ITHEA

International Journal INFORMATION MODELS & ANALYSES

2015 Volume 4 Number 4

International Journal
INFORMATION MODELS & ANALYSES
Volume 4 / 2015, Number 4

IJ IMA is official publisher of the scientific papers of the members of the ITHEA® International Scientific Society

IJ IMA rules for preparing the manuscripts are compulsory.
The **rules for the papers** for ITHEA International Journals are given on www.ithea.org .
The camera-ready copy of the paper should be received by ITHEA® Submission system http://ij.ithea.org .
Responsibility for papers published in IJ IMA belongs to authors.

International Journal "INFORMATION MODELS AND ANALYSES" Volume 4, Number 4, 2015

Edited by the **Institute of Information Theories and Applications FOI ITHEA**, Bulgaria, in collaboration with
Institute of Mathematics and Informatics, BAS, Bulgaria,
V.M.Glushkov Institute of Cybernetics of NAS, Ukraine,
National Aviation University, Ukraine
Universidad Politechnika de Madrid, Spain,
Hasselt University, Belgium
Institute of Informatics Problems of the RAS, Russia,
St. Petersburg Institute of Informatics, RAS, Russia
Institute for Informatics and Automation Problems, NAS of the Republic of Armenia,

Publisher: **ITHEA®**

Sofia, 1000, P.O.B. 775, Bulgaria. www.ithea.org, e-mail: info@foibg.com
Technical editor: **Ina Markova**

Printed in Bulgaria

ISSN 1314-6416 (printed) **ISSN 1314-6432 (Online)**

RISK BEHAVIOUR IN A SET OF INTERVAL ALTERNATIVES

Gennady Shepelev

Abstract: *Problem comparing alternatives under interval uncertainty is studied. It is assumed that the compared alternatives have indicators of quality in the form of interval estimates. It is shown that mentioned problem cannot be unambiguously resolved by purely mathematical methods and requires using of decision maker's preferences. From two possible situations of comparing, situation of unique choice and situation of repeated one, the first situation, which is typical for problems of forecasting, is analyzed. Quantitative measure of plausibility of implementation for tested hypothesis about preference of an alternative in comparison with others in their set and measure of risk connected with possible falsity of such hypothesis are introduced. It is shown that this risk is increased with increasing number of compared alternatives. Some methods to calculate risks as well as procedure of decision-making in the framework of a set of alternatives are proposed.*

Keywords: *comparing interval alternatives, dependence of the risk on number of alternatives, probability logic in comparing interval alternatives, methods and procedures of decision-making for the problem.*

ACM Classification Keywords: *H.1.2 Human information processing. G3 Distribution functions. I.2.3 Uncertainty, "fuzzy", and probabilistic reasoning.*

Introduction and motivation

Many important problems are analyzed under uncertainty. First of all these are problems of forecasting when experts have to deal with estimates of the future values of the problem parameters and indicators. In most practical cases these quantities are measured in numerical scales and have, due to uncertainty, interval representations. Such interval estimates are given quite often by experts or are received as resultants of some models with interval input data. Certain interval indicators may play a role of comparison criteria for choice problems if it is necessary to choose some objects (alternatives) from their set. We will call alternatives with interval values of comparison criteria (or, synonymous, interval quality indicators) interval alternatives.

These choice problems cannot be exhaustively solved by purely mathematical methods. Indeed, if there is a non-zero intersection of compared intervals generally impossible definitively to conclude in a choice

process on superiority of an interval alternative over the others in their set. Any alternative may be “better” in the future, at the time of “removal” of uncertainty, when the interval estimates are replaced by exact (point) values of comparison criteria. Therefore at the time of the comparison can be judged only on the chances that one alternative will be preferable to others. It means that the problem comparing interval alternatives is a decision-making problem demanding including preferences of decision makers (DM) or experts in the process of decision-making. It should be emphasized that even after the selection of an alternative, which seems preferable at the moment of decision-making; always there is a risk that in the future any other alternative will be actually better. This is an essential feature of such problems. Therefore formal methods of comparison serve in this case only as a means of information-analytical support for the decision making process and cannot guarantee choice of truly the best alternative. Thus comparison criteria become in fact measure of preference.

So we suppose that all alternatives are comparable in preference (system of alternatives is full) and at the moment of choice a disjunction containing alternatives is not a strict disjunction (XOR), when the only alternative is choose as preferable. The choice of a preferred alternative depends now on the chances of its preference among the members of the disjunction. Such preference relations can be called relations involve risks or relations based on the degree of assurance in the truth of a testable hypothesis of preference. Apparatus of distribution functions has been selected here for quantification of preference chances for compared interval alternatives and the associated risks. Then the problem may be studied in the framework of probability logic [Nilsson, 1986] when besides truth and falsity analyzed logic expressions (opinions, assertions) may have in-between values of truth interpreted as chances of truth of the expressions.

It seems that the tool of distribution functions is the most familiar to experts-practitioners. This is important because expert analysis of practical problems is most productive if it is carried out on professional language that is familiar to experts, with using methods and terminology that are conventional for them. Thus knowledge concerning uncertainty is expressed in the framework of distribution functions approach just as in probability theory (but, that is typical for the many problems of expert analysis, beyond the frequency concept of probability).

To permit experts describe their knowledge concerning uncertainty of values within the interval estimates arbitrary distribution functions will be used. This is contrary to the view of some researchers [Diligensky, 2004] who believe that only uniform distributions are permitted on the “true” intervals. But if one take this concept, operations of interval analysis, to which is necessary to resort when working with models, become in fact impossible. Indeed, it was shown in [Sternin, 2011] that the distribution of the difference (sum) of two uniform distributions would be trapezoidal distribution. Thus applying already the simplest arithmetic operations to the initial intervals with uniform distributions on them does not allow

recognizing the results of such operations as “true” interval if we take the requirement of equality of chances of implementation for all values in it (Gibbs – Jaynes’ principle) as mandatory. If an expert would like nonetheless use only uniform distributions but express own knowledge more accurately he/she can switch to a class of generalized interval estimates [Chugunov et al, 2008] and resort to generalized uniform distributions [Sternin, 2010].

There are two main types of decision-making problems: problems of the unique and problems of the repeated choice. Each of these types of problems has specific comparison criteria. Note that situation of unique choice is typical for problems of forecasting.

Two approaches are usually used in the evaluating preference of interval alternatives and associated risks. In the framework of the first approach compared alternatives are considered as isolated, unconnected objects. Value of preference criterion is calculated for each of these alternatives and then, regardless of this indicator, one or the other risk indicator is calculated. To compare alternatives and choose preferred object the alternatives are evaluated on these two criteria. In spite of the fact that many problems of interval comparing belong to the class of unique choice as indicators of preference in this approach are often used averages of corresponding chance distributions (mathematical expectations), which are rather adequate to problems of repeated choice. Such indicators as variance, left and right semi variances, the mean absolute semi deviation and others [Ogryczak, 1999; Baker, 2015] are used as risk indicators in this approach. We draw attention to the fact that the values of the comparison criteria in this approach does not depend on the number of alternatives in their given set.

In the framework of the second approach compared alternatives are considered as an interconnected integrity. It is seems that this approach is more in line with features of the problems of unique choice. Risk selecting an alternative as preferred one in their set depends here firstly on the relative location of the compared intervals (configuration of compared alternatives) and then on their amount in the set. The presence of the group of mutually influencing alternatives increases the risk of making the wrong decision when choosing a preferred alternative. This is due to a “collective effect” just as it happens, for example, in condensed matter physics when properties of condensed matter systems composed of interacting components significantly differ from properties of more or less independent parts [Halperin, 2010].

Dimensionless chances of truth of tested by expert hypothesis concerning preference of an analyzed alternative relative to others are comparison criteria within this approach. Chances of truth of the opposite hypothesis, which complement the first chances up to unity, serve as a measure of risk. In this approach point implementations of different alternatives from analyzed set are considered as independent and priori all the alternatives have equal rights with respect to the choice.

Slightly specify that will be understood further at risk. In accordance with the standard (ISO/FDIS 31000:2009) risk is defined as “the effect of uncertainty on the achieved goals”. More narrowly risk is a characteristic of decision-making situation, which has the uncertainty of the outcomes and what is more the presence of adverse effects is the obligatory condition. Thus the concept of risk is a combination of chances and consequences of adverse events. However consequences are specific to each particular decision-making problem and on the type and on the size but the chances is one of the universal characteristics of risk. As rule consequences are dimensional values, chances are dimensionless.

For these reasons chances of preference as the selection criterion will be used in the paper. Corresponding risks will be estimated on based of these chances.

The start step in the realization of this approach is pairwise comparing alternatives, when the number of objects to be compared and its impact on risk do not take into account [Shepelev, 2013; 2014]. Criterion of comparison of interval alternatives with arbitrary distributions of chances, which was called “assurance factor”, was proposed on this way. It is equal to the difference between chances of the truth of tested hypothesis on preference of an alternative in their set and the chances of the truth of the opposite hypothesis. Numerical (for arbitrary distributions of chance) and analytical (for uniform and triangular distributions) methods calculating the assurance factor as well as decision-making procedure based on this criterion were proposed. The assurance factor and chances of preference are equivalent as comparison criteria. The first of them is more convenient in some cases. For example, for some simple distributions of chances one may establish a relation between such criteria as the difference of the averages for two compared alternatives and assurance factor [Shepelev, 2013; 2014] and their dissimilarity in other cases. Questions about depending of the risk of making right and wrong decisions on the number of comparable alternatives and calculation of corresponding chances remained however not studied. Earlier this subject was touched in paper [Diligensky, 2004]; here we look at it in more detail.

General statements for estimating of risk in a group of interval alternatives

Suppose that there are K alternatives I_i, i = 1, 2,…, K with the same interval quality indicators. Let dimensionless quantity $C(I_i \succ (I_1, I_2,.., I_{i-1}, I_{i+1},…, I_K))$ is the chances, in other words degree of assurance, in the truth of a testable hypothesis of preference, that the alternative I_i is more preferable than all at once alternatives (I_1, I_2,.., I_{i-1}, I_{i+1},…, I_K) from initially given their set (I_i is “better” of others “on the whole”). The term “all at once” means here that

$$I_i \succ (I_1, I_2,.., I_{i-1}, I_{i+1},\ldots, I_K) \equiv (I_i \succ I_1) \wedge (I_i \succ I_2) \wedge (I_i \succ I_3) \wedge \ldots \wedge (I_i \succ I_{i+1}) \wedge \ldots \wedge (I_i \succ I_K).$$

where $\equiv$ and $\wedge$ are symbols of equivalence and conjunction respectively. It is clear on sense that

$$0 \le C(I_i \succ (I_1, I_2,\ldots, I_{i-1}, I_{i+1},\ldots, I_K)) \le 1.$$

Risk that I_i would not in reality preferred will be measured by means of dimensionless quantity $R_s(I_i \succ (I_1, I_2,.., I_{i-1}, I_{i+1},\ldots, I_K))$ complementing previous chances to unity so that

$$Rs(I_i \succ (I_1, I_2,.., I_{i-1}, I_{i+1},\ldots, I_K)) = 1 - C(I_i \succ (I_1, I_2,.., I_{i-1}, I_{i+1},\ldots, I_K)).$$

As can be seen $R_s(I_i \succ (I_1, I_2,.., I_{i-1}, I_{i+1},\ldots, I_K))$ is degree of assurance in the truth of a hypothesis, which is opposite to the testable hypothesis of preference.

One may see that the following statement is true (T):

$$(I_i \succ (I_1, I_2,.., I_{i-1}, I_{i+1},\ldots, I_K)) \vee \neg (I_i \succ (I_1, I_2,.., I_{i-1}, I_{i+1},\ldots, I_K)) = T,$$

where $\neg$ is symbol of negation. Then corresponding chances

$$C(I_1 \succ (I_2, I_3,\ldots, I_K)) + C(\neg (I_i \succ (I_1, I_2,.., I_{i-1}, I_{i+1},\ldots, I_K))) = 1$$

and $Rs(I_i \succ (I_1, I_2,.., I_{i-1}, I_{i+1},\ldots, I_K)) = C(\neg (I_i \succ (I_1, I_2,.., I_{i-1}, I_{i+1},\ldots, I_K)))$.

The statement $\neg I_i \succ (I_1, I_2,.., I_{i-1}, I_{i+1},\ldots, I_K))$ means that at least one alternative from their compared set would be preferable than I_i. Let illustrate the meaning of introduced in this way the measure of risk for case of three alternatives. Here we have the following possible preferences and chains of disjunctions:

$((I_1 \succ I_2 \succ I_3) \vee (I_1 \succ I_3 \succ I_2)) \vee ((I_2 \succ I_1 \succ I_3) \vee (I_2 \succ I_3 \succ I_1)) \vee ((I_3 \succ I_1 \succ I_2) \vee ((I_3 \succ I_1 \succ I_2)) \equiv (I_1 \succ (I_2, I_3)) \vee (I_2 \succ (I_1, I_3)) \vee (I_3 \succ (I_1, I_2))$ or $Rs(I_1 \succ (I_2, I_3)) = C(I_2 \succ (I_1, I_3)) + C(I_3 \succ (I_1, I_2))$.

