AVERAGE RISK APPLICATION FOR THE SECURITY LEVEL ESTIMATION OF INFORMATION ASSETS

Alexander Arkhipov, Sofia Arkhipova

National Technical University of Ukraine "KPI", Pobeda street, 37, Kiev, 03056, Ukraine,
ph.: (044) 241-86-55, E-mail: sonet@zeos.net

Annotation

The subject of this article is the opportunity of average risk probability-theoretic method use at the information risk analysis during the security investigation of information systems. The expressions, which allowed quantity indicators calculating of efficiency and protection systems' security against set of threats, are received.

Introduction

The application of information risk methodology is considered to be traditional effective at various stages of the tasks decision concerned with a construction, attending and the analysis of information safety systems functioning, estimation of the information security level provided with them [1,3]. Information risks are used more often for essential threats extraction and factors investigation, which promotes their realization, also for the efficiency estimation stage of possible construction variants of information security systems (ISS) and selection the best of them.

The trivial formula of risk estimation for essential threats selection is:

$$R_t = P_t q\,, \tag{1}$$

where P_t - the probability of threat realization t, and q - the damage caused by this realization. But for the efficiency estimation of ISS and provided with them information security level the presence of an integrated risk estimation from possible realization of threats set $T = \{t_i\}, i = \overline{1,N}$ is required before and after ISS construction. The procedure of a similar integrated estimation reception has not finally generated yet, nevertheless the average risk method is supposed to be perspective for solving this task. We will consider some features of average risk determination during ISS analysis.

Features of average risk calculation on sets of attacks and vulnerabilities

Let's assume, that realization of threat t is in a full measure possible as a result of successful realization of any attacks formed final set $A = \{a_j\}, j = \overline{1,N}$. We define the risk of attack through the so-called three-factorial formula [1]:

$$R_{aj} = p_t p_{vj} q = p_{aj} q, \tag{2}$$

where p_t – the probability of threat originating, p_{vj} - the probability of vulnerabilities appearance v_j, causing an opportunity of the attack organization a_j, successful realization probability of which is $p_{aj} = p_t p_{vj}$. We believe also, that each of attacks is based on the appropriate vulnerability $v_j \in V = \{v_1,...,v_N\}$, in other words between elements of sets A and V exists mutual conformity. In this case the risk of threat realization t should correspond to the integrated risk estimation of separate attacks realizations. We research an opportunity of total risk functional application [1] (in [4] - common risk) that is often recommended for a presence of an integrated estimation:

$$R'_t = \sum_{j=1}^{N} R_{aj} = q p_t \sum_{j=1}^{N} p_{vj} = q p_t p_{\Sigma v}\,. \tag{3}$$

From comparison of formulas (1) and (3) follows, that value $p_{\Sigma v}$ should have probabilistic character, in particular $0 \le p_{\Sigma v} \le 1$. However, taking into account, that it is fair the condition for each probability of vulnerability appearance $0 \le p_{\Sigma v} \le 1,\ j = \overline{1,n}$. As a whole the inequality is fair for $p_{\Sigma v}$:

$$0 \le p_{\Sigma v} \le N\,, \tag{4}$$

that is value $p_{\Sigma v}$ generally does not correspond to the requirements showed to probabilistic measure, particularly, it may take the values essentially exceeding 1. Therefore, product $p_t p_{\Sigma v}$ in expression (3) is not probabilistic characteristic of threat t, and functional R'_t cannot be considered as risk in the standard understanding of this term.

It is known from the statistical decisions theory that generalizing characteristic of the system risk correctly integrating in its elements private risks is the average risk [5]. The expression for average risk calculated at finite discrete set of private risk coincides structurally with the sum on the left part of the expression (3). However it is necessary to take into account that average risk functional is under construction for the events forming full group [5]. The set of attacks A has not this property because the requirement of paired events incompatibility is not carried out for them:

$$a_k \cap a_j \neq 0 \text{ when } a_k, a_j \in A, k \neq j, \tag{5}$$

and the requirement of completeness is not carried out too(the set of attacks does not include the event of any attacks absence). Examine average risk finding caused by an opportunity of threat successful realization t by using private risks of attacks. It is necessary transform the initial set of attacks A so that set À* made from the complex attacks A forming full group of events [6]. For this purpose we shall implement concept of event $\overline{a_j}$, opposite to attack a_j, which occurrence probability is $p(\overline{a_j}) = 1 - p_{aj}$, and sets $\overline{A} = \{\overline{a_j}\}, j = \overline{1, N}$. Then set of complex attacks is $A^* = \{\alpha_1, ..., \alpha_g, ..., \alpha_L\}$, representing all possible combinations C_{2n}^n, made from elements of integrated set $A \cup \overline{A}$, forms full group of events that is not joint among themselves in pairs. The expression for full group of events probabilities is:

$$\sum_{l=1}^{L} p(\alpha_l) = 1. \tag{6}$$

Representation about complex attacks structure (that has quite real practical realization) can be received by having reproducing some of them description through the elements of attacks initial set A and its additions $\overline{A}$. For example:

$$\alpha_1 = a_1 \cap a_2 \cap ... \cap a_N -$$

it is crossing of all events formed set A (i.e. joint all set of attacks realization),

$$\alpha_2 = a_1 \cap a_2 \cap ... \cap \overline{a_N},\ \alpha_3 = a_1 \cap a_2 \cap ... \cap a_{N-1} \cap a_N, ..., ,$$
$$\alpha_1 = a_1 \cap a_2 \cap a_3 \cap ... \cap \overline{a_{N-2}} \cap \overline{a_{N-1}} \cap \overline{a_N}, ...,\ \alpha_l = \overline{a_1} \cap \overline{a_2} \cap ... \cap \overline{a_N}.$$

Probabilities of complex attacks realization are defined by quite obvious formulas following directly from structures of the appropriate attacks:

$$\left.\begin{aligned} p(\alpha_1) &= p(a_1)p(a_2)...p(a_N) = \prod_{j=1}^{N} p_{aj}, \\ p(\alpha_2) &= (1 - p_{aN}) \prod_{j=1}^{N-1} p_{aj}, \\ p(\alpha_l) &= p_{a1} p_{a2} p_{a3} ... (1 - p_{a(N-2)})(1 - p_{a(N-1)})(1 - p_{aN}), \\ p(\alpha_L) &= \prod_{j=1}^{N} (1 - p_{aj}) = 1 - \sum_{l=1}^{L} p(\alpha_l). \end{aligned}\right\} \tag{7}$$

Some complexities originate in estimation of the damage which is the result of successful end of the appropriate complex attack [6]. However in this specific situation damage from realization of the first $L-1$ attacks is equaled q, and last - 0, i.e. actually we have set of attacks $A^* = \{\alpha_1, ..., \alpha_{l-1}\}$. The average risk described probable damage, originating in case of successful realization of threat t, will make in a result:

$$R_t = \sum_{l-1}^{L-1} R(\alpha_l) = q\sum_{l-1}^{L-1} p(\alpha_l) = q(1-p(\alpha_L)) = q(1-\prod_{j=1}^{N}(1-p_{aj})) = qP_t. \quad (8)$$

It is received for the three-factorial formula of risk in view of the formula (2):

$$R_t = q(1-p_t^N\prod_{j=1}^{N}(p_t^{-1}-p_{vj})), \quad (9)$$

where probability of threat realization t according to the expression (1) is:

$$P_t = 1-p_t^N\prod_{j=1}^{N}(p_t^{-1}-p_{vj}). \quad (10)$$

Thus depending on a detailed elaboration degree of knowledge about the threats and factors inducing these threats probability P_t may be defined both at the attacks level (through attacks probabilities p_{aj}, $j=\overline{1,N}$, the right part of the expression (9)) and at the vulnerability level (expression (10)).

Risk estimation at the threats level, calculation of ISS security and efficiency

There is a necessity for construction and estimations comparison of the generalized possible damage from threats set *T* before and after ISS construction in the presence of information about possible threats elements of set *T* representing real danger to an information assets, in particular, for couples $(q_{i,}P_{ti})$, determining damage from threat realization t_i and its realization probability P_{ti}. Application of the average risk apparatus is rather perspective at this stage [6], however it also demands reformatting of the threats initial set forming full group. Taking into account that usual lists of typical threats contain tens and even hundreds positions, the reformatting procedure of initial threats sets may turn out to be extremely difficult. In order to prevent this trouble it is expedient to take advantage of such threats classification which is formed only insignificant quantity of so-called base threats. In particular, base threats may be threats of availability *t1*, integrities *t2* and confidentiality *t3*. Separation of attacks (or vulnerability) should be executed in appropriate way, result of which becomes extraction of the three pointed threats. Then the set is formed from *23* complex threats as it was already described above for a level of attacks (vulnerability):

