УДК 004.056.5

Nachev A., Zhelezov St.

ASSESSING THE EFFICIENCY OF INFORMATION PROTECTION SYSTEMS IN THE COMPUTER SYSTEMS AND NETWORKS

Анотація:

Особливості систем захисту інформації в комп'ютерних системах та мережах вимагають розробки нетривіальних методів для їх аналізу та оцінки. Спроби рішення в цій області наведено в даній статті.

Ключові слова: *комп'ютерні системи і технології, модель, інформаційна безпека.*

Аннотация:

Особенности систем защиты информации в компьютерных системах и сетях требуют разработки нетривиальных методов для их анализа и оценки. Попытки решения в этой области приведены в этой статье.

Ключевые слова: *компьютерные системы и технологии, модель, информационная безопасность.*

Abstract: *The specific features of the information protection systems in the computer systems and networks require the development of non-trivial methods for their analysis and assessment. Attempts for solutions in this area are given in this paper.*

Key words: *Computer Systems and Technologies, Model, Information security.*

Introduction

Information protection systems in computers and networks are characterized by specific features [5], which imposes the need for the development and use of particular methods for their analysis and assessment [4]. An attempt to solve a problem of a similar nature is made in this paper by proposing suitable mathematical models that allow to determine the impact of losses from possible threats and to assess the effectiveness of information protection systems.

A generalized model for determining the loss in a computer system (network) from the impact of possible threats

Let the computer network in the particular operating conditions is endangered by n threats. The amount m_i, $i=\overline{1,n}$ arising threats of $i-$th type for a certain period of operation of the computer network (operating cycle) is a random variable with an exponential law of distribution with parameter λ_i.

The occurrence of $i-$th, $i=\overline{1,n}$, threat leads to losses z_i.

With the total number of n threats the relative share of $i-$th, $i=\overline{1,n}$, threat will be set through $\frac{m_i}{n}, i=\overline{1,n}$. With the independence in the emergence of threats and additivity of their effects it will cause relative losses to the aggregate losses from the impact of all threats amounting to $\frac{m_i}{n}\Delta z_i, i=\overline{1,n}$. Therefore, the aggregate losses from the occurrence of all n threats will

be $\bar{З} = \sum_{i=1}^{n} \frac{m_i}{n} \Delta z_i$. The ratio $\frac{m_i}{n}$ represents the probability p_i that with the occurrence of a threat, it will prove to be of $i-$ th type.

Given the defined initial conditions the amount m_i of arising threats of $i-$ th type, $i = \overline{1,n}$, the time of operation (operating cycle) will be determined by the formula:

$$m_i = \lambda_i T_{цф}. \tag{1.1}$$

For the same time the total amount of occurring n type threats $\sum_{i=1}^{n} m_i$ will be:

$$\sum_{i=1}^{n} m_i = \sum_{i=1}^{n} \lambda_i T_{цф} = T_{цф} \sum_{i=1}^{n} \lambda_i . \tag{1.2}$$

The probability p_i, that if a threat arises it will be of $i-$th type, $i = \overline{1,n}$, will be defined as follows:

$$p_i = \frac{\lambda_i T_{цф}}{T_{цф} \sum_{i=1}^{n} \lambda_i} = \frac{\lambda_i}{\sum_{i=1}^{n} \lambda_i}. \tag{1.3}$$

Losses caused by the $i-$th threat are difficult to be defined in absolute terms, as the economic losses, losses of time, the volume of data destroyed etc. do not defy an objective preliminary estimate in such a format. It is therefore appropriate to use estimates of relative losses resulting from the investigation held in the assumption that all threats to the computer network (system) represent a complete set of events, i.e.:

$$0 \le \Delta z_i \le 1; \qquad \sum_{i=1}^{n} \Delta z_i = 1.$$

The losses Δw_i, that arise with the occurrence of the $i-$th threat will be defined in compliance with the probability of its occurrence, i.e.

$$\Delta w_i = p_i z_i, \tag{1.4}$$

where z_i represents the relative losses, caused by the $i-$ th threat.