Analogically for K alternatives

$C(I_1 \succ (I_2, I_3,\ldots, I_K)) + C(I_2 \succ (I_1, I_3,\ldots, I_K)) + C(I_3 \succ (I_1, I_2, I_4,\ldots, I_K)) +\ldots+ C(I_K \succ (I_1, I_2,\ldots, I_{K-1})) = 1$

Hence

$Rs(I_1 \succ (I_2, I_3,\ldots, I_K)) = C(I_2 \succ (I_1, I_3,\ldots, I_K)) + C(I_3 \succ (I_1, I_2, I_4,\ldots, I_K)) +\ldots+ C(I_K \succ (I_1, I_2,\ldots, I_{K-1}))$.

One can see now that $C(I_i \succ (I_1, I_2,.., I_{i-1}, I_{i+1},\ldots, I_K))$ is monotonically non-increasing function of K, that is the chances that a certain alternative would be preferable in comparison with all the others do not increase with increasing number of the alternatives. Indeed, if the number of compared alternatives is increased the number of non-negative terms in the unit sum of corresponding chances is also increased. Therefore

$$C(I_i \succ (I_1, I_2,\ldots, I_{i-1}, I_{i+1},\ldots, I_K)) \le C(I_i \succ (I_1, I_2,\ldots, I_{i-1}, I_{i+1},\ldots, I_{K-1})), \quad (1A)$$

that proves monotonic non-increasing of chances. Then corresponding risk will be monotonically non-decreasing function of number of compared alternatives:

$$Rs(I_i \succ (I_1, I_2,\ldots, I_{i-1}, I_{i+1},\ldots, I_{K-1})) \le Rs(I_i \succ (I_1, I_2,\ldots, I_{i-1}, I_{i+1},\ldots, I_K)). \quad (1B)$$

By another words the more of number of the alternatives the more risk of wrong decision-making.

The fact of increasing overall risk with increasing number of alternatives is clearly demonstrated by the following equation:

$Rs(I_1 \succ (I_2, I_3,\ldots, I_K)) + Rs(I_2 \succ (I_1, I_3,\ldots, I_K)) + Rs(I_3 \succ (I_1, I_2, I_4,\ldots, I_K)) +\ldots+ Rs(I_K \succ (I_1, I_2,\ldots, I_{K-1})) = K - 1$.

The relationship (1A) takes place for chances of all possible exceptions of one interval estimation I_i from their set $(I_1, I_2,.., I_{i-1}, I_{i+1},\ldots, I_K)$. Therefore the chances $C(I_i \succ (I_1, I_2,.., I_{i-1}, I_{i+1},\ldots, I_K))$ is not more than minimal chances, which may occur in the right side of (1A) and, respectively, $R_s(I_i \succ (I_1, I_2,.., I_{i-1}, I_{i+1},\ldots, I_K))$ is not less than other risks, which may occur in the left side of (1B) after exception of some interval estimations.

Numerical method calculating chances and risks in a group of interval alternatives

Chances of preference for an alternative with arbitrary distributions on compared intervals can be calculated by the method of statistical testing. To be specific, situations of comparison will be analyzed when greater value of quality indicator corresponds to more preferred state and the hypothesis is tested that the first interval from their set with Q representatives is more preferable than others.

Let i_{lr} is point implementation of interval I_l in the r-th trial of Monte Carlo (l = 1, 2,.., Q; r = 1, 2,…, S). If S independent tests for each of the compared intervals was made and S_f is the number of tests for which $i_{1r} > \text{MAX}(i_{2r},\ldots, i_{Qr})$, then S_f/S is an estimate for $C(I_1 \succ (I_2,\ldots, I_Q))$. This numerical method is applicable to any distributions on compared intervals when we cannot receive analytical formula as well as in the case of a large number of compared alternatives with simple distributions when obtained, in principle, analytical formula are difficult foreseeable.

Among simple distributions commonly used in practice should be noted uniform, triangular and trapezoidal distributions. Random numbers N_x for these distributions with density $f_x(z)$ used in the method of statistical testing can be obtained by the inverse function method from the standard random number N_u for uniform distribution defined on the interval [0, 1]. In accordance with this method $N_u = \int_L^{N_x} f_x(z)dz$. This integral can be taken for mentioned simple distributions.

We have for a uniform distribution on the interval [L, R]:

$$f_E(z) = 1/(R - L),\ N_E = (1 - N_u)L + N_uR.$$

For triangular distribution

$$f_t(z) = \frac{2}{R-L}\begin{cases}\dfrac{z-L}{M-L},\ L \le z \le M,\\ \dfrac{R-z}{R-M},\ M < z \le R\end{cases}$$

where M is a mode of the distribution, and

$$N_t = \begin{cases} L + \left[N_u (R-L)(M-L)\right]^{1/2}, \; N_u \le (M-L)/(R-L), \\ R - \left[(1-N_u)(R-M)(R-L)\right]^{1/2}, \; N_u > (M-L)/(R-L). \end{cases}$$

For trapezoidal distribution

$$f_T(z) = \frac{2}{S} \begin{cases} \dfrac{z-L}{M_1-L}, & L \le z \le M_1, \\ 1, & M_1 < z < M_2, \\ \dfrac{R-z}{R-M_2}, & M_2 \le z \le R \end{cases}$$

where $S = R + M_2 - M_1 - L$ and M_1 и M_2 are the left and right vertices of the distribution respectively. Then

$$N_T = \begin{cases} L + \left[N_u S (M_1 - L)\right]^{1/2}, \; N_u \le (M_1 - L)/S, \\ (N_u S + M_1 + L)/2, \; (M_1 - L)/S < N_u < (2M_2 - M_1 - L)/S, \\ R - \left[(1-N_u)(R-M_2)S\right]^{1/2}, \; N_u > (2M_2 - M_1 - L)/S. \end{cases}$$

Although numerical methods allow calculating the chances and risks involved in the specific problems considered here, only analytical methods make it possible to obtain more general conclusions. Let us consider firstly case of several coinciding interval alternatives and obtain analytical expressions for this case for the simplest distributions of chances.

Risk behavior in a set of coincided interval alternatives

Assume for simplicity that distributions in the compared interval alternatives are uniform distributions. Assume also that all alternatives at the number of K are represented by coinciding intervals. Illustrations of general statements, which were formulated above, will be in this case the brightest. It can be seen that for two coinciding intervals $C(I_1 \succ I_2) = \dfrac{1}{D} \int_L^R f_2(x_2) \int_{x_2}^R f_1(x_1) dx_1 dx_2$, where $f_i(x_i)$ are corresponding

densities, $x_i \in I_i$ are current values in corresponding intervals and D is normalization factor. Then for uniform distributions we have: $C(I_1 \succ I_2) = \frac{1}{(R-L)^2}\int_L^R dx_2 \int_{x_2}^R dx_1$ = ½.

For three intervals

$$C(I_1 \succ (I_2, I_3)) = \frac{1}{(R-L)^3}[\int_L^R dx_3 \int_{x_3}^R dx_2 \int_{x_2}^R dx_1 + \int_L^R dx_2 \int_{x_2}^R dx_3 \int_{x_3}^R dx_1].$$

Here the first term corresponds to the current values of variables for which $x_2 > x_3$ and the second term to the situations when $x_3 > x_2$. This gives $C(I_1 \succ (I_2, I_3)) = 1/3$. For K intervals we have (K – 1)(K – 2)···1 of integral summands, which reflect all possible relations (<, >) between current values of variables. Ultimately $C(I_1 \succ (I_2, I_3,\ldots, I_K)) = 1/K$ and risk associated with the adoption of the initial hypothesis is 1 — 1/K.

One can see that if for the situation when two interval alternatives appear to be equivalent at the moment of comparison chances of right choice of preferred alternative equals risk of wrong choice then for a larger number of alternatives this risk increases rapidly. It can think that it is not a property of uniformity of distributions but property of equivalence of alternatives. To test this hypothesis we consider the case of triangular distributions.

The formula for calculating chances becomes more complicated in the case of a triangular distribution. The reason for this is rooted in the presence of two branches in the density of chances distribution for triangular distribution: left branch f_l, which lies on the left from value of mode, and right branch f_r on the right from mode. Let M_1, M_2 are modes of corresponding distributions and $M_2 \le M_1$ and we want to estimate chances $C(I_2 \succ I_1)$. These chances are the sum of four integrals C_i as may see on region of integration, which is represented here by square on the (X_1, X_2) plane:

$$C_1 = \int_L^{M_2} f_{1l}(x_1) \int_{x_1}^{M_2} f_{2l}(x_2) dx_1 dx_2, C_2 = \int_L^{M_2} f_{1l}(x_1) \int_{M_2}^{R} f_{2r}(x_2) dx_1 dx_2, C_3 = \int_{M_2}^{M_1} f_{1l}(x_1) \int_{x_1}^{R} f_{2r}(x_2) dx_1 dx_2,$$

$$C_4 = \int_{M_1}^{R} f_{1r}(x_1) \int_{x_1}^{R} f_{2r}(x_2) dx_1 dx_2.\ C(I_2 \succ I_1) = \frac{M_2 - L}{2(M_1 - L)} + \frac{(R-M_2)^3 - (R-M_1)^3}{6(M_1 - L)(R-M_2)(R-L)}.$$

.

Hence for $M_2 = M_1$ we have $Rs(I_1 \succ I_2) = C(I_2 \succ I_1) = ½$. The same result was obtained in the paper [Shepelev, 2014] by another method. Thus under equality of the two modes of triangular distributions defined on coinciding pair of intervals, when interval estimates are equivalent, risk $Rs(I_1 \succ I_2) = ½$ exactly as was for the case of uniform distributions. If the modes are not equal to each other risks (and chances) are more or less than ½ depending on location of modes. So compared alternatives are equivalent if their distributions of chances (not necessarily uniform) are the same and the same are their supports. Thus the same knowledges about interval alternatives resulting in their equivalence generate the highest risk during choice of the best alternative.

Chances and risks for such defined equivalent alternatives behave like for the uniform distributions i.e. the chances of preference fall hyperbolically with increasing of number K of alternatives and risk equals $1 - 1/K$. This is confirmed by numerical method calculations. Analytical relations for the chances of preference become rather cumbersome when the number of alternatives is more than two already for triangular distributions.

The case of other configurations

Besides the configuration of coinciding estimates for the two comparable alternatives there are, up to a permutation of alternatives in their pair, else two non-trivial configurations, i.e. configurations with non-zero intersections of intervals. It is configuration of the right shift when $L_2 < L_1 < R_2 < R_1$ and configuration of imbedded intervals when $L_1 < L_2 < R_2 < R_1$.

For these configurations and uniform distributions to receive relations for the preference chances and corresponding risks is convenient to use a method based on simple geometric considerations. For configuration of the right shift in the framework of complete system of events it is easier to distinguish events favoring the truth of the hypothesis $I_2 \succ I_1$ (size of risk for hypothesis $I_1 \succ I_2$). These are events when point implementations lie in the region $(i_1 \in [L_1, R_2]) \cap (i_2 \in [L_1, R_2])$, $i_1 \in I_1$, $i_2 \in I_2$. However some of these events at the same time are also favorable for the truth of hypothesis $I_1 \succ I_2$. Exactly half of the events favor each of these hypotheses in the case of uniform distributions on compared intervals as we can see above. This is not so in the case of other distributions. Then, for uniform distributions on the compared intervals,

$$C(I_2 \succ I_1) = Rs(I_1 \succ I_2) = (R_2 - L_1)^2/(2\Delta I_1 \Delta I_2),\ \Delta I_i = R_i - L_i,$$

and

$$C(I_1 \succ I_2) = 1 - \frac{(R_2 - L_1)^2}{2\Delta I_1 \Delta I_2}.$$

It's easy to see that the closer I_1 to I_2 and R_1 to R_2 the closer the risk to ½. For two intervals this value of the risk is maximal for configuration of the right shift. Indeed, the more R_1 the less the risk (at constant L_1 and L_2); the more L_1 the less the risk (at constant R_1 and R_2). Therefore this configuration is favorable for the preference of I_1.