$$\tau_1 = t_1 \cap t_2 \cap t_3,\ \tau_2 = t_1 \cap t_2 \cap \overline{t_3},\ \tau_3 = t_1 \cap \overline{t_2} \cap t_3, \_, \tau_7 = \overline{t_1} \cap \overline{t_2} \cap t_3,\ \tau_8 = \overline{t_1} \cap \overline{t_2} \cap \overline{t_3},$$

And the last complex threat is only formally one. For each complex threat is calculated realization probabilities according to its structure $P_m = P(\tau_m), m = \overline{1,8}$:

$$P_1 = P(\tau_1) = P_{t1}P_{t2}P_{t3},\ P_2 = P(\tau_2) = P_{t1}P_{t2}(1-P_{t3}),\ P_3 = P(\tau_3) = P_{t1}(1-P_{t2})P_{t3}, \_,$$

$$P_7 = (1-P_{t1})(1-P_{t2})P_{t3},\ P_8 = \prod_{i=1}^{3}(1-P_{ti}) = 1-\sum_{m=1}^{7}P_m.$$

Besides damages values are estimated in case of successful threats realization in the assumption of threats consequences additivity [6,7]. For example, we have for previewed threats: $q(\tau_1) = q_1+q_2+q_3$, $q(\tau_2) = q_1+q_2$, $q(\tau_3) = q_1+q_3, \_, q(\tau_7) = q_3$, $q(\tau_8) = 0$. The average risk is received from possible realization of threats set T = $\{t_1, t_2, t_3\}$ as a result:

$$R_T = \sum_{m=1}^{7} q_m P_m. \quad (11)$$

Forming and consummation either of ISS variants involves probability variation of all levels, precisely reduction of these probabilities to some residual level (signed with the subscript "0"): $\{p_{vj0}\}$, $\{p_{aj0}\}$, $j=\overline{1,N}$, $\{P_{ti0}\}$, $i=\overline{1,N}$. The residual average risks R_{t0}, R_{T0} correspond to the residual probabilities. Knowledge about the residual risks allows to estimate the security level provided with either of ISS variants and

to give efficiency quantitative estimation of these variants. In particular, it is possible to use the next parameter as a parameter of security:

$$PR = (R_T - R_{T0}) / R_T = 1 - R_{T0} / R_T , \quad (12)$$

which limiting value equal 1 is achieved at the absolute information security (in this case $R_{T0} = 0$ theoretically), and minimal value is equal 0 (protection is absent, $R_T = R_{T0}$).

Efficiency of protection variants in view of expenses C on the ISS construction and service can be estimated with such parameter:

$$E = (R_T - R_{T0} - C) / C = (R_T - R_{T0} 0 / C - 1 . \quad (13)$$

Based on the formula (13) the most effective ISS will be such one that provides a maximum of the prevented damage per unit cost, caused by ISS construction and its service for the certain time interval.

Conclusions

Application of the private risks sum, caused by realization of each attack separately (so-called total risk) as an integrated risk estimation of attacks (threats) generally gives incorrect results using information assets for securities estimation of information systems.

Way out is application of the average risk probability-theoretic scheme for reception of information risk integrated estimation, giving the strict decision of this task.

Bibliography:

[1] Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. М.: Компания Ай Ти; ДМК Пресс, 2004. - 348с.
[2] Симонов С.В. Методология анализа рисков в информационных системах// Конфидент. Защита информации. - №2. – 2001. – с. 48-53.
[3] Петренко С.А., Петренко А.А. Аудит безопасности Intranet. – М.: ДМК Пресс, 2002. – 416с.
[4] Воробиенко П., Нечипорук О., Щербина Ю. Принципы построения модели угроз информационным ресурсам систем и сетей связи // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Вип. 7 – К.: 2003. – с. 11-13.
[5] Пугачев В.С. Теория вероятности и математическая статистика. – М.: Наука, 1979. – 496с.
[6] Архипов О.Є., Касперський І.П. Застосування методології передбачення для оцінювання шкоди, заподіяної витоком секретної інформації // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Вип. 2(15) – К.: 2007. – с. 13-19.