The total losses caused by the occurrence of all the n threats in terms of their independence and additivity of their effects will be defined as:

$$\bar{З} = \sum_{i=1}^{n} \Delta w_i .$$

Given (1.3) and (1.4) we will finally obtain:

$$\bar{З} = \frac{1}{\sum_{i=1}^{n} \lambda_i} \sum_{i=1}^{n} \lambda_i z_i . \tag{1.5}$$

The assessment of the losses, caused by any threat is proposed to be carried on the basis of the investigation held as follows [1, 2]:

A group of N experts assess the extent of possible losses arising from each of the n threats. The degree of risk is defined in relative units, as all threats to the computer network (system) represent a complete set of events, i.e. the following condition is being fulfilled:

The assessment of the $j-$th, $j=\overline{1,N}$, for the $i-$th threat is ζ_{ij}. If the experts are of the same or similar level of qualification

$$z_i = \frac{\sum_{j=1}^{N} z_{ij}}{N}. \tag{1.6}$$

The degree of convergence of the opinions of experts with big enough N is being assessed through the dispersion D_i, defined as:

$$D_i = \frac{1}{N}\sum_{j=1}^{N}\left(z_{ij} - z_i\right)^2, \tag{1.7}$$

which determines a standard deviation

$$\sigma_i = \sqrt{\frac{1}{N}\sum_{j=1}^{N} z\left(z_{ij} - z_i\right)^2} \tag{1.8}$$

Provided that the experts have varying degrees of competence the weight k_j, $0 \le k_j \le 1$, $j=\overline{1,N}$ is being introduced to each one of them. In this case, the expression (1.6) will take the following form:

$$z_i = \frac{\sum_{j=1}^{N} z_{ij} k_j}{\sum_{j=1}^{N} k_j}. \tag{1.9}$$

Accordingly, for the standard deviation of ζ_i we will get:

$$\sigma_i = \sqrt{\frac{1}{\sum_{j-1}^{N} k_j}\sum_{j=1}^{N}\left(z_{ij} - z_i\right)^2 k_j} \tag{1.10}$$

Let us consider a case when for the losses caused by every threat every expert gives three estimates: optimistic, pessimistic and the most probable. We shall denote by γ, $\gamma=\overline{1,3}$ the type of assessment, and by α_γ the weight of the assessment with number γ. Then the expert assessment q_i will be determined as [1,2]:

$$z_i = \frac{\sum_{j=1}^{N} \frac{\sum_{\gamma=1}^{m} z_{ij\gamma}\alpha_\gamma}{\sum_{\gamma_1}^{m} \alpha_\gamma}}{\sum_{j=1}^{N} k_j} \tag{1.11}$$

Let us mark with α_1 the weight of the pessimistic, with α_2 the weight of the most probable and with α_3 the weight of the optimistic assessment. Then the expert assessment for ζ_i, according to (1.11) will be:

$$z_i = \frac{\sum_{j=1}^{N} \frac{z_{ij1_1}\alpha_1 + z_{ij2}\alpha_2 + z_{ij3}\alpha_3}{\alpha_1 + \alpha_2 + \alpha_3} k_j}{\sum_{j=1}^{N} k_j}. \tag{1.12}$$

The degree of convergence of the assessments of the experts will be determined as [1,2]:

$$\sigma_i = \sqrt{\frac{\sum_{j=1}^{N} \sigma_{ij}^2 k_j}{\sum_{j=1}^{N} k_j} + \frac{\sum_{j=1}^{N} \left(q_{ij} - q_i\right)^2 k_j}{\sum_{j=1}^{N} k_j}}, \tag{1.13}$$

where:

$$\sigma_{ij}^2 = \frac{\left(z_{ij3} - z_{ij1}\right)^2}{\alpha_4} \tag{1.14}$$

$$z_{ij} = \frac{\sum_{\gamma=1}^{3} z_{ij\gamma}\alpha_\gamma}{\sum_{\gamma=1}^{3} \alpha_\gamma} \tag{1.15}$$

The expression (1.15) is the expert assessment of the losses caused by the occurrence of the $i-$th threat given by $j-$th expert. In (1.14) α_4 expresses the degree of uncertainty of the $j-$th expert. It is recommended [1, 2, 3] to use $\alpha_1 = 1$; $\alpha_2 = 4$; $\alpha_3 = 1$, $\alpha_4 = 36$.

