УДК 004.621.3:519.816

S. Zybin

THE ONE METHOD TO DECISION MAKING SUPPORT FOR FORMATION OF COMPLEX SECURITY INFORMATION PROGRAMS

This article, written for analysis of a support decision-making approach. This approach can be used for the formation of complex information security programs, taking into account the threats and risks. This approach is based on the introduction of models and risks in the hierarchy of objective tasks and the goal evaluation of the tasks. Under the threat, we understand a condition of the environment, impacts the efficiency of the task. Complex goal-oriented program is executed in this environment. Risk is defined as a result of a random event that is caused by the influence of external relative factors. The event is a situation arises that affects the execution program. Threat models and risks have been proposed. The risk model is a risk factor, which is a random process and has a special goal. The threat is simulated by a special program, which is entered in the hierarchy of goals.

Keywords: security program, decision making, protection system, DSS, decision support system, evaluation, simulating, judgement.

Introduction

Problem solving of the state information security can be obtained with the use of decision support systems. Decision-making is a compulsory step in any purposeful activities. Thus in the conditions of limited resources of all kinds, and increase of activities is continuously increasing difficulty decisions that are made, and the requirements for their efficiency.

The complex program to ensure information security is a set of activities united by unity of global goals and shared resources [1, 2]. The main objectives of the complex program to ensure information security development is a selection of programs to be included in the complex program and the resources distribution between programs. This complex program to ensure information security usually can be scheduled for long intervals of time, so we need to evaluate the effectiveness of programs in a given time interval.

It is necessary to take into account the possibility of threats and risks during developing the complex program to ensure information security. Analyze their impact and on this basis provide for measures to counter them or eliminate them.

We need to solve the following problems in the formation of the complex program to ensure information security considering the threats and risks:

- we need to determine the quantitative characteristics influence of threats and risks to the effectiveness of the complex program to ensure information security;
- we need to identify quantitative rates of the performance program considering threats and risks;
- we need to divide resources between counter means of threats and risks, and programs with goal to increase information security.

Known methods for solving the first problem include the identification of risks. This is a qualitative analysis. And also provide the probability estimation and the size of the possible damage. This is a quantitative analysis [3, 4]. However, the problem of estimation program effectiveness into account of risk cannot be solved and remains at the discretion of the expert - the decision maker. Moreover, the definition of damage in absolute terms is often impossible for the complex program to ensure information security.

Main goal of the article

The goal consists in developing of the support decision-making approach for the formation of complex information security programs, taking into account the threats and risks. And also we should work out mathematical threat models and risks.

Main part

The problem solving method of evaluating the relative effectiveness considering threats and risks kindly develop on the basis of the methods to solve this problem without taking into account

these factors. The most common methods today got a multicriteria evaluation of programs [5]. The area of their application delimited by two conditions which must be satisfied by a specific task.

The first condition is the existence of multiple criteria, each of which can estimate a separate alternative.

The second condition is the ability of decision maker to evaluate in some way each alternative on separate criterion.

The first condition in the majority cases for the formation of complex programs do not performs because there are significant differences in the nature of the programs included in complex program. The second condition is very problematic, since the selection of the optimal alternative or ranking of a large number of variants requires taking into account of estimates for a large number of related criteria. This situation occurs when making decisions for the formation complex programs.

Therefore, methods of decision support during the formation information security programs considering threats and risks can be developed by modification of the evaluation variants goal-oriented methods [1, 2, 5]. The relative effectiveness of the programs should be evaluated as a time function, given at the planning interval [3]. Therefore, the possibility of taking into account the time factor in the evaluation of programs is fundamental for decision-making support tasks.

The main idea of the proposed approach to the analysis of threats and risks impact is that the events which cause threats or risks are considered as an integral part of the program. This means threats or risks are part of the external environment impact program. Therefore, these program-models of threats or risks are included in the hierarchy program objectives. [6] We link their links with other programs and objectives. Thus, each of the program-models of threats or risks has at least one goal or program, the achievement of which it has a direct impact. Following [6], we define such objectives direct above-goals program model threat or risk. The influence of the threat and / or risk, as well as other programs, evaluate the degree impact on the achievement of the main objectives of the program. The effectiveness of the program is estimated to provide on availability of threats and risks in view of their probability characteristics. Such approach makes it possible to divide resources to parry the threats and risks on a par with the dividing of resources to programs that make up their essence.

To implement the proposed approach is necessary to solve a series of specific problems. The first is associated with the development of mathematical models of threats and risks. It allows include events that cause the threat and/or risk, in hierarchy of objectives. The essence of the second problem is to develop a method of impact quantitative evaluation of the threat and/or risk. The next problem is following. We should find ways to evaluate the relative effectiveness of the program at the presence of threats and risks.