Triangular distributions cases are somewhat more complicated because of the different possible positions of the modes. Let $\Delta I_1 > \Delta I_2$, $L_2 < L_1 < R_2 < R_1$ (right shift) and $M_2 < L_1$, $M_1 > R_2$ (the simplest configuration). The range of permissible point implementations in the (X_1, X_2) plane is a rectangle elongated to the right and its part, which corresponds area $X_2 > X_1$, lies above and on the left from line segment $X_2 = X_1$ with boundary points (L_1, L_1) and (R_2, R_2). Hence

$$C(I_2 \succ I_1) = Rs(I_1 \succ I_2) = \int_{L_1}^{R_2} f_{1l}(x_1) \int_{x_1}^{R_2} f_{2r}(x_2) dx_1 dx_2 = \frac{(R_2 - L_1)^4}{6\Delta_1 \Delta_2 (R_2 - M_2)(M_1 - L_1)}.$$

Small, at first glance, changes of locations of distributions modes greatly complicate the formula for risk. So, when $L_1 < M_2 < M_1 < R_2$ (other things being equal), $Rs(I_1 \succ I_2) = C_1 + \ldots + C_4$,

$$C_1 = \int_{L_1}^{M_2} f_{1l}(x_1) \int_{x_1}^{M_2} f_{2l}(x_2) dx_1 dx_2, \; C_2 = \int_{L_1}^{M_2} f_{1l}(x_1) \int_{M_2}^{R_2} f_{2r}(x_2) dx_1 dx_2,$$
$$C_3 = \int_{M_2}^{M_1} f_{1l}(x_1) \int_{x_1}^{R_2} f_{2r}(x_2) dx_1 dx_2, \; C_4 = \int_{M_1}^{R_2} f_{1r}(x_1) \int_{x_1}^{R_2} f_{2r}(x_2) dx_1 dx_2.$$

Taking these integrals is not difficult; the resulting formulas allow us to establish the following. Choice of the type of distribution, which is distinct from uniform one, results in increasing of demands to the knowledge of experts. So in a situation of right shift under choice of triangular distributions expert should has in mind that for the same values of modes that lie at the area of intersection of interval estimates risk is practically unchanged with the displacement modes in this area. For example, for I_1= [10, 20], I_2 = [9, 19] $Rs(I_1 \succ I_2)$ = 0.42; $C(I_1 \succ I_2)$ = 0.58 for all equal values of modes ($M_1 = M_2$) from 11 to 18. Interestingly, that selecting uniform distributions practically does not change the results: $Rs(I_1 \succ I_2)$ = 0.4; $C(I_1 \succ I_2)$ = 0.6. (But the risk is slightly reduced). At the same time for M_1= 18, M_2 = 16 $Rs(I_1 \succ I_2)$ = 0.33; $C(I_1 \succ I_2)$ = 0.67. Thus the specification of chance distributions on compared alternatives

requires high qualification of the expert and elaborating special procedures for working an expert with probability distributions on interval estimates.

If one from distributions is uniform it is easy to obtain formulas for the risk by the method used here or to use the relations obtained earlier in [Shepelev, 2014]. General conclusion in both cases is that, ceteris paribus, the more the value of mode in I_1 in general (and in comparison with the mode in I_2 for triangle distribution there) the less risk of making a wrong decision on the preference of the first alternative.

For case of embedded intervals events that are favorable to the truth of the hypothesis $I_1 \succ I_2$ are $\{(i_1 \in [R_2, R_1]) \cap (i_2 \in [L_2, R_2])\} \cup \{(i_1 \in [L_2, R_2]) \cap (i_2 \in [L_2, R_2])\}$. Hence, for uniform distributions,

$$R(I_1 \succ I_2) = 1 - \frac{R_1 - L_2}{\Delta I_1} + \frac{\Delta I_2}{2\Delta I_1},\ L_1 < L_2 < R_2 < R_1.$$

Further we will need the formula for the same configuration when $L_2 < L_1 < R_1 < R_2$:

$$R(I_1 \succ I_2) = 1 - \frac{L_1 - L_2}{\Delta I_2} - \frac{\Delta I_1}{2\Delta I_2}.$$

The case of triangular distributions is technically similar here to the case of right shift.

Set of possible configurations is considerably richer for three compared intervals. We will consider only one of them, for which $L_2 < L_1 < L_3 < R_2 < R_3 < R_1$, as an example. Subset of the complete system of events favoring the truth of the hypothesis $I_1 \succ (I_2, I_3)$, is as follows:

$\{(i_1 \in [R_3, R_1]) \cap (i_2 \in [L_2, R_2]) \cap (i_3 \in [L_3, R_3])\} \cup \{(i_1 \in [R_2, R_3]) \cap (i_2 \in [L_2, R_2]) \cap (i_3 \in [R_2, R_3])\} \cup \{(i_1 \in [R_2, R_3]) \cap (i_2 \in [L_2, R_2]) \cap (i_3 \in [L_3, R_2])\} \cup \{(i_1 \in [L_3, R_2]) \cap (i_2 \in [L_3, R_2]) \cap (i_3 \in [L_3, R_2])\} \cup \{(i_1 \in [L_3, R_2]) \cap (i_2 \in [L_2, L_3]) \cap (i_3 \in [L_3, R_2])\}$..

In the transition to the respective chances it should keep in mind that for uniform distributions at the intersection of the two sub-intervals in expression for chances ratio ½ appears, and at the intersection of three subintervals ratio 1/3. After some transformations we obtain:

$$C(I_1 \succ (I_2, I_3)) = \frac{R_1 - R_3}{\Delta I_1} + \frac{R_3 - R_2}{\Delta I_1 \Delta I_3}\left(\frac{R_3 - R_2}{2} + R_2 - L_3\right) + \frac{(R_2 - L_3)^2}{\Delta I_1 \Delta I_2 \Delta I_3}\left(\frac{L_3 - L_2}{2} + \frac{R_2 - L_3}{3}\right).$$

and $Rs(I_1 \succ (I_2, I_3)) = 1 - C(I_1 \succ (I_2, I_3))$.

Operating in a similar manner, we have:

$$C(I_2 \succ (I_1, I_3)) = \frac{(R_2 - L_3)^2}{\Delta I_1 \Delta I_2 \Delta I_3}\left(\frac{R_2 - L_3}{3} + \frac{L_3 - L_1}{2}\right) \text{ and}$$

$C(I_3 \succ (I_1, I_2)) = 1 - C(I_1 \succ (I_2, I_3)) - C(I_2 \succ (I_1, I_3)) = 1 - Rs(I_3 \succ (I_1, I_2))$.

Since the above expression depends only on the differences of the boundaries of intervals, then, in the case of uniform distributions, relations for chances of preference does not change when the borders are changed on the same number (translation invariance).

A numerical example

Consider a numerical example for this configuration, its parameters and the results of calculations based on the above analytical formulas are presented in Table 1. Data of the Table 1 show that $C(I_1 \succ (I_2, I_3))+C(I_2 \succ (I_1, I_3))+ + C(I_3 \succ (I_1, I_2)) = 1$, $Rs(I_1 \succ (I_2,I_3)) + Rs(I_2 \succ (I_1, I_3)) + Rs(I_3 \succ (I_1, I_2)) = 3 - 1 = 2$, the chances of preference for one interval alternative with respect to two others are less than the minimum chances of its preference in the pair-wise comparison (e.g. 0.602 < MIN(0.833, 0.625)). These findings are in full agreement with the statements of section 2 of this paper. With increasing the right (left) boundary of the second interval the chances of its preference are increased and the chances of the other two alternatives are reduced.

Previously we have seen that risks grow larger and chances of preference become small in the case of nearness of interval alternatives boundaries for a large number of compared objects. These indicators are also very sensitive to changes in the borders of the worst alternative. Suppose, for example, we have three alternatives $I_1 = [10, 18]$, $I_2 = [9, 16]$, $I_3 = [11, 17]$, then $C(I_1 \succ (I_2, I_3)) = =0.438$, $C(I_2 \succ (I_1, I_3)) = 0.161$, $C(I_3 \succ (I_1, I_2)) = 0.401$. Wherein $C(I_1 \succ I_2) = 0.679$, $C(I_1 \succ I_3) = =0.490$, $C(I_3 \succ I_2) = 0.702$. Small increasing the right boundary of the second alternative substantially changes the magnitude of the preference chances: if the first and third alternatives are unchanged and $I_2 = [9, 16.5]$ then $C(I_1 \succ (I_2, I_3)) = 0.423$, $C(I_2 \succ (I_1, I_3)) = 0.196$, $C(I_3 \succ (I_1, I_2)) = =0.381$. Wherein $C(I_1 \succ I_2) = 0.648$, $C(I_1 \succ I_3) = 0.490$, $C(I_3 \succ I_2) = 0.664$. It is evident that a change in the parameters of at least one alternative changes the magnitudes of all chances in the “collective” estimation unlike the pairwise comparison.

Table 1. Preference chances and risks for three compared intervals

Left and Right Borders of the Compared Intervals			
L_1	10	10	10
R_1	18	18	18
L_2	8	8	9
R_2	14	15	14
L_3	11	11	11
R_3	15	15	15
Preference Chances and Risks of Testing Hypothesis			
$C(I_1 \succ (I_2, I_3))$	0.602	0.577	0.597
$C(I_1 \succ I_2)$	0.833	0.777	0.800
$C(I_1 \succ I_3)$	0.625	0.625	0.625
$Rs(I_1 \succ (I_2, I_3))$	0.398	0.423	0.403
$C(I_2 \succ (I_1, I_3))$	0.070	0.131	0.084
$C(I_2 \succ I_1)$	0.167	0.223	0.200
$C(I_2 \succ I_3)$	0.188	0.286	0.225
$Rs(I_2 \succ (I_1, I_3))$	0.930	0.869	0.916
$C(I_3 \succ (I_1, I_2))$	0.328	0.292	0.319

$C(I_3 \succ I_1)$	0.375	0.375	0.375
$C(I_3 \succ I_2)$	0.813	0.714	0.775
$Rs(I_3 \succ (I_1, I_2))$	0.672	0.708	0.681

What will happen with the estimates of preferences when fourth alternative will be added to a set of three ones? For definiteness let I_1 = [10, 18], I_2 = [8, 14], I_3 = [11, 15], I_4 = [10.5, 16]. Calculations carried out by statistical testing method for four interval estimates and by the foregoing formula for three and two estimates give the following results:

$C(I_1 \succ (I_2, I_3, I_4)) = 0.498$; $C(I_2 \succ (I_1, I_3, I_4)) = 0.034$; $C(I_3 \succ (I_1, I_2, I_4)) = 0.187$; $C(I_4 \succ (I_1, I_2, I_3))= = 0.281$; $C(I_1 \succ (I_2, I_3)) = 0.602$; $C(I_1 \succ (I_2, I_4)) = 0.567$; $C(I_1 \succ (I_3, I_4)) = 0.507$; $C(I_1 \succ I_2) = =0.833$; $C(I_1 \succ I_3) = 0.625$; $C(I_1 \succ I_4) = 0.594$. (We restricted ourselves to the hypothesis of preference of the first alternative when comparing estimates of the preference chances for "collective" and pairwise comparison). Again 0.498 < MIN(0.602, 0.567, 0.507), $C(I_1 \succ (I_2, I_3, I_4))+ C(I_2 \succ (I_1, I_3, I_4)) + C(I_3 \succ (I_1, I_2, I_4)) + C(I_4 \succ (I_1, I_2, I_3)) = 1$.

So the chances are reduced and the risks grow.

Hypothetical case of decision-making with account of "collective" effect

Let's consider the hypothetical case of decision-making with account of "collective" effect for three interval alternatives described in the paper [Kononov, 2010] where three possible projects using the resources of the Kovykta gas condensate field are examined. Internal rate of return (IRR) of the project[1] is used in the cited paper as a criterion of comparison. Interval estimates for possible values of IRR in each project were obtained there and ranking of projects by preference and choice of the best one were performed by Hurwicz's method while different values of "pessimism – optimism" coefficient λ were used for different projects. Data mentioned in [Kononov, 2010] are presented in Table 2.

[1] We leave aside the question of the validity finding preference of projects on the basis of such criteria as IRR (see in this regard [Vilensky, 2015]).

Table 2. Interval estimates of IRR for three investment projects

Alternatives	Project Name	IRR (%)	λ
Alt_1	The gas supply to the Unified Gas Supply System of Russia	14.8 – 19.8	0.75
Alt_2	Export of liquefied natural gas to the Asia-Pacific region	11.7 – 23.6	0.5
Alt_3	Gas export to China	10.7 – 27.7	0.25

Recall that according to Hurwicz's method interval estimate [L, R] is replaced by a point estimate $T(\lambda)$ by the formula $T(\lambda) = (1 - \lambda)L + \lambda R$, where $0 < \lambda < 1$ is "pessimism – optimism" coefficient. Note that the choice of different values of λ for different alternatives is not commonly accepted and the concrete choice of these values is difficult to justify. At the same time in some cases mentioned choice is the only way to reconcile knowledge/prediction of expert with the results of Hurwicz's method for right shift configuration of compared intervals when $L_2 < L_1 < R_2 < R_1$. For this configuration under the identical values of the "pessimism – optimism" coefficients the first interval is more preferable than the second one for any λ from the segment [0, 1]. Differing values of λ lead to different results that can fit in with the expectations of experts.

