2k}(t) + (n\mu_1^* + k\eta)P_{1k}(t)$$

At k > n

The mathematical model of SMO M / E2 / n / m is considered in detail in [22].

The queuing system, which consists of QS of the first and second types, simulates a multi-stage counteraction to groups of attackers.

The probabilities of penetration and neutralization of attackers can be calculated from the formulas (5) and (6). A multistage counteraction QS structure is shown in Fig.1.

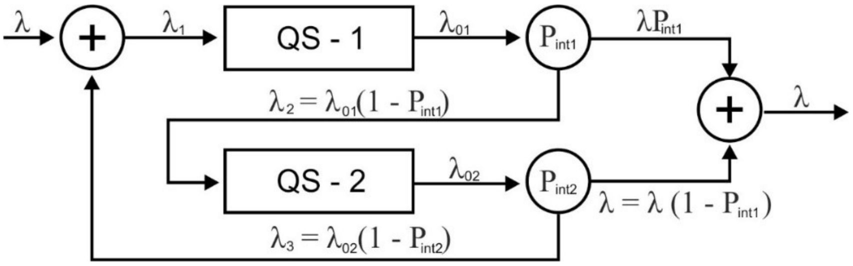

Figure 1: *Multistage counteraction QS*

The following equations will take place in stationary mode:

$\lambda 1 = \lambda 01$; $\lambda 2 = \lambda 02$;

$\lambda 2 = \lambda 01(1 - \mathrm{Pneut}) = \lambda(1 - \mathrm{Pneut1}) = \lambda \mathrm{Pint1}$; (8)

$\lambda 01 = \lambda 01(1 - \mathrm{Pneut1}) \cdot \mathrm{P}_{\mathrm{int2}}^{-1} = \lambda \mathrm{Pint1} \cdot \mathrm{P}_{\mathrm{int2}}^{-1}$;

$\lambda 2 = \lambda 02(1 - \mathrm{Pneut2}) = \lambda(1 - \mathrm{Pneut1})\ (1 - \mathrm{Pneut2}) \cdot \mathrm{P}_{\mathrm{neut2}}^{-1} = \lambda \mathrm{Pint1} \cdot \lambda \mathrm{Pint2} \cdot \mathrm{P}_{\mathrm{neut2}}^{-1}$

Conditions of QS stationary work:

$$\omega_1 = \frac{\lambda}{n_1(\mu_1 + \eta_1)} < 1;$$

$$\omega_2 = \frac{\lambda P_{\mathrm{int1}}}{n_2(\mu_2 + \eta_2)} < 1; \tag{9}$$

Total mathematical expectation of the demand staying in the QS:

$$\bar{t} = (\bar{t}_{QS1} + \bar{t}_{QS2}) P_{\mathrm{int2}}^{-1}.$$

Consider an example.

An object guarded by a three-person security unit (n = 3) is attacked by a group of intruders with a rate of $\lambda = 1$ [group / unit time]. Each group with a probability of as can have a different number of attackers. The distribution law of the number of malefactors in the group is uniform, i.e. with a probability of 0.2 in the group there can be 1,2,3,4 or 5 malefactors: a1 = a2 = a3 = a4 = a5 = 0.2. The time spent by intruders on the object $\bar{t}_{\mathrm{int}}$ is a limited random variable that is subject to the exponential law with the parameter $\eta = \frac{1}{\bar{t}_{\mathrm{int}}}$.

Intensity of counteraction by guards is $\mu = \frac{1}{\bar{t}_{\mathrm{gr}}}$ [malefactors neutralized by guard / unit of time].

It is necessary to determine the probability of neutralizing intruders/ malefactors by protecting the object at different ratios λ: μ: η.

Figure 2 shows the object protection QS for the example under consideration.

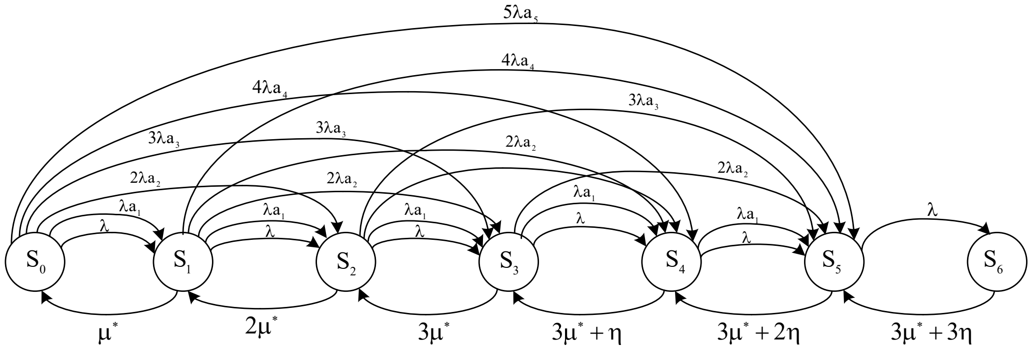

Figure 3: *Object protection QS for the example under consideration*

Kolmogorov's differential equations for the probabilities of the states of these QS will be:

$$\frac{dP_1(t)}{dt} = -\lambda P_0(t) + \mu^* P_1(t) \quad ;$$

$$\frac{dP_1(t)}{dt} = -(\lambda + \mu^*) P_1(t) + \lambda a_1 P_0(t) + 2\mu^* P_2(t) \quad ;$$

$$\frac{dP_2(t)}{dt} = -(\lambda + 2\mu + 2\eta) P_2(t) + \lambda a_1 P_1(t) + 2\lambda a_2 P_0(t) + 3\mu^* P_3(t) \quad ; \qquad (10)$$

$$\frac{dP_3(t)}{dt} = -(\lambda + 3\mu + 3\eta) P_3(t) + \lambda a_1 P_2(t) + 2\lambda a_2 P_1(t) + 3\lambda a_3 P_1(t) + 3\lambda a_3 P_0(t) + (3\mu + 4\eta) P_4(t)$$

$$\frac{dP_4(t)}{dt} = -(\lambda + 3\mu + 4\eta) P_4(t) + \lambda a_1 P_3(t) + 2\lambda a_2 P_2(t) + 3\lambda a_3 P_1(t) + 4\lambda a_4 P_0(t) + (3\mu + 5\eta) P_5(t)$$

$$\frac{dP_5(t)}{dt} = -(\lambda + 3\mu + 5\eta) P_5 + \lambda a_1 P_4(t) + 2\lambda a_2 P_3(t) + 3\lambda a_3 P_2(t) + 4\lambda a_4 P_1(t) + 5\lambda a_5 P_0(t) + (3\mu + 6\eta) P_6(t)$$

Normalizing condition $\sum_{k=0}^{6} = 1$;μ* = μ+η.

For stationary operating conditions of these QS, the linear equations have the form

$$0 = -\lambda P_0(t) + \mu^* P_1 \, ;$$

$$0 = -(\lambda + \mu^*) P_1 + \lambda a_1 P_0 + 2\mu^* P_2 \, ;$$

$$0 = -(\lambda + 2\mu^*) P_2 + \lambda a_1 P_1 + 2\lambda a_2 P_0 + 3\mu^* P_3 \, ;$$

(11)

$$0 = -(\lambda + 3\mu^*) P_3 + \lambda a_1 P_2 + 2\lambda a_2 P_1 + 3\lambda a_3 P_1 + 3\lambda a_3 P_0 + (3\mu^* + \eta) P_4 \, ;$$

$$0 = -(\lambda + 3\mu^* + \eta) P_4 + \lambda a_1 P_3 + 2\lambda a_2 P_2 + 3\lambda a_3 P_1 + 4\lambda a_4 P_0 + (3\mu^* + 2\eta) P_5 \, ;$$

$$0 = -(\lambda + 3\mu^* + 2\eta) P_5 + \lambda a_1 P_4 + 2\lambda a_2 P_3 + 3\lambda a_3 P_2 + 4\lambda a_4 P_1 + 5\lambda a_5 P_0 + (3\mu^* + 3\eta) P_6 \, .$$

The P_{ntr} probability was determined from formulas (5,6). Figure 3 shows the graph of the dependence of the P_{ntr} probability at different values of μ and η.

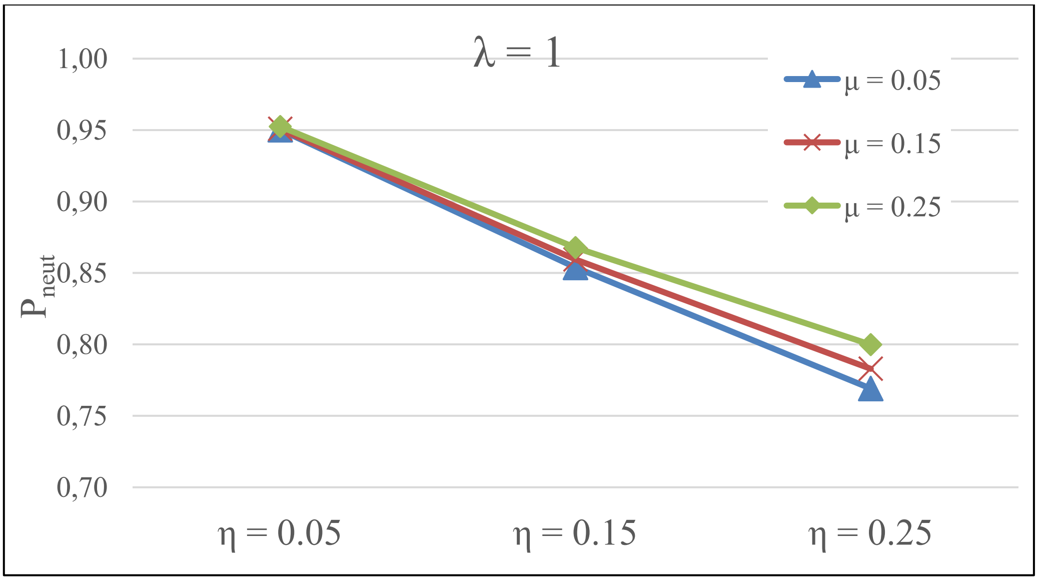

Figure 3: *Probability of attackers' neutralization against the counteraction intensity*

From Figure 3 it is seen that with increasing the counteraction intensity, the value of the P_{ntr} probability increases even with a decrease in the time spent by intruders on the protected object.