An analysis of threats can reveal certain properties that characterize this concept. Firstly, it should be noted that the threat is a consequence of the event which is the occurrence of the situation, that are affecting on the program execution. However, the threat is a result of the certain group activities of people. And the risk is mainly a result of a random event. Second, the intensity of the impact threat to the fulfillment of tasks is a random variable, which changes with the times.

A common feature of the "threat" and "risk" concepts is the impact of the environment on program execution and the fact that they are the result of its impact on program execution.

Based on the spent researches will formulate definitions.

Definition 1.

The threat is, affecting the task efficiency state of the environment in which the complex goal-oriented program is executed.

In addition, we can conclude about means neutralizing existence of the threats that have an impact on its level of risk.

From this follows the possibility of the threat model construction, which represents a certain task. And there is at least one task or goal, the level of achievement of which depends on the execution level of the threat task-model. Also, a treat task-model may be subtasks as other objects that affect its efficiency, i.e. action to neutralize the threat.

Thus, the threat model has all the properties of the problem with some features.

Defined in the relevant threat r_i a number $0 \le M_i \le 1$, which is called the degree of threat realization , with $M_i = 0$, in the absence of the influence of threats and $M_i = 1$ at its maximum possible impact. In addition, we will characterize the threat r_i by probability p_t of its realization in time *t*. This value should determine the experts by using group methods of expert estimation [2,8].

Definition 2.

Particular influence coefficient $\propto_{ij}$ of the threat r_i on achievement of its direct above-goal λ_j (task level execution P_j) are increasing the level achievement of the above-goal λ_j (task level execution P_j), which has turned out as a result of the full realization of r_i.

The article goes on, if this does not cause ambiguities, we will use the term "above-goal" to refer of goal. The treat task model direct influences the goal level achievement. And we will use the term task. This threat affects the level execution of the task.

We need to adequately describe the support task of decisions concerning complex goal planning. This should be done taking into account the threats and risks. To do this, it is advisable to take into account changes over time their effects. Proceeding from this shall speak about instantaneous values at time *t* influence coefficient $\propto_{ihk}(t)$ of the threat r_i to achievement it direct above-goal λ_h, which is defined by the following formula

$$\propto_{ih}(t) = \begin{cases} 0, if\ t < \tau_{ih}; \\ \beta(\propto_{ih}, t)\ othewise, \end{cases} \quad (1)$$

here $\propto_{ih}$ – the stationary value of the influence coefficient for the threat r_i on direct above-goal λ_h;

τ_{ih}– the expert evaluation of the threat impact delay r_i on above-goal λ_h;

β – the polynomial function, which describes the change in the threat impact coefficient along the time.

Since reliable information as to the accuracy of expert evaluations of the polynomial coefficients $\beta(\propto_{ih}, t)$ is missing, we define in the (1) $\beta(\propto_{ih}, t) = \propto_{ih}$. We will only take into account the threat impact delay on its direct above-goal. Experts define this value.

Stationary values of the influence coefficient $\propto_{ih} \in A_h, i = (1, n_h)$, direct sub-goal of the above-goal $\propto_h$, which can include threats satisfies the condition $\sum_{i=1}^{n_h} |\propto_{ih}| = 1$.

In general threat r_i is direct sub-goal of several above-goal λ_1, λ_2, …, λ_h, …, λ_z, and any above-goal λ_h has some set $\{\Lambda_h = \Lambda_{hk}\}$ of alternative subsets for compatible direct sub-goal, $\Lambda_{hk} \cap \Lambda_{hl} \neq \emptyset$, $k \neq l$. Therefore, there is a case when $\lambda_i \in \Lambda_{hk}$, $\lambda_i \in \Lambda_{hl}$, $k \neq l$ and the same threat r_i will have different stationary values $\propto_{ihk}$, $\propto_{ihl}$ of influence coefficient on the same of it direct above-goal λ, have been calculated for different alternative subsets Λ_{hk}, Λ_{hl}.

If achievement of the sub-goal λ_i is promote to achievement of the direct above-goal λ_h, then it stationary value of the influence coefficient is $\propto_{ihk} > 0$, otherwise $\propto_{ihk} < 0$. The concept content of threat is clear and therefore partial coefficients of problem influence, which are corresponding threat models, are negative. At the beginning of process, the definition of the stationary value of the influence coefficient for sub-goal hierarchy must transformed in such a way, that stationary values of the influence coefficient to all sub-goal were positive. This can achieve by replacing sub-goals, which adversely affect the corresponding above-goal, sub-goals, which are their logical inversions.

Now define the characteristics of the threat. The first characteristic that determines the type of threat is a way of conditions expression and consequences of its implementation. If the implementation conditions of the threat can express by result of the measurement for one, specific value of resource then such threat called quantitative by input, or threat is called qualitative by input.