A generalized model for determining the degree of effectiveness of an information protection system

In the event of an $i-$th threat its effects are being avoided by a P_{ni} probability, $i = \overline{1,n}$. Accordingly, the probability that losses will be overcome will be equal to $P_i = 1 - P_{ni}$.

We shall mark by p_i the probability of occurrence of an $i-$th threat.

Obviously, in the foregoing circumstances, the losses $\overline{W}_i$ from the impact of the $i-$th threat can be presented as:

$$\overline{W_i} = p_i z_i (1 - P_{ni}), \quad (2.1)$$

With independence of the occurrence and the impact of threats and in case of additivity of their effects, in view of (2.1) for the overall effects of the impact of threats to the computer system (network) the following will be obtained:

$$\overline{W} = \sum_{i=1}^{n} \overline{W} = \sum_{i=1}^{n} p_i z_i (1 - P_{ni}). \quad (2.2)$$

According to (1.4) the product $p_i z_i$ presents the losses that occur as a result of threats of $i-$th type, i.e. $\Delta w_i = p_i z_i$ where p_i is defined by (1.3). Then:

$$\overline{W} = \sum_{i=1}^{n} \overline{W} = \sum_{i=1}^{n} \Delta w_i (1 - P_{ni}). \quad (2.3)$$

To assess the effectiveness of the system for protection the index *protection coefficient* will be introduced:

$$K = \frac{\overline{3}}{\overline{W}}. \quad (2.4)$$

The same shows how many times the impact of threats to information security in computer systems and networks has been limited with the application of appropriate protective measures.

Given (1.4), (1.5), (2.3) the expression (2.4) can be presented in the following generalized form:

$$K = \frac{\overline{3}}{\overline{W}} = \frac{\sum_{i=1}^{n} \Delta w_i}{\sum_{i=1}^{n} \Delta w_i (1 - P_{ni})} = \frac{\sum_{i=1}^{n} p_i z_{ini}}{\sum_{i=1}^{n} p_i z_i (1 - P_{ni})}. \quad (2.5)$$

The probability to avoid the consequences from the arising threats will depend on how much is taken of all factors, qualitative and quantitative requirements for the information protection system in the computer systems and networks in their design. In other words, if x_{ij} is the extent of the implementation of the $j-$th requirement to the information protection system regarding the $i-$ th threat, the probability P_{ni} in removing the effects of the $i-$th threat can, in general, be presented by the function

$$P_{ni} = f_i (x_{i1,} x_{i2}, x_{i3}, ..., x_{ij,.....} x_{ik}), \quad (2.6)$$

where k is the amount of measures taken to prevent the consequences in case of an $i-$th threat.

To determine the probability P_{ni}, $i=\overline{1,n}$ the methodology given in [4] will be used. In this connection, let there be m requirements to the information protection system of the computer system (network) of which k are quantitative and $m-k$ are qualitative. To assess the degree of fulfillment of the $j-$ th, $j=\overline{1,k}$ quantitative requirement for the information protection system in relation to the $i-$th effect its normed meaning will be used $\overline{x_{ij}}$, $j=\overline{1,k}$, $0 \le x_{ij} < 1$. For norming the function of this type will be used:

$$\overline{x_{ij}} = \frac{x_{ij} - x_{ij}^{нл}}{x_{il}^{нд} - x_{u}^{нл}}, \tag{2.7}$$

where x_{ij} - the current meaning of the $j-$th requirement to prevent the impact of the $i-$th threat; $x_{ij}^{нд}$ and $x_{ij}^{нл}$ respectively the best and the worst meaning of the $j-$th requirement to prevent the impact of the $i-$th threat.