Using the table 2 values of λ we have for results of alternatives ordering after applying Hurwicz's method: $Alt_1 \succ Alt_2 \succ Alt_3$. Indeed, $T_1(0.75) = 18.55$; $T_2(0.5) = 17.65$; $T_3(0.25) = 14.95$. However, the order in the set of comparable alternatives is highly dependent on the choice of λ values if these values are the identical. Namely, for alternatives that are considered in table 2 for $\lambda << 0.196$ $Alt_1 \succ Alt_2 \succ Alt_3$, for $0.196 < \lambda < 0.34$ $Alt_1 \succ Alt_3 \succ Alt_2$, for $0.34 < \lambda < 0.45$ $Alt_3 \succ Alt_1 \succ Alt_2$, at last for $\lambda > 0.45$ $Alt_3 \succ Alt_2 \succ Alt_1$. We draw attention to the fact that value of $\lambda = 1/3$ recommended in [Vilensky, 2015] for choosing similar alternatives is in this case just on the border of the two above selected bands of values λ. Therefore the difference of preferences determined by Hurwicz's method for the first and the third alternatives becomes insignificant.

It is advisable to analyze this problem now by means of the proposed in this paper approach. We estimate the same problem situation comparing alternatives "as a whole". To do so we need the

relations for preference chances for the configuration $L_3 < L_2 < L_1 < R_1 < R_2 < R_3$, that is for configuration of embedded intervals. This is the configuration of interval estimates of IRR in the discussed case. Suppose as before that the distributions on compared intervals are uniform. These relations are shown below.

$$C(I_1 \succ (I_2, I_3)) = \frac{(\Delta I_1)^2}{3\Delta I_2 \Delta I_3} + \frac{(L_1 - L_3)(R_1 - L_2) + (L_1 - L_2)(R_1 - L_3)}{2\Delta I_2 \Delta I_3},$$

$$C(I_2 \succ (I_1, I_3)) = \frac{(\Delta I_1)^2}{3\Delta I_2 \Delta I_3} + \frac{(R_2 - R_1)(R_2 - 2L_3 + R_1) + \Delta I_1 (L_1 - L_3)}{2\Delta I_2 \Delta I_3}.$$

$C(I_3 \succ (I_1, I_2)) = 1 - C(I_1 \succ (I_2, I_3)) - C(I_2 \succ (I_1, I_3))$.

The results calculating the chances are shown in Table 3.

Table 3. Preference chances for gas utilization alternatives

Tested Hypothesis	Chances Values
$Alt_1 \succ (Alt_2, Alt_3)$	0.193
$Alt_1 \succ Alt_2$	0.471
$Alt_1 \succ Alt_3$	0.388
$Alt_2 \succ (Alt_1, Alt_3)$	0.298
$Alt_2 \succ Alt_1$	0.529
$Alt_2 \succ Alt_3$	0.409
$Alt_3 \succ (Alt_1, Alt_2)$	0.509

$Alt_3 \succ Alt_2$	0.591
$Alt_3 \succ Alt_1$	0.612

One can see that both in pair-wise comparison and in the comparison “as a whole” the third alternative preferred others. However the risk of wrong decision is not much less than preference chances of the third alternative. After removing the first alternative from the list of compared ones as an alternative with preference chances for the pairwise comparison less than half, the risk associated with choice of the third alternative is reduced to about 0.4. Note that comparison on base of value of the mathematical expectation leads to the similar choice: $Av(Alt_1) = 17.3$; $Av(Alt_2) = 17.65$; $Av(Alt_3) = 19.2$ (see [Shepelev, 2014]). However using the latter approach doesn’t permit estimate the risk associated with decision-making. Besides coincidence of the choice results for these two selection criteria takes place only for uniform distributions on compared intervals [Shepelev, 2013].

Conclusion

Thus the effect of the comparison of interval alternatives “as a whole” is manifested primarily in reducing value of preference chances for each alternative with respect to its chances under pair-wise comparison. This leads to a quantitative increasing risk value of selection as preferred alternative such one, which may not actually be per se later. The nature of this effect lies in the fact that in the presence of non-zero intersection for already two compared alternatives there is a non-zero risk of making the wrong decision. This risk is enhanced with increasing amounts of compared alternatives especially if some of these chances are not too different from each other. However, it should be borne in mind that the perception of risk is individual and can vary from one DM to another. Therefore the risk value resulting from the use of the proposed method is nothing more than a calculated risk, which can serve only as an estimate for the DMs.

What can be done to reduce the calculated risk? During deciding on preferred alternative choice or in the process of ordering alternatives by preference it’s useful to conduct a preliminary analysis of their initial set. Firstly, after selecting an alternative that preference is tested, one should select in the set of alternatives those, which do not have the intersection with analyzed alternative. If the left boundary of such intervals no less than the right boundary of the tested one the latter is certainly worse. If the right boundary of such intervals not greater than the left boundary of the tested one they can be excluded because they are certainly worse than the last interval. Secondly, one may try to unify some similar or complementary alternatives. By reducing the number of intervals in their initial set one may increase the

calculated preference chances of analyzed alternative and decrease risks. At last, after calculating the preference chances of tested alternative during pairwise comparisons it is advisable to exclude those alternatives whose preference chances with respect to tested alternative is less than 0.5 and, respectively, the risk is more than 0.5.

Are there any other amendments to the results of the pairwise comparison of alternatives due to "collective" effect? Particularly important is the following question: is there difference of the alternatives order in their set defined by the "collective" preference chances and the order for pairwise comparison? The answer to this question is negative: the order established in the process of pairwise comparison is the same as the order for comparison "as a whole".

Thus for this approach the "best" alternative will be the alternative with the highest chances at pairwise comparisons in the set of compared alternatives. However adequate the risk estimation of making wrong decision we obtain by comparing this alternative simultaneously with all the others, "as a whole".

The large number of alternatives aimed at achieving the same goals is a characteristic of the upper hierarchical levels of decision-making. Perhaps that is a reason why for the upper levels of management the risk of making not quit correct decision is more likely (ceteris paribus). Thus meaningful choice of a part of initial set of alternatives to lower levels with the delegation of authority to estimate such objects is represented with point of view of the considered here approach as quite justified.

Difficulties in the work of the experts and decision-makers under interval uncertainty are associated with the complexity of representation of their knowledge and grounding decision-making. DMs often desire to overcome the uncertainty by replacement of interval estimations with point ones on base of their experience, preferences and intuition. Experts from their side desire express their knowledge by rather simple distributions. Of course, exact distributions of chances are unknown for interval alternatives. But one can assume that in many cases these distributions are unimodal ones, and for many types of distributions can be roughly approximated by triangular distributions.

In this regard let's pay attention to following circumstance. Although the methods used in the proposed approach for comparison of alternatives by preference are quantitative because of approximate nature of expert information hardly makes sense to emphasize exactly how much calculated indicator of the quality of one alternative is over/under than for the other one. It seems that here are more appropriate judgments based on ordinal scales i.e. on stating that one of the alternatives is preferable others without quantifying the degree of the preference, such as has place in problems with not quantitative but with qualitative criteria [Larichev, 2006].

Since process of decision-making is quite difficult DMs and experts need means of analytical support. In particular, it's useful that DMs or experts had some ideas of the magnitude of the risk associated with their choice, which is defined not only by configurations of pairwise comparisons but also by a specific set of comparable alternatives. Some such methods are proposed in this paper, which may permit to DMs or experts check how their knowledge and largely intuitive choice is consistent with the formal results and adjust their decisions. Using in the process of alternatives comparing different methods increases the volume and variety of information that is useful to DM and may contribute to increasing adequacy of decision-making.

Acknowledgements

The paper is published with partial support by the project ITHEA XXI of the ITHEA ISS (www.ithea.org) and the ADUIS (www.aduis.com.ua).

References

[Baker, 2015] Baker H.K., Filbeck G. Investment risk management. NY: Oxford university press. 2015.

[Chugunov, 2008] Chugunov N., Shepelyov G., Sternin M. The generalised interval estimations in decision making under uncertainty. //Int. J. Technology, Policy and Management. Vol. 8, No. 3, pp. 298 – 321. 2008.

[Diligensky, 2004] Diligensky N.V., Dymova L.G., Sevastyanov P.V. Nechetkoe modelirovanie i mnogokriterialnaya optimizatsiya proizvodstvennykh sistem v usloviyakh neopredelennosti: tekhnologiya, ekonomika, ekologiya. M.: Izdatelstvo mashinostroenie -1. 2004- in Russian.

[Halperin, 2010] Halperin B., Sevrin A. (Eds.). Quantum theory of condensed matter. World Scientific. 2010.

[Kononov, 2010] Kononov Yu. D., Loktionov V.I., Stupin P.V. Uchet faktora neopredelennosti pri otsenke variantov ispolzovaniya kovyktinskogo gaza //Proc. of the Int. Symposium on "Energy of Russia in XXI Century: Development Strategy – Eastern Vector". Irkutsk, Russia. 2010.– in Russian.

[ISO/FDIS 31000, 2009]. International Standard ISO/FDIS 31000, Risk management - Principles and Guidelines. 2009

[Larichev, 2006] Larichev O.I. Verbalnyy analiz resheniy. M.: Nauka. 2006. – in Russian.

[Nilsson, 1986] Nilsson N. J. Probabilistic logic. Artificial Intelligence. Vol. 28, No. 1, pp. 71-87. 1986.

[Ogryczak, 1999] Ogryczak W, Ruszczyński A. From stochastic dominance to mean-risk models: semideviations as risk measures // European journal of operational research. 1999. V. 116. P. 33 – 50.

[Sternin, 2010] Sternin M., Shepelev G. //Generalized Interval Expert Estimates in Decision Making. Doklady Mathematics. Vol. 81, pp. 485 - 486. 2010.

[Shepelyov, 2011] Shepelyov G., Sternin M. Methods for comparison of alternatives described by interval estimations. //Int. J. Business Continuity and Risk Management. Vol. 2, No. 1, pp. 56 – 69. 2011.

[Shepelyov, 2013] Shepelyov G., Sternin M. The applicability of mathematical expectation indicators in comparing interval alternatives. //Advances in Decision Technology and Intelligent Information Systems. Vol. 14, pp. 32-36. 2013.

[Shepelev, 2014] Shepelev G., Sternin M. The adequacy of point criteria during the evaluation and comparison of interval alternatives problems. //Scientific and technical information processing. Vol. 41, No. 6, pp. 404 – 412. 2014.

[Vilensky, 2015] Vilensky P.L., Livshits V.N., Smolyak S.A. Otsenka effektivnosti investitsionnykh proektov. Teoriya i praktika. M.: Poly Print Service. 2015. - in Russian

Author's Information

Gennady Shepelev *– Laboratory Head of Institute for Systems Analysis of Federal Research Center "Informatics and Control" of RAS; e-mail: gis@isa.ru*

PROJECT MANAGEMENT IN CYBERSECURITY RESEARCH IN UKRAINE

Maria Dorosh, Vitalii Lytvynov, Maxim Saveliev

Abstract: *This paper presents an approach to cyber security research project management. The paper includes the Project Management Office model and conception that can be created in educational and research institution like University. The organization structure of the cyber security research project and the peculiarities of university team organization on cyber security research project are shown.*

Keywords: *project management, cyber security, educational and research projects.*

ACM Classification Keywords: *K.6.1 Management of Computing and Information Systems - Project and People Management*

Introduction

The formation of information society influences the dynamic development of various types of cooperation realised by means of modern information technologies. These changes are aimed at large-format expansion of multi-vector information consulting environment that initiates and supports innovations, and promotes the development of project approach in the process of creation and implementation of strategic development projects and programmes [Chukhrai, 2015].

The synthesis of advanced information and communication technologies and the rapid development of computer technology play a great role in this process: they have caused the creation of fundamentally new global substances –information space and information society, which have practically unlimited potential and play a significant role in the economic and social development of any country in the world.

However, the development of information and communication technologies leads to the emergence of new threats at the level previously unknown to mankind. On the one hand, it provides an access to restricted information, the use of which can cause economic damage such as terrorism, sabotage and diversion to individual companies as well as society in general. On the other hand, it gives the opportunity to misrepresent real and public data, the usage of which can negatively influence economics and society in general. Thus, it is cyber security that is the main factor of sustainable development of modern information society.

Cyber security has become an important research policy in universities and research institutes all over the world. This article presents the information about approaches to cyber security research project management in Ukraine.

Analysis of Recent Researches and Publications

The analysis of publications dealt with the research on the development of special methods and models for providing cyber security [Stasiuk, 2012], [Okhrimenko, 2012] proves that uncontrolled dissemination and unrestricted use of information- and cyberspace by the world's leading countries in the form of arena of action in the course of modern information resistance have led to the following negative results: the majority of other countries (including Ukraine) are characterised by technological lagging and inequality in the sphere of information, nano-, bio-, telecommunication and other high technologies; information flows are duplicated and excessive IP are accumulated by the main subjects of information activity in these countries; public and military authorities of these countries lack qualitative information exchange; information sphere (infosphere) of these countries is not protected from the negative influence of internal and external cybernetic attacks (cyber-attacks) and threats (cyber threats) which can be deliberate, accidental, natural or artificial in their nature, etc. [Buriachok, 2011].