Since the influence of treat task-model on achievement their direct above-goal is negative, then in the worst case level of their performance without compensating effects taken equal to 1. This resource is defined as a quantitative expression of the threat compensation conditions, which results that the level implementation of treat task-model will be zero. A task resource, which is a

model of the threat "attacks on information resources" is the sum of separate attacks on the various elements of these resources.

If the resource value of quantitative by input threat is known, such threat is quantitative by input certain. The resource value of such a threat is uniquely determined by experts when building a hierarchy of goals. If the value of its resource is unknown, then such threat is input threat quantitative by uncertain. For such threats are defined agreed generalized expert estimates of the resource value [1,8].

A treat task-model always is direct sub-goal some goal or objective. It is characterized by the result of its implementation. If the result of the full implementation of threat can be expressed by effect (the result of the measurement of one value), the threat is a quantitative by output, otherwise it is quality by output.

In determining the degree of achievement of above-goal should take into account the effects of the achievement only sets of compatible goals. Since threat operates independently from performers, it should be considered compatible with each of the sub-goal. Therefore, the treat task-model is included in each subset of the compatible sub-goal of above-goal towards which affects direct threat. Therefore, we can formulate the following definition.

Definition 3.

Direct sub-goal λ_i and λ_j, are including threats of some above-goal λ_s, called compatible, if the achievement of one does not exclude the feasibility of achievement another and there is incompatible in otherwise.

On the basis spent researches start creating a generalized threat model. The instant value $M_h(t)$ of degree threat implementation r_h at time *t* is defined as follows:

$$M_h(t) = \begin{cases} 0, if \ \sup\limits_k \sum\limits_i \propto_{ihk} (t) M_i(t) < \Pi_h; \\ \Pi_h, if \ \sup\limits_k \sum\limits_i \propto_{ihk} (t) M_i(t) = \Pi_h; \\ f\left(\sup\limits_k \sum\limits_i \propto_{ihk} (t) M_i(t)\right), if \ \Pi_h < \sup\limits_k \sum\limits_i \propto_{ihk} (t) M_i(t) < 1 - \sum\limits_q \left| \propto^{(-)}_{qhk} (t) \right|; \\ 1, if \ \left(1 - \sum\limits_q \left| \propto^{(-)}_{qhk} (t) \right|\right) \le \sup\limits_k \sum\limits_i \propto_{ihk} (t) M_i(t) \le 1, \end{cases} \quad (2)$$

here Π_h – the threat threshold r_h;

$f(\sup_k \sum_i \propto_{ihk} (t) M_i(t))$ – the function of degree threat implementation r_h;

k – the subset number Λ_{hk} of compatible direct sub-goals of the threat r_h;

i – the sub-goal number $\lambda_i \in \Lambda_{hk}$;

$\propto_{ihk} (t)$ – the instant value at time *t* of the partial sub-goal coefficient influence $\lambda_i \in \Lambda_{hk}$ to the threat achievement r_h, which calculated on condition, that the sub-goal λ_i is considered as a subset element Λ_{hk} of compatible direct sub-goals of the threat r_h;

$M_i(t)$ – the instant value of the degree achievement sub-goal λ_i at the time *t*;

$\propto^{(-)}_{qhk} (t)$ – the instant value at the time *t* of the partial sub-goal coefficient influence $\lambda_q \in \Lambda_{hk}$, which negatively affects the threat r_h.

Important special cases of threats are quasilinear threats and threshold threats.

The degree M_j of quasilinear execution of the treat task-model r_j is defined by the expression

$$M_j = \begin{cases} \sup\limits_h \sum\limits_s \propto_{sjh} M_{sjh}, if \ \sup\limits_h \sum\limits_s \propto_{sjh} M_{sjh} \leq 1; \\ 1, \qquad\qquad if \ \sup\limits_h \sum\limits_s \propto_{sjh} M_{sjh} > 1, \end{cases}$$

here h – the subset number Λ_{jh} of compatible direct sub-goal of the treat task-model r_j;
s – the sub-goal number $\lambda_{sjh} \in \Lambda_{jh}$;
$\propto_{sjh}$ – the particular influence coefficient of sub-goal $\lambda_{sjh} \in \Lambda_{jh}$ on threat achievement r_j.

The expression for calculation M_j of the threshold achievement degree of the threat r_j is following

$$M_j = \begin{cases} 1, if \ \sup\limits_h \sum\limits_s \propto_{sjh} M_{sjh} \geq \left| 1 - \sum\limits_{j \in J_i^-} \propto_j \right|; \\ 0, otherwise; \end{cases}$$

here J_i^- – set of sub-goal threat numbers r_j with a negative impact.