III. Conclusion

The use of models of protection of critical infrastructure from unauthorized interference acts will determine the rational ratios of the quantitative composition of security units, the intensity of countermeasures and concentration of additional security forces against the intensity of penetration of malicious groups with a random number of attackers, ensuring an acceptable probability of detection, prevention and neutralization of such groups.

References

[1] Shumov V.V. Models against terrorism: classification. Trudy ISA RAN. Vol 62, 3/2012, pp.106-115 (In Russian).

[2] Social Science for Counterterrorism. Putting the Pieces Together/Davis P.K., Cragin K., Editors. RAND Corporation, 2009.

[3] Wright P.D, Liberatore M.I., Nydick R.L, A Survey of Operations Reserch Models and Application in Homeland Security/Interfaces, 2006.V.36, №6, pp.514-529.

[4] Sullivan T.J., Perry W.L. Identifying indicators of chemical, biological, radiological and nuclear (CBRN) Weapons development activity in sub-national terrorist group/ J. Oper. Res. Soc. 2004, N 55 (4), PP. 361-374.

[5] Pate-Cornell E. Fusion of intelligence information: A Bayesian approach/ Risk Anal. 2002, N 22(3), pp. 445-454.

[6] Novikov D.A. Hierarchical models of military action/ Management of Large systems. Vol. 37. Moscow: Institute for Management Problems of Russian Academy of Sciences, 2012, C.25-62 (In Russian).

[7] Bachrach Y., Draief V., Goyal S. Security games with contagion/University of Cambridge, 2011.

[8] Bier V., Oliveros S., Samuelson L. Choosing what to protect: Strategic defensive allocation against an unknown attacker//Journal of Public Economic Theory, 2006, N9, pp. 1-25.

[9] Kiekintveld C., Tambe M., Marecki J. Robust Bayesian Methods for Stackelberg Security Games//Conference: Autonomous Agents & Multiage Systems/Agent Theories, Architectures and Languages – ATAL, pp. 1467-1468, 2010.

[10] Borovsky A.S., Tarasov A.D. An integrated approach to the development of a general model for the functioning of physical protection systems of objects // Trudy ISA RAN. Vol. 61. 1/2011, pp. 3-13 (In Russian).

[11] Dormidontov A.V., Mironova L.V., Mironov V.S. On the possibility of applying the countermeasures model to assessing the security level of transport infrastructure facilities // Naichny Vestnik MGTU. Vol 21, № 03, 2018, pp.67-77 (In Russian).

[12] Ginis L.A., Kolodenkova A.Ye. Fuzzy modeling to prevent risk situations at critical infrastructure facilities / Vestnik UGATU, Vol. 21, № 4(78), 2017, pp. 113-1120 (In Russian).

[13] Norkin V.I., Gaivoronsky A.A., Zaslavsky V.A., Knopov P.S. Optimal Resource Allocation Models for Critical Infrastructure Protection / Cybernetic I and System Analysis. Vol. 54 № 5, 2018, pp.13-26 (in Russian).

[14] Pita J., Jain M., Western C., Portway C., Tambe M., Ordonez F., Kraus S., Paruchuri P. Deployed ARMOR protection: The application of a games theoretic model for security at the

Los Angeles International Airport/In Proc. Of AAMAS,2008.

[15] Taylor M.E., Kiekintveld C., Western C., Tambe M. Beyond Runtimes and Optimality: Challenges and Opportunities in Evaluating Deployed Security Sistems/ In Proceeding of the AAMAS – 09 Workshop on Agent Design: Advancing from Practice to Theory, May 2009.

[16] Ryzhikov Yu.I. Simulation modeling. Theory and technology. S.-Petersburg: Korona Print, 2004, 384 p. (In Russian).

[17] Ryzhikov Yu.I. Calculation of service systems with group arrival of requests /Information and Control systems № 2. 2007, pp.39-49 (In Russian).

[18] Monsik V.B., Skrypnikov A.A., Fedotov A.Yu. Queuing systems for indivisible group claims with a queue of unlimited length / Nauchnyi Vestnik MGTU GA № 184, 2012, p. 108-112 (In Russian).

[19] Gnedenko B.V., Kovalenko I.N. Introduction to queuing theory. – Moscow: Nauka, 1987. – 336 p (In Russian).

[20] Shuenkin V.A., Donchenko V.S. Applied models of queuing theory. Kyiv: NMKVO, 1992, 398 p (In Russian).

[21] Ventsel E.S., Ovcharov L.A. The theory of stochastic processes and its engineering applications. – 2nd edition., Moscow: Vysshaya Shkola, 2000. — 383 p (In Russian).

[22] Katsman M. D., Mathematical models of ecologically hazardous rail traffic accidents / M. D. Katsman, V. K., Myronenko, V. I. Matsiuk // Reliability: theory&applications. – Vol. 10, № 1(36). – San Diego, USA – 2015. – P. 28–39.