It should be noted that there are no publications dedicated to the project approach, use or creation of new modern methods of project management in the sphere of development and implementation of cyber security systems. That is why it is very urgent for Ukraine and the majority of other countries in the world to carry out research aimed at developing new or improving existing ways of organizing reconnaissance and delivering attacks on IT and cryptosystems, as well as means of resistance to outside influence from possible cyber-attacks and cyber threats.

Taking into consideration the information mentioned above we can introduce the purpose of our study: to present the peculiarities of project management in the sphere of development and implementation of cyber security systems as well as development of new approaches to the formation of such project management system.

In order to reach this aim the following tasks should be completed:

- - to analyse the state and prospects of international cooperation in the course of implementing projects connected with the creation and development of an entire cyber security system;
- - to create such project management system on the basis of higher education institutes of Ukraine;
- - to define the peculiarities of managing project team on the basis of higher education institutes.

Review of Ukraine-NATO Cooperation on Cyber Security Researches

Recent events taken place in Ukraine have influenced Ukraine to become an active participant in international discussions concerning the whole sphere of international relations on which information technologies are able to influence.

It is known that the main world leader in the sphere of development and implementation of cyber security programmes is the North Atlantic Alliance; and Ukraine was the first among non-aligned countries that began to consult with the North Atlantic Alliance on cyber security issues and announced that the country was interested in the development of universal international legal documents concerning this area. At the end of 2008 the Security Service of Ukraine initiated the establishment of the Working Subgroup on Cyber Defence under the aegis of the Ukraine-NATO Joint Working Group on Military Reform (JWG MR); this fact should have been the first step towards the development of cooperation between Ukraine and NATO in this sphere.

On 2 April 2009 the NATO headquarters spread the enclosed document under the title “Framework for Cooperation on Cyber Defence between NATO and Partner Nations”. This document was a logical continuation of a number of former doctrinal documents which defined NATO’s policy on cyber defence. Thus, NATO has created political and legal background and determined appropriate framework for establishing practical cooperation with partner nations, including Ukraine, interested in it.

According to the mentioned document, an essential element of NATO policy in the sphere of cyber defence is the principle that Allies have the prime responsibility for protecting their national communication and information systems, but at the same time NATO must have the ability to support Allies who are victims of a cyber-attack of national significance. Partner nations are urged to take necessary measures in order to harmonize national legislation in the sphere of cyber security in accordance with international norms such as the Council of Europe’s Convention on Cyber Crime.

During 2009-2011 Ukraine actively cooperated with NATO. There were five stages of consultations of the Working Subgroup on Cyber Defence under the aegis of JWG MR in the “ad hoc” format. On the fourth stage, which took place in October 2011 in Yalta, the current state of development of the Strategy of Ukraine in the Sphere of Cyber Defence Project was discussed, but it was neither accepted no executed. The last stage of consultations took place in 2013 in Yalta. After that, Ukraine had no opportunity to perform its activity in this sphere due to a number of objective and subjective reasons [Kandaurov, 2011].

Today the activity on cyber security and information defence is defined, first of all, in the Doctrine of Information Security of Ukraine and the Law on Fundamentals of National Security of Ukraine, and depends on the contradictions between the capabilities of existing methods and techniques of searching, collecting and getting information, as well as protecting our country's IP from foreign cyber influence, on the one hand, and user requirements for providing informational support, for example, to the administrative Board of the Ministry of Defence, the Armed Forces of Ukraine and our state in general, on the other hand.

One of the main drawbacks on the way of problem solving is that the legislation of Ukraine and the majority of other countries of the world has not given fixed definitions of the following notions: cyber-attack, cyber security, cyber influence, cyber warfare, cyber defence, cyber weapon, cyber operation, cyberspace, cyber reconnaissance and other terms that could be taken into account, for example, in the foreign policy activity of countries on the mentioned issues.

For the introduction of this terminology and determination of priority directions of activity in this sphere it was suggested to renew the development of the Cyber Security Strategy of Ukraine Project (2015-2018). This project defines:

- - basic terms and definitions;
- - threats in the sphere of cyber security;
- - main principles of cyber security of Ukraine;
- - main directions of resistance to threats in the sphere of cyber security;
- - system of cyber security of Ukraine;
- - stages of Strategy realization.

Therefore, cyber security requires taking coordinated measures and introducing integrated approaches under the aegis of the state and in close cooperation with the private sector and civil society, without which it is impossible to solve this problem. Furthermore, one country cannot resist cybercrime alone. The effective cooperation between various countries both at the state level and the level of cooperation between government organizations and representatives of the business sphere in the field of IT-technologies is necessary.

Scientific institutions, in particular higher education institutes, should play a leading role in providing scientific support in the process of realizing such a strategy. They can take an active part in the development, planning and implementation of projects involving international partners for the creation of

new approaches to project management in the sphere of development and implementation of cyber defence systems.

In June 2015 an international Cyber Security: Ukraine and the World forum was held in Kiev under the aegis of the Ukrainian Public IT Alliance Organization and the American Chamber of Commerce in Ukraine: the heads of services on security and protection of information of public authorities, bank, financial and corporate sectors discussed the risks of threats and presented new achievements and technologies in the sphere of cyber security. The Concept of Interuniversity Cyber Security Centre was presented on the forum as a project the main task of which is providing and improving the level of cyber security as a component of information security and national security of Ukraine. The project was presented by Kharkiv Zhukovskyi National Aerospace University "KhAI" and Kharkiv V.N. Karazin National University. This concept includes informational, educational, research, technological and communication components, but it does not define the project component and has no management system determined for the implementation of further development and practical application of this concept.

Unfortunately, the management systems of higher education institutes still use old management methods, despite the fact that new requirements for the development of education and society have changed and considerably expanded the directions of activity of all departments of educational institutes. The situation is that teachers and researchers teach their students and develop new systems in the sphere of management, technology and engineering, but they have no opportunity to use them within university. It concerns project management just as well.

At present project activity is carried out at all levels of management in various areas at universities. For example, the following projects can be executed within any Subdepartment:

- carrying out scientific and methodical seminars within the Subdepartment;
- organization and carrying out conferences;
- publication of the collective monograph;
- assisting in licensing particular specialities;
- implementation of some parts of projects (sub-projects) carried out at the university, etc.

In order to carry them out functional structures of project management are used, when a project coordinator is a director or employee of the structural subdivision who is responsible for the project

implementation. However, such a structure has its own drawback: coordinators in project management lack professional skills and knowledge. Of course, it does not mean that it is obligatory to get professional project managers involved in project management, but it demands the creation of a united project management office that will assist in training, consulting and strategic higher education institute project portfolio management.

Conception of Project Management Office (PMO) for Cyber Security Research in University

The main function of the project management office should be to establish the cooperation between stakeholders of projects and maintain effective communication in order to achieve synergistic effect and open new opportunities. This function can be realised by means of modern information technology applications.

Conceptual scheme presenting project management at institutes of higher education (Fig. 1) includes project management office functioning. This model is based on the following five elements of project activity [Neizvestnyi, 2005]:

- systematic approach;
- project life cycle;
- intellectual space of knowledge about project;
- project stakeholders;
- use of general management skills.

The scheme presents project management office built on the basis of the Kerzner project management maturity model [Kerzner, 2003]. This model includes different convergence layers used to connect other parts of a project; these layers make it possible to create innovative management methods and models.

Media convergence layer contains the approximation, agreement of various requirements, restrictions and possibilities concerning a project that are specified by stakeholders and environment. The systematic presentation of a project being formed by stakeholders, the core of values of all members should be defined and fixed in the form of project documentation, and innovative methods of convergence of project participants' values should be applied.

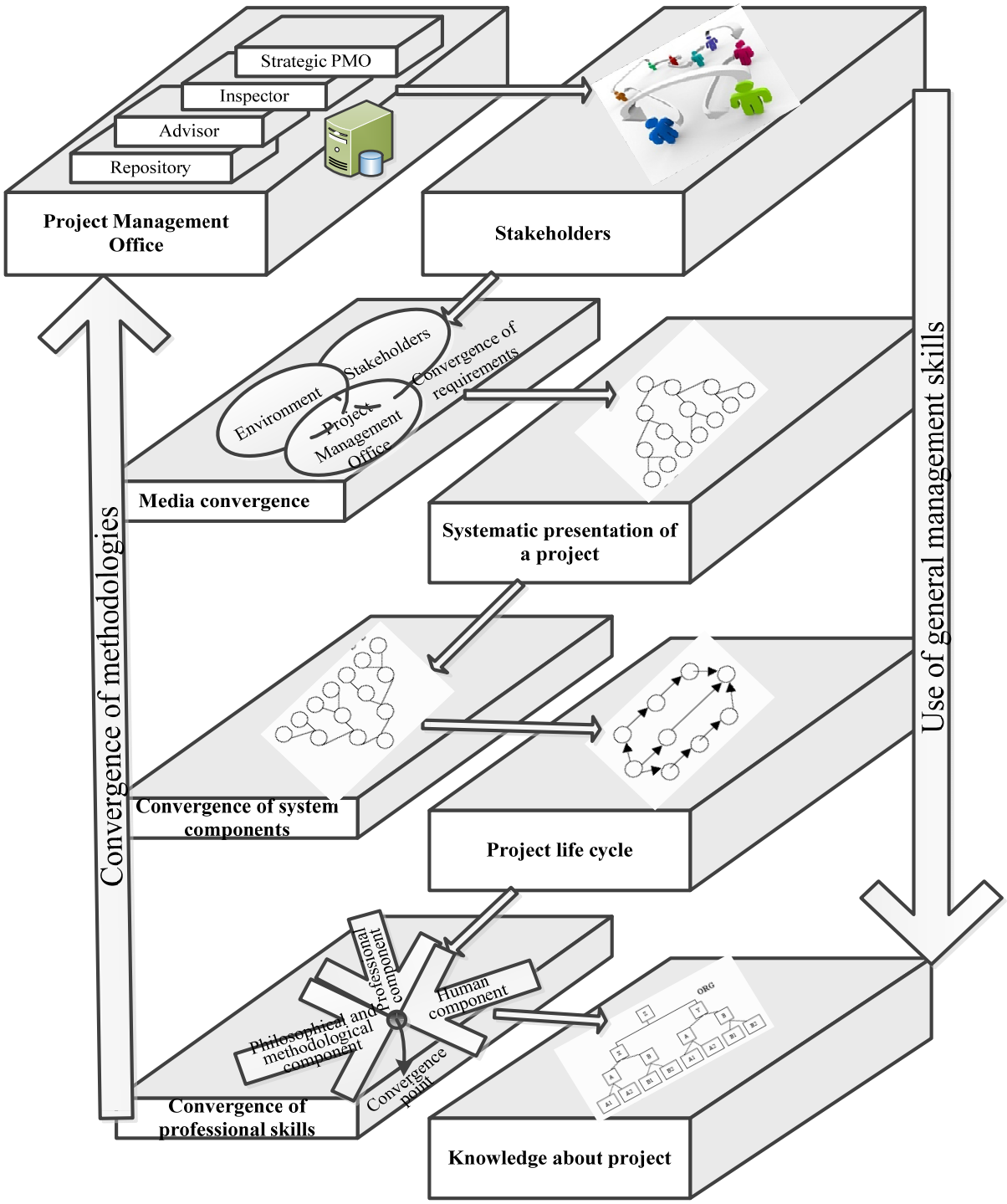


Fig. 1. Conceptual Scheme Presenting Project Management at Institutes of Higher Education

Convergence of system components layer contains the integration processes of coordinated informational, organizational, logistical and administrative components of a project and a basic institution (institute of higher education). Of course, it is not desirable to integrate these systems fully, because it can make it complicated to control the main parameters of the project during its implementation. It is necessary to separate the projects of different functional subdepartments of institute of higher education, though the same resources can be used by them.

Convergence of professional skills layer combines competencies that are peculiar to various types of professional activity involved in the project. In addition, it is necessary to take into consideration the combination of professional, philosophical, methodological and human components of a modern specialist. These components are the basis for convergence of methodologies which makes it possible to introduce innovative project methods and models.

It is also necessary to take into consideration the fact that project team and stakeholders responsible for cyber security projects constitute a virtual, motivational space, in which stakeholders devote themselves to their project, being in different geographical, cultural, special and organizational environments, and cooperate sharing their points of view on the project content, planning, control and communication within that project. The quality of an intellectual space influences significantly the project execution.

In addition, cyber defence projects are carried out under the aegis of international organizations, within which misunderstandings and contradictions caused by cultural peculiarities of participants from different countries often arise. Thus, using convergence methods will help to overcome these problems and lead to understanding between project participants.

It is known that all members of a project team cooperate with each other virtually through the Internet. That is why the effectiveness of communication within modern virtual project team depends on understanding project objectives and the fact whether the project participants are interested in working on it. First of all, a great attention is paid to correct professional communication skills regardless of geographical, temporary or cultural environment to which the project team members belong. In general, the configuration of relations between them forms the essence of project intellectual space.

Project Approach in the Process of Preparation for Participation in the International Cyber Security Program in Chernihiv National University of Technology.

Let us consider the peculiarities of using project approach in the process of preparation for participation in the International Cyber Security Program in Chernihiv National University of Technology.

The main objectives of cooperation between partner from different countries in cyber defence sphere are as follows:

- to improve the ability of partner nations to protect their critical communication and information infrastructures against cyber-attack;
- to provide a basis for support measures in cases of cyber-attack;
- to help restore normal functioning following such attacks.

Many specialists working in Chernihiv National University of Technology have been already engaged in the implementation of grant projects and programmes; their experience shows that there is a great need for a comprehensive and serious preparation for their implementation. The University is going to participate in the the NATO Science for Peace and Security grant programme and preparation has been started since October 2015.

First of all, the project team was formed, and its organizational structure which includes both external and internal project members was developed (Fig. 2).

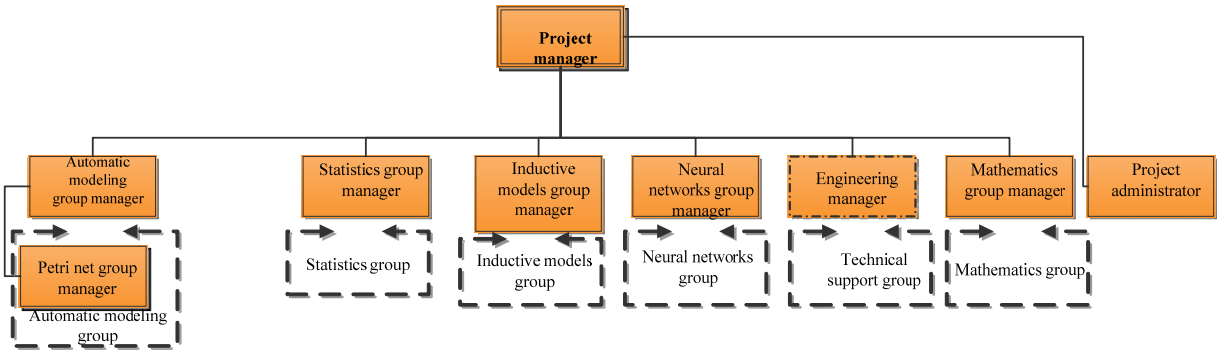


Fig. 2. Organizational Structure of Project Preparation for Project Cyber Security Execution

The project is managed by the project manager, and the organizational administrator carries out organizational activity. Also functional project groups were formed according to the areas of research. Experts, scientists, postgraduate students as well as students from different courses are members of such groups. In this case, the involvement of students plays an important role in the educational and methodological process, as such an activity teaches to solve real problems, bring them to completion, and work in team; it also helps coordinate and plan one own's activity.

In addition, the project scheduling being conducted makes it possible to control the process implementation and draw a conclusion about the effectiveness of some phases execution.

At present phase of the project implementation we can determine that:

- Project implementation by University teams always pursues two objects: first of all, acquiring new knowledge and mastering skills by project participants; secondly, successful project implementation in spite of fixed project restrictions (time-frame, money, quality). At the same time, students, postgraduate students and faculty will constitute the basic human resource of the project.

- In the process of such projects implementation the students lack the necessary knowledge, postgraduate students lack experience, and the faculty is limited to existing teaching load norm and bureaucratic procedures.

There are some more obstacles on the way of successful project execution:

- Time limitation. As a rule, students' projects are carried out within one semester (12 – 16 weeks). During this time it is difficult to form a team and conduct a quality work.

- Behavioral problems. Being students, young people have not formed professional relationship towards work and colleagues. They tend to form groups according to their personal preferences. Conflicts unknown to a teacher and project manager influence negatively the formation of groups.

- Restrictions in choosing research problem. As a result the students have no motivation to carry out a project.

We can distinguish the following two types of project work:

- project work carried out by the students of the same year of studying,

- general project work carried out by the faculty (students can be involved just as well).

In the first case, team members are characterized by approximately equal knowledge and ambition. In order to set up such a group Agile Scrum model was used. One of the main problems is to appoint a leader who forms the team and defines its activity. That is why this role is performed by teachers, but senior students are also given some tasks to be done.

In the second case, there is an absolute project leader. The team members carry out project tasks according to their functional abilities.

Thus, practical implementation of professional project management in higher education institutes gives the opportunity to use innovative scientific achievements of leading scientists involving students and postgraduate students to work in team, such an approach can significantly improve the efficiency of learning process and reduce the gap between theory and practice.

Conclusion

Finally, we can draw the following conclusions:

- the analysis of the state and prospects of further international cooperation in the course of implementing projects connected with the creation and development of an entire cyber security system has shown the necessity to continue active cooperation with NATO in cyber defence of Ukraine issues;
- the suggested conceptual scheme presenting cyber security project management is supposed to be used at institutes of higher education; it contains all the components necessary for the development of innovative project management methods and models on the basis of project management office;
- the results of practical application of professional project approach have revealed the main specific features of human resource management in such projects, that can become the basis for the development of new management methods and models at present.

Bibliography

[Chukhrai, 2015] . Chukhrai N.I., Nowakowski I.I. (2015). Project management as a basis for effective development of the information society. Bulletin of National Technical University "KPI". Collected Works. Series: Strategic management, portfolio management, programs and projects, №2 (1111), 3-8. (in Ukrainian).

[Stasiuk, 2012]. Stasiuk A.I., Korchenko A.A. (2012). Basic model parameters to build systems detect attacks. Scientific and technical journal "Protecting information",№ 2 (55), 6-18. (in Russian).

[Okhrimenko, 2012] .Okhrimenko A.A., Korchenko A.O. (2012). Model identification spoofing attacks on information systems resources. Information Technology and Data Protection: Third International Scientific Conference [Abstracts], 210. (in Ukrainian).

[Buriachok, 2011]. Burachok V.L. (2011). Estimation algorithms degree of security specific information telecommunication systems . Scientific and technical journal “Protecting information”, №3, 21-30. (in Ukrainian).

[Kandaurov, 2011]. Kandaurov S. M. (2015) The question of cyber security. Interaction between Ukraine and NATO in the field of cyber security. Internet resource: http://www.uan.ua/ua/content. (in Ukrainian).

[Neizvestnyi, 2005]. Neizvestnyy S.I. (2005). Project Management : a tutorial, IT, 221. (in Russian).

[Kerzner, 2003]. Kerzner H. (2003). Strategic planning for project management using a maturity model. Publisher: DMK Press, IT Co., 320. (in Russian).

Authors' Information

Maria Dorosh *– PhD in PM, Chernihiv, National University of Technology, 95, Shevchenko street, Chernihiv-27, Ukraine, 14027; e-mail: mariyaya5536@gmail.com*

Major Fields of Scientific Research: Project Management

Vitalii Lytvynov *– Dr. Sc., Prof. Chernihiv, National University of Technology, 95, Shevchenko street, Chernihiv-27, Ukraine, 14027; vlitvin@ukrsoft.ua*

Major Fields of Scientific Research: modeling of complicated systems, computer aided management systems, decision support systems

Maxim Saveliev *– Institute of Mathematical Machines and Systems Problems, Ukraine;*
e-mail: mcsim@sitex.com.ua

Major Fields of Scientific Research: Software Engineering, Automated System Life Circle Models, Requirements Evolution, System Analysis, System-of-Systems

IMPROVING OF EXISTING PERMISSION SYSTEM IN ANDROID OS

Volodymyr Kazymyr, Igor Karpachev

***Abstract**: Smartphones for last five-ten years had become ubiquitous. Despite the fact, that these small devices are very widespread around the world - security are still being understood. As a result, the security is extremely vital. Basically security area is very underdeveloped and still vulnerable. On the one hand this article is an investigation of existing pros and cons of android security system. On the other hand it is an example of how to improve current mobile security state.*

***Keywords**: security model, OS Android, functional security.*

***ACM Classification Keywords**: D.4.6 Access controls*

1. Introduction

Smartphones has added additional requirements to the mobile computing. All set of application has support variety of the areas on mobile markets. Hardware, software, and different business access – such applications are available on markets (e.g. Apple Store, Google Play, Blackberry App World, Amazon App Store etc.). Moreover most of these applications are surprisingly inexpensive.

Smartphones are shifted now from simple standalone devices to a specific collaborate models (client-server architecture). In this case applications exposed a lot of private data to the external world. Applications usually seek appropriate providers of a service type at run-time, instead of binding itself to the specific implementation during development. This approach is very similar to plugin approach. Such approach has created very extensible culture of “use and extend” which lead to significant increasing of innovative applications on modern market. The very best example from existing platforms is Android operating system. The security of the android is very similar to other, and called “system-centric”. Based on that conclusion, application statically identifies all permission/interfaces required during development process. These rules will govern application’s data at installation time.

The main problem that application/developer has very limited ability to identify to whom or how these permissions will be exercised after words. Developer should assert which level of protection application desires. End user has no idea which set of permission application requires, so they do not have sufficient context to do so.

Purpose: aim of the current article is to find a better way to assign a new permission model to applications in order to improve security.

2. Methodology, Limiting factors and evaluation

Currently PayPal is a most widespread service around the world. Let's take as an example PayPal service built on OS Android. This service is kind of a bridge between the credit card of current user and purchasing of different items/features/goods from such applications as email client, Google Play market, browser, music players, etc. Considering this, PayPal is an application, which shares permissions with a lot of other services. Therefore, user ends up with a situation when it's quite difficult to decide which app should be granted with PayPal billing service. Android doesn't provide any API for clarifying this situation or enforcing a security policy based upon this, unfortunately [Miller, 2012]. Android developers put a lot of efforts in creating huge set of applications and features, which will help end user to protect device, but there is no API, which will help to protect application itself. Basically there are three main features, which are not available in an android application security framework:

1) Permission assignment policy - Applications have limited ability to control to whom permissions for accessing their interfaces are granted, e.g., white or black list applications.

2) Interface exposure policy - Android provides only rudimentary facilities for applications to control how their interfaces are used by other applications.

3) Interface use policy - Applications have limited means of selecting, at run-time, which application's interfaces they use.

This paper introduces the Secure Application Approach (SAA) that extends the existing Android security architecture with policies that address these key application requirements. Figure 1 below depicts basic Secure Approach with payment system on Android OS.

Applications provide installation time policies that regulate the allocation of permissions that protect their interfaces. At runtime, communication between or access of applications is subject to security policies declared by both the caller and callee applications. Saint policies are much more superior than the static permission checks currently available in Android by limiting access based on runtime state, e.g., phone or network configuration, location, time, etc. The Saint framework will be defined and the complexities of augmenting Android with extended policy enforcement features are will be discussed, and mechanisms for detecting incompatibilities and dependencies between applications will be developed. The discussion begins with an encouraging example.

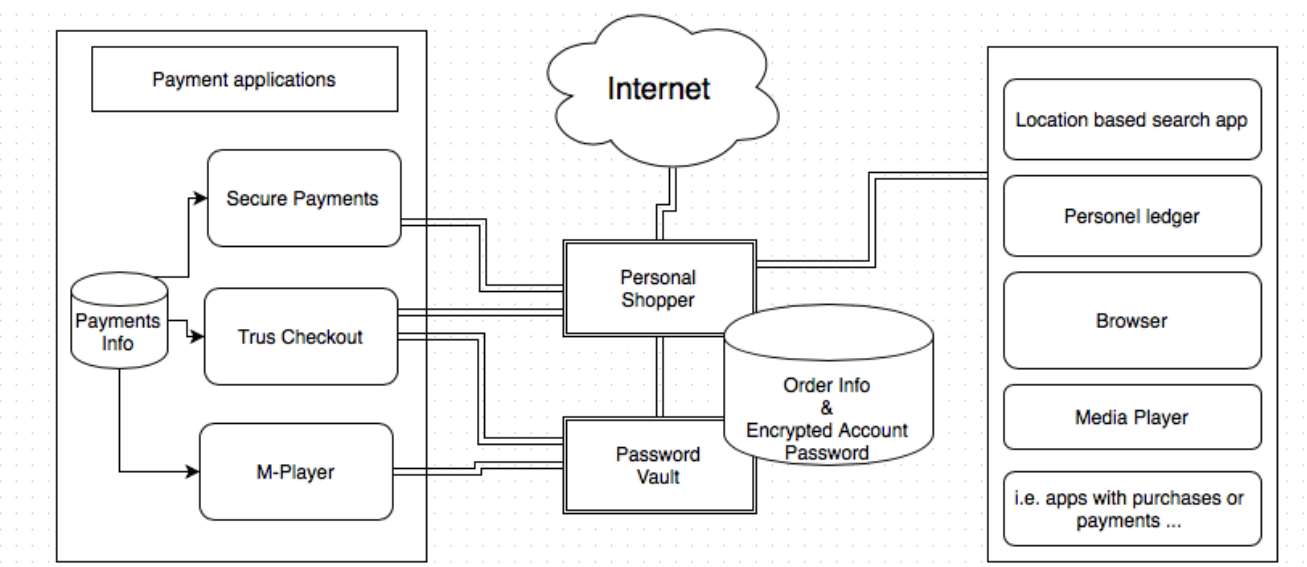


Figure 1. Discretion of the user and interacts with vendors and payment applications to purchase them.

3. Smartphone applications security

Figure 1 presents the made-up smartphone shopping application "Personal Shopper". "Personal Shopper" tracks the items a user wants to buy and interacts with other payment applications to purchase them. User select the desired goods through the user interface of the smartphone (theoretically by clicking on units on a browser, media player, etc.), creating a seller independent "shopping cart". Users later purchase items in one of two ways. The user can direct the application to "find" an item by clicking on it. In this case the application will search for all known online vendors or various shopping search sites (e.g., Google Product Search) to find the desired item. Where various vendors provide the same item, the user then selects their vendor choice through a provided menu. The second way for finding a desired product is by geography—a user walking through, for instance, a mall, the usage of location based search application can alert them on the availability of the product in the nearest physical store. In this case, the user will be directed to the brick-a-brick vendor to obtain the item.

Unrelatedly of how the item is found, "Personal Shopper's" second objective is to aid the purchase process itself. In this particular case, it works with provided example checkout applications as SecurePayer and TrustCheckout. Personal- Shopper gets the access to checkout applications and acts

as a mediator between the buyer and the merchants to both aspects as improving the efficiency of shopping and customer privacy protection. Usually procedure is quite simple – user provides credentials in order to authenticate to service. After their completion, all the transactions are recorded in a personal ledger application.

Consider a few (of many) security requirements this application suggests:

1) Only trusted payment services should be ever used by the PersonalShopper. Figure 1 shows, it may trust only SecurePayer and TrustCheckout, but it does not trust any other unknown payment providers (e.g., the M-Payer provider).

2) PersonalShopper may only want to restrict the use of the service to only trusted networks under safe conditions. For instance, it may wish to restrict searches while the phone is roaming or highly unprotected areas (e.g., airports) or while battery is low.

3) The use of certain version of the service software may be required by the PersonalShopper. Such as, the pass- word vault application v. 1.1 may contain a bug that disclosures password information. Thus, the application would require the password vault be v. 1.2 or higher.

4) PersonalShopper may wish to confirm transaction information is not leaked by the phone's ledger application. Thus, the application wishes to only use ledgers that don't have access to the Internet.

5) Security requirements may be placed on PersonalShopper by the applications and services it uses. For example, to save location privacy, the location based search application may only offer PersonalShopper location information only where PersonalShopper has the permissions to access location information itself, e.g., the phone's GPS service.

None of these policies are currently supported by today's Android security system. While some of these may be partially emulated using combinations of complex application code, permission structures, and code signing they are simply outside the scope of Android's security policy. As a result (and core to our widespread experience building systems in Android), applications must cobble together custom security features on top of the fundamental structures currently provided by the Android system. Where possible at all, this process is ad hoc, error prone, repetitive, and inexact [Anderson, 1992].

What is needed for Android is to provide applications a more semantically rich policy infrastructure. The following investigation begins by outlining the Android system and security mechanisms. Section IV examines a range of policies that are potentially needed for fulfillment of the applications' security requirements as well as highlighting those that cannot be satisfied by the current Android. Further, goals, design, and implementation of the Saint system is introduced

«Android»

Android is an operation system, which has been developed by OHA – Open Handset Alliance in 2005. Android became extremely popular among developers and end-users for it's open source nature and common language for development Java (or C++ - JNI).

The Content Provider API implements an SQL-like interface; however, the application developer is left with the backend implementation. The API involves support to read and write data streams, e.g., if Content Provider shares files. Unlike the other component types, Content Providers are not addressed via Intents, but rather a content Uniform Resource Identifier (URI). That is the collaboration of application components for which we are more concerned. Figure 2 shows the common IPC between component types.

The bases of the Android's application-level security framework are permission labels, which are enforced in the middleware reference monitor [Enck, 2009]. Basically, a permission label is a unique text string that can be described by both the OS and third party developers. Android defines various base permission labels. From an OS centric point, permission labels are statically assigned for the applications, indicating the sensitive interfaces and resources available at run time; the permission set cannot grow after installation.

Application developers identify a list of permission labels the application requires in its package manifest; however, requested permissions are not always granted.

Permission label descriptions are distributed across the framework and package manifest files. Each definition specifies "protection level." The protection level can be "normal," "dangerous," "signature," or "signature or system." After application installation, the protection level of requested permissions is checked. Permission with the "normal" protection level is always granted [Cheswick, 2003]. Permission with the "dangerous" protection level is always granted if the application is installed. However, the user must confirm all requested dangerous permissions together. Finally, the signature protection level influences permission granting without user input. Each application package is signed by a developers' key (as is the framework package containing OS defined permission labels). A signature-protected permission is only granted if the requesting permission labels is signed by the same developer key that is signed the package defining the permission label. Many OS defined permissions use the signature protection level to ensure that the access is granted only to the applications distributed by the OS vendor. Finally, the "signature or system" protection level operates the same as the signature level, moreover the permission is granted to applications that are signed by the system image key.

Additional use for permission label policy model is to protect applications from each other. Most permission label security policy could be found in an application's package manifest. As mentioned before, the package manifest specifies the permission labels that correspond to the application's functional requirements. The package manifest also specifies a permission label to protect each component of the application (e.g., Activity, Service, etc). Inter Process Communication may initiate communication in another or the same component of if target has specific permission.

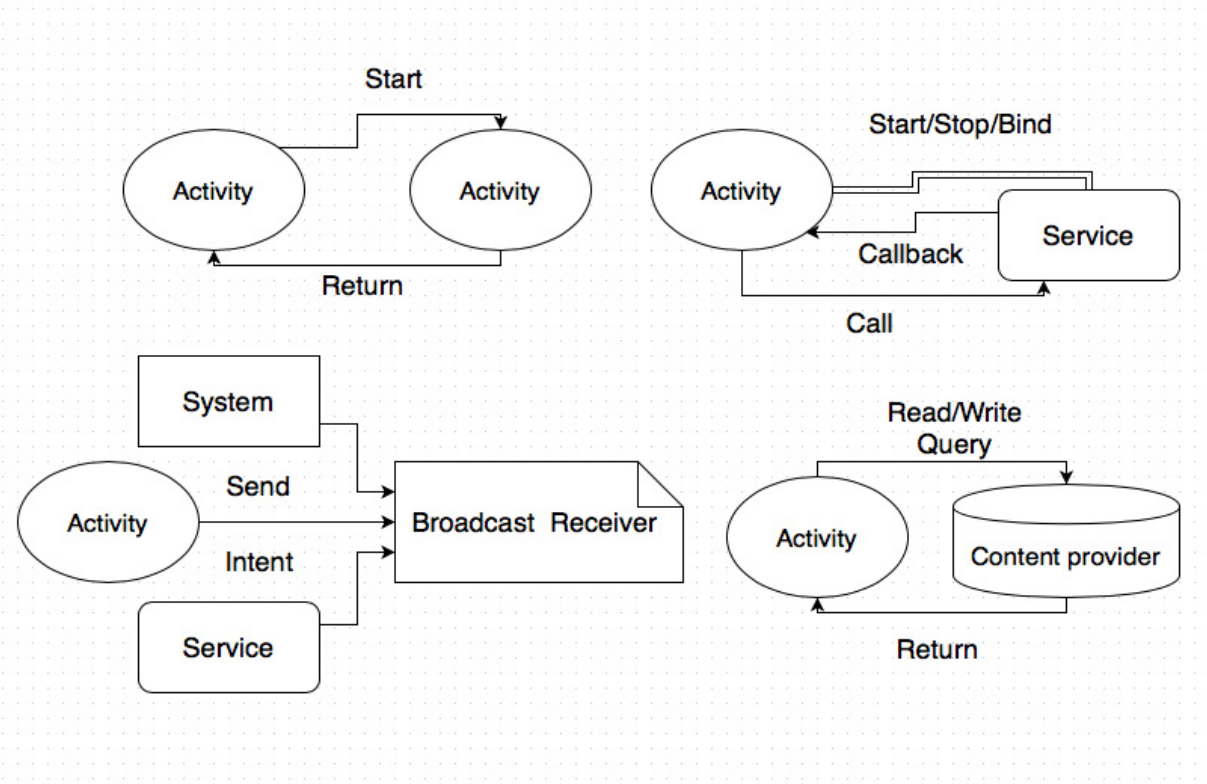


Figure 2. Typical Android application component IPC

While Android is based on Linux, the middleware presented to application developers hides usual OS concepts. The platform focuses on applications, and much of the core phone functionality is implemented as applications in the same manner used by third party developers [McDaniel, 2012].

Android applications are primarily written in Java and compiled into a custom byte-code (DEX). Each application executes in a separate Dalvik virtual machine interpreter instance running as a unique user identity.

From the perspective of the underlying Linux system, applications are ostensibly isolated. This design minimizes the effects of a compromise, e.g., an exploited buffer overflow is restricted to the application and its data [Cheswick, 2003].

All inter-application communication passes through middleware's binder IPC mechanism (our discussion assumes all IPC is binder IPC). Binder provides base functionality for application execution. Applications are comprised of components. Components primarily interact using the Intent messages. While Intent messages can explicitly address a component in an application by name, Intent versatility is more apparent for Intent messages addressed with implicit action strings, for which the middleware automatically resolves how to handle the event, potentially prompting the user. Recipient components assert their desire to receive Intent messages by defining Intent filters specifying one or more action strings.

There are four types of components used to construct applications; each type has a specific purpose. Activity components interface with the user via the touchscreen and keypad. Typically, each displayed screen within an application is a different Activity. Only one Activity is active at a time, and processing is suspended for all other activities, regardless of the application. Service components provide background processing for use when an application's Activities leave focus. Services can also export Remote Procedure Call (RPC) interfaces including support for callbacks [Bishop, 2003]. Broadcast Receiver components provide a generalized mechanism for asynchronous event notifications. Traditionally, Broadcast Receivers receive Intents implicitly addressed with action strings. Standard event action strings include "boot completed" and "SMS received." Finally, Content Provider components are the preferred method of sharing data between applications.

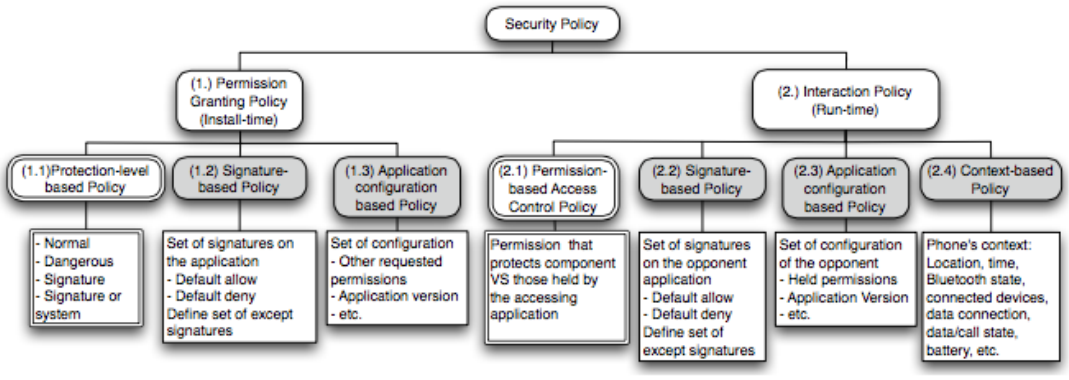


Figure 3. Policy tree illustrates the example policies required by applications. The double-stroke boxes indicate support by the existing platform.

Using this policy and permission protection levels, application developers can specify how other applications access its components. The permission label-based security policy stems from the nature of mobile phone development. Manually man- aging access control policies of hundreds (thousands) of potentially unknown applications is infeasible in many regards. Hence, Android simplifies access control policy specification by having developers define permission labels to access their interfaces. The developer does not need to know about all existing (and future) applications. Instead, the permission label allows the developer to indirectly influence security decisions. However, herein lies the limitations of Android's security framework.

«Application policies»

It was explored a myriad of applications as a means of understanding the appropriate set of policy expressibility. Initial policy taxonomy is presented in Figure 3.

The permission-granting policy regulates permission assignment. In addition to controlling permission granting using Android's protection level-based policy (1.), an application A may require signature-based policy (1.2) to control how the permissions it declares are granted based on the signature of the requesting application B (A and B may be signed by different developer keys). Instead, the policy grants (or denies) the permission by default with an exception list that denies (grants) the applications signed by the listed keys. An application may also require configuration-based policy (1.3) to control permission assignment based on the configuration parameters of the requesting application, e.g., the set of requested permissions and application version.

The interaction policy (2.) regulates runtime interaction between an application and its opponent. An application A's opponent is an application B that accesses A's resources or is the target of an action by A, depending on the access control rule (i.e., B is A's opponent for rules defined by A, and A is B's opponent for rules defined by B). Android's existing permission-based access control policy (2.1) provides straightforward static policy protection, as described in Section III. However, this policy is coarse-grained and insufficient in many circumstances. Applications may require signature-based policy (2.2) to restrict the set of the opponent applications based on their signatures. Similar to above, the default-allow and default-deny modes are needed. With configuration- based policy (2.3), the applications can define the desirable configurations of the opponent applications; for example, the minimum version and a set of permissions that the opponent is allowed (or disallowed). Lastly, the applications may wish to regulate the interactions based on the transient state of the phone. The phone context- based policy (2.4) governs runtime interactions based on context such as location, time,

Bluetooth connection and connected devices, call state, data state, data connection network, and battery level. Note that initially, policy types 2.2 and 2.3 may appear identical to 1.2 and 1.3; however, the former types also place requirements on the target application, which cannot be expressed with 1.2 and 1.3. However, 1.2 and 1.3 are desirable, because when applicable, they have insignificant runtime overhead. We now present two example application policies related to our motivating example, Personal Shopper, which interacts with checkout applications, password vaults, location-based search applications, and personal ledgers [Enck, 2009].

Install-time Policy Example: In our Personal Shopper example, the location-based search application (com.abc.lbs) wants to protect against an unauthorized leak of location information from its "Query By Location" service. Permission granting policy can be applied when the Personal Shopper requests the permission com.abc.perm.getloc used to protect "Query By Location". It needs application configuration-based policy to specify that for the permission com.abc.perm.getloc to be granted, the requester must also have the "ACCESS LOCATION" permission.

Run-time Policy Example: To ensure that the checkout application used for payment is trusted, their signatures must be checked. The Personal Shopper needs signature-based policy to specify that when the source "Personal Shopper" (com.ok.shopper) starts an Activity with action "ACTION PAY", the policy ensures resolved applications are signed by keys in a given set.

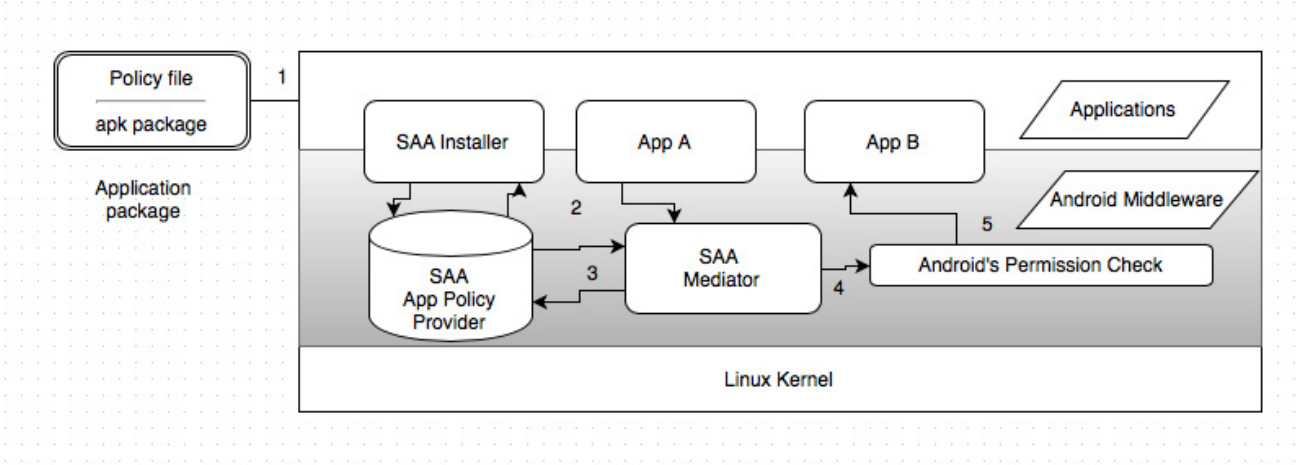


Figure 4. Process (a-c) with additional permission granting policies and mediates component IPC (1-5) to enforce interaction policies specified by both the caller and callee applications.

4. Conclusions

This article addressed existing limitations in android operation system. Particularly in real-time permission assignment and inter process communication policies. The main idea was to provide clear way of expose android permissions to application's functionality. Driven by an analysis of the PayPal service this article gives an example of an initial taxonomy of relevant security content. Current approach has a lot of drawbacks as well and not going to replace existing permission assign policy in android operation system. This is just an example of how these technologies can be improved.

Bibliography

[Miller, 2012] Miller C. Mark D. Independent Security Evaluators, Exploiting Android Devices 2012.

[Anderson, 1992] Anderson J. P. Computer security technology planning study, volume II. 1992, 82-94.

[Enck, 2009] Enck W. Understanding Android Security, 2009, 50-58.

[Cheswick, 2003] Cheswick W., Firewalls and Internet Security: Repelling the Wily Hacker, 2003, 82-94.

[McDaniel, 2012] McDaniel, Prakash A. Methods and Limitations of Security Policy Reconciliation, 2012, 77-87.

[Bishop, 2003] Bishop M, *Computer Security:A standad science*, 2003.

[Enck, 2009] Enck W., Ongtang M., McDaniel P. On Lightweight Mobile Phone Application Certification, 2009.

Authors' Information

Volodymyr Kazymyr – Dr. Sc., Prof. Chernihiv, National University of Technology, 95, Shevchenko street, Chernihiv-27, Ukraine, 14027; vvkaymyr@gmail.com

Major Fields of Scientific Research: computer science, information technologies, complicated computer systems.

Ihor Karpachev – Ph.D. Student, Chernihiv National University of Technology, 95, Shevchenko street, Chernihiv-27, Ukraine, 14027; benchakalaka@gmail.com

Major Fields of Scientific Research: security problems in existing mobile operating system.

PRIVATE GROUPS IN PEER-TO-PEER NETWORKS

Oleh Hordiichuk, Oleksiy Bychkov

Abstract: *Peer-to-peer architectures are designed for the sharing network, storage and computing resources solving a scalability problem. At the same time they lack capabilities for creating private groups that are necessary for a limited access data exchanging – a common task for e-learning systems. In this paper proposed a new peer-to-peer system that is able to create private groups that is built on top of WebRTC stack and thus is capable to run in modern browsers without additional software installation. It solves problems of authentication, data validity, management control and secure peer discovery in distributed network systems by using private and public keys as well as data exchanging rules that provide same level of data dissemination security as in client-server applications. This system provides ability of creating closed groups of students, where teacher is able to transmit data securely and combine low operational cost of video streaming and file sharing advantages of Tailcast topology. Moreover teacher's capabilities are not limited to only data dissemination process, this application gives additional functions like banning and kicking users as well as a secure access promoting to other participants of the network. While proposed techniques are designed and implemented for the Tailcast topology, it's shown that it is possible to apply these recommendations in most peer-to-peer applications including other video-streaming topologies, distributed hash tables and file sharing.*

Keywords: *peer-to-peer, security, distributed systems, e-learning*

ACM Classification Keywords: *C.2.4 Distributed Systems*

Introduction

Rapid development and success of file sharing systems like BitTorrent motivates researches to apply this idea in other direction and e-learning systems are not an exception. Most of modern e-learning systems are using video materials for knowledge representation that are known to be heavyweight in network distribution meaning. That is why distributing media often is not affordable for universities, when we are talking about more than 1000 of simultaneously watching students. In this case if video stream has the lowest quality and high definition resolution (720p) that is equal to 2Mbit/s, university requires a server with network bandwidth equal to at least 2Gbit/s. At the same time peer-to-peer systems are capable to solve this problem without costly allocated bandwidth channels and use bandwidth of watchers instead. However these applications introduce additional delay that could be equal to more

than 1 minute in such well-known commercial peer-to-peer solutions like SopCast. Such behavior makes real-time video streaming and user interaction impossible. That is why in this paper the Tailcast [Hordiichuk, 2013] topology is used as due to its hybrid-tree network topology structure additional delay is minimized. But at the same the system proposed in this paper could be implemented over other existing network topologies like Kademlia [Maymounkov, 2002], Chord [Stoika, 2001], Prime [Magharei, 2009] and others. The only limitations on the network topology for the proposed system is to have a connected graph network and a ability of peer to make sure in validity of the stream source that do not impact on the structure.

Anyway every peer-to-peer system generally do not have any mechanisms for restricting access of data distributed among peers, so in case of e-learning any student has access to any material that is currently available in the network. In this situation it is possible either to make unauthorized copying of data or to attack the network by distributing invalid data that leads to an unpredictable behavior of the whole system. Also the teacher doesn't have any control over situation in peer-to-peer systems. If there exists chat or file sharing function in such system, it is impossible for teacher to ban or kick peers that are distributing spam messages or files anonymously. Another problem is a providing some level of a management access in a case, when the teacher wants to listen student's answer via webcam or distribute own solution of the task over the whole group. In this case due to a decentralized behavior of the system teacher needs to have an ability to notify all students in the group that one of them has permissions to perform this action. As well as an opposite task of returning access is also complicated without direct notification from a central server in peer-to-peer systems. This leads to a situation where benefits of using peer-to-peer networks are nullified by security problems and that is why it is important to develop the system without these restrictions.

It should be also mentioned that ease of use of educational systems is one of the mandatory features in modern e-learning systems. At the same time most of existing peer-to-peer systems require installation of additional software that increase usage complexity. So for solving this problem the system described in this paper is built on top of WebRTC stack that gives ability to use it only with a modern web-browser. However it is not limited only to this protocol stack and same idea could be applied on any modern peer-to-peer protocol. At the same time it doesn't rely on any browser plugins and could be used as a separate library even in desktop and tablet applications of any vendor. These features increase potential of the solution by making possible to integrate it as a component of a more complex existing educational system without additional limitations. However WebRTC is not a pure sockets implementation and it has some design characteristics like impossibility to establish direct connection without a signaling server due to a protocol security considerations. But at the same time such behavior limits ability of decentralized peer discovery in the network. The system proposed in this paper is also addresses these

problems and try to make process as distributed as possible without decreasing security level by using intermediate peers as signaling servers and certified message exchanging process for removing safety limitations.

Related work

Security is a common problem in peer-to-peer networks that is frequently discussed by researches. Most of approaches are based on trust and reputation models, where historical behaviors and decisions of every peer are used to predict how peer will behave in future. Main idea is to use both own and neighbors reputation observation for calculating trust value that is used for making future communication decision. Reputation systems face a problem such as having an ability to differentiate real feedback from the false one. Another common problem is dealing with a dynamic personality of every participant. For some period of time peer could act as a reliable partner, but after change its behavior and attach the network. Or even more complex type of attacks where malicious peers in addition to previous approaches also communicate with their neighbors using different behavior and thus tangle reputation algorithm. These problems as well as other attacks considered in PeerTrust framework [Xiong, 2004] and SORT [Can, 2013], where used several trust metrics combined with reputation recommendations observed from another peers.

Another approach is to use voting mechanism that helps to figure out secure resources. The more valid peers vote in the network the more exactly malicious peer detection will be. Actually this process is very similar to reputation calculation as votes could be represented as reputation values. However peer-to-peer network is not completely democratic as not all of peers have same count of votes. This happens due to that fact that peers suddenly join and leave the network and newcomers could be malicious with higher probability than old peers. Therefore newcomers must not have more votes than stable ones. An example of such systems are described in VectorTrust [Zhao, 2013] and [Gupta, 2003].

While reputation systems are able to win malicious peers attack in case when they are in majority and provide completely decentralized form of security management, they are not designed to solve problem related to private groups creation. First of all these systems are not completely decentralized as they have presence of the teacher that naturally is a leader of the swarm and thus must have an ability to manage its group. However in this case reputation based systems could consider the teacher as an absolutely truthful source and all other peers can have a mandatory rule for processing commands only from secure neighbors. That does not solve a problem, as at any time there is still non-zero possibility to receive a malicious file or another type of information that is unacceptable in any e-learning system.

Therefore the system described in this paper doesn't rely on reputation security; instead it uses private and public keys for signing and verifying commands from the teacher. This is very similar to Skype authorization and command execution process that is briefly described in [Hoßfeld, 2008]. Here a central server signs a token for the authorized client that is used by other peers for connection identification and validation. Also every time someone joins the network it receives a public key from central server that gives ability to validate messages from other peers. It helps participants to split authorized peers from unauthorized ones. In this paper similar idea is used, the teacher acts as a central server and students as peers. However authorization scheme in messaging protocols like Skype doesn't solve problem of validity data dissemination, secure access promotion among peers as well as attacks from malicious peers. These as well as other problems described and their solution proposed in this paper.

Connection establishment protocol description

In this paper we consider the private grouping as a process of creating peer-to-peer system, where one of the peers acts as a leader of the system (teacher's role) and others as followers (student's role). The leader is responsible for authentication process and must have an ability of secure data dissemination. It means that every follower in the system should recognize generated data from the leader and dismiss data from malicious peers. This behavior could be achieved if the leader and followers adhere following rules during establishing a connection:

1. The follower must be authorized by the leader using login and password or a secret message;
2. The follower and the leader must exchange their public keys;
3. If authorization process is successful then the leader signs and sends a connection token to the follower. Also the follower receives connection information about some amount of existing peers in the network