Now we proceed to the development of the risk model. The concept of the risk is characterized by uncertainty, related to the possibility of adverse situations and their consequences problems during the implementation [3, 4]. In other words, a risk should be understood consequence of the random event that is caused by external factors to the program. This event is an arise situation which affects the program execution. The risk is the result of a random event that is to take place, or not. Thus, depending on is whether the developer optimistic or pessimistic, the essence of an event that causes the risk can be formulated as following way. In one case, such that its occurrence would cause a negative impact on the program execution, or such that it will have a positive impact.

Depending on the nature of events which cause a risk we are distinguished: a technical, technological, political, economic, military, financial and environmental risks, risks of force majeure and specific risks [4, 9]. Here the same event can cause risks which have very different effects on execution. The risks need to be evaluated on the basis of a systematic approach, taking into account the goals and its structures.

We introduce the definition of some concepts.

Definition 4.

The risk factor ψ for program P called the process ξ_ψ, that $\exists\, p_i \in P[V(p_i)\xi_\psi(t) \neq V(p_i)\neg\xi_\psi(t)]$, here $V(p_i)\xi_\psi(t) \neq V(p_i)\neg\xi_\psi(t)$ – it is objective relative efficiency (for program) $p_i \in P$ taking into account the risk factor $\xi_\psi(t)$ and without taking into account.

Definition 5.

The indicator risk ψ called fictitious goal λ_ψ, a single sub-goal of which is a risk factor ψ.

A risk factor is a sub-goal for the risk indicators such as λ_{ψ_1} and λ_{ψ_2}. Sub-goals λ_{ψ_1} and λ_{ψ_2} are risk indicators, which fully described by degree achievement functions.

In the general case the instantaneous value $M_h(t)$ of sub-goal direct achievement λ_h at the time *t* defines by the expression (2).

When you set goal function to achieve risk-indicator function, you need to consider the following features:

- since goal thresholds satisfy [10] $0 \leq \Pi_h \leq 1$, then the value of a random process $\xi_\psi(t)$, which determines the risk factor ψ, must satisfy the condition $0 \leq \xi_\psi(t) \leq 1$, also;

- if $\left[\partial M(\lambda_{\psi_1})/\partial\xi_{\psi}(t)\right] < 0$, as a risk factor for the purpose of λ_{ψ_i}, is an indicator of this risk, we must choose $\left[1-\xi_{\psi}(t)\right]$ instead $\xi_{\psi}(t)$.

Conclusions

The support decision-making approach proposes in this article. This approach can be used for the formation of complex information security programs, taking into account the threats and risks. Under the threat, we understand a condition of the environment, impacts the efficiency of the task. Complex goal-oriented program is executed in this environment. Risk is defined as a result of a random event that is caused by the influence of external relative factors. The event is a situation arises that affects the execution program. Threat models and risks have been proposed.

References

1. Тоценко В.Г. Методы и системы поддержки принятия решений. Алгоритмический аспект. / Тоценко В.Г. – К: Наукова думка, 2002. – 382 с.
2. Орловский С.А. Проблемы принятия решений при нечёткой исходной информации. / Орловский В.Г. – М: Наука, 1981. – 208 с.
3. Згуровский М.З. Информационный подход к анализу и управлению проектными рисками. / Згуровский М.З., Коваленко Н.И., Кондрак К., Кондрак Э. // Проблемы управления и информатики. – № 4, 200, с. 148-156.
4. Грачёва М.В. Анализ проектных рисков. / Грачёва М.В. Учебное пособие для вузов. – М.: ЗАО "Финстатинформ", 1999, – 216 с.
5. R.L. Keeney and H. Raiffa. Decisions with multiple objectives: Preferences and value tradeoffs. J. Wiley, New York, 1976.
6. Руа Б. Проблемы и методы принятия решений в задачах со многими целевыми функциями // Вопросы анализа и процедуры принятия решений. М.: Мир, 1976. – С. 20 – 58.
7. Катренко А. В. Теорія прийняття рішень: підручник з грифом МОН / Катренко А. В., Пасічник В. В., Пасько В. П. – К.: Видавнича група BHV, 2009. – 448 с.: ил.
8. **Saaty,** T. L. (2008) **"Decision making with the analytic hierarchy process"**, Int. J. Services. Sciences, Vol. 1, No. 1, pp.83–98.
9. Макаров И.М., Виноградская Т.М., Рубчинский А.А., Соколов В.Б. Теория выбора и принятия решений. – М: Наука, 1982. – 328 с.
10. Зибін С.В., Хорошко В.О. Оцінка якості функціонування комплексних систем технічного захисту й систем підтримки ухвалення рішення в їхньому складі. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2 (24), 2012 р. – С. 7-15.

Надійшла 28.02.2017 р. Рецензент: д.т.н., проф. Бурячок В.Л.