Based on (2.7) we have the following estimate ratios:

$$\overline{x_{ij}} = \frac{x_{ij} - x_{ij\ \min}}{x_{ij\max} - x_{u\ \min}} \text{ with } x_{ij}^{nd} = x_{ij\max};\ x_{ij}^{нл} = x_{ij\min}, \tag{2.8}$$

$$\overline{x_{ij}} = \frac{x_{ij\max} - x_{ij}}{x_{ij\max} - x_{u\ \min}} \text{ with } x_{ij}^{nd} = x_{ij\min};\ x_{ij}^{нл} = x_{ij\max}, \tag{2.9}$$

$$\overline{x_{ij}} = 0 \text{ with } x_{ij} < x_{ij\max};\ x_{ij} > x_{ij\min} \tag{2.10}$$

$$\overline{x_{ij}} = 1 \text{ with } x_{ij} = x_{ij\,opt} \tag{2.11}$$

$$\overline{x_{ij}} = \frac{x_{ij} - x_{ij\ \min}}{x_{ij\,opt} - x_{u\ \min}} \text{ with } x_{ij\min} \le x_{ij} \le x_{ij\,opt} \tag{2.12}$$

$$\overline{x_{ij}} = \frac{x_{ij\max} - x_{ij}}{x_{ij\max} - x_{ij\,opt}} \text{ with } x_{ij\,opt} \le x_{ij} \le x_{ij\max} \tag{2.13}$$

With decomposition of the function (2.6) in MacLoren's order and taking into account the first members of the order the following is obtained [4]:

$$P_{ni} = P_{ni}(0) + \sum_{i=1}^{m} \frac{\partial P_{ni}}{\partial x_{ij}} x_{ij}, \tag{2.14}$$

where $P_{ni}(0)$ is the probability to prevent the $i-$th threat when there is no fulfillment of the requirements and the information protection system.

The quantity $\frac{\partial P_{ni}}{\partial x_{ij}} = \beta_{ij}$ characterizes the degree of impact of the $j-$th requirement on the probability for eliminating the $i-$th threat; $0 \le \beta_{ij} \le 1$; $\sum_{j=1}^{m} \beta_{ij} = 1$ for $i = \overline{1,n}$. Then:

$$P_{ni} = \sum_{j=1}^{k} \beta_{ij} \overline{x_{ij}} + \sum_{j=k+1}^{m} \beta_{ij} \mu(x_{ij}). \tag{2.15}$$

In view of (2.15) the expression (2.3) will get the following final form:

$$\overline{W} = \sum_{i=1}^{n} \overline{W} = \sum_{i=1}^{n} p_i z_i \left\{ 1 - \left[\sum_{j=1}^{k} \beta_{ij} \overline{x_{ij}} + \sum_{j=k+1}^{m} \beta_{ij} \mu(x_{ij}) \right] \right\}. \tag{2.16}$$

Conclusions and future work

The proposed mathematical apparatus can be considered as a basis for further searches within the scope of the problem of protecting information in computer systems and networks. Besides the theoretical aspect, it would be useful in assessing the effectiveness of designed and actually operated systems.

Literature:

1. Стоянов А. Анализ и обработка на експертна информация от проведено изследване за диагностика на дизелова горивна уредба / А. Стоянов, Г. Кръстев // Научни трудове на Русенски университет. – 2008. – Том 47, Серия 4. – С. 71–74.

2. Евланов Л. Г. Теория и практика принятия решений / Л.Г. Евланов. – М.: Экономика, 1994. – 176 с.

3. Макаров И. Теория выбора и принятия решений / Макаров И., М. Виноградская, Н. Рубчинский, В. Соколов. – М.: Наука, 2002. – 330 с.

4. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты / В.В. Домарев. – М., СПб., Киев: Dia Soft, 2002. – 688 с.

5. Станев Ст. Компютърна и мрежова сигурност /С. Станев, С. Железов. – Шумен: Университетско издателство „Епископ Константин Преславски”, 2005. – 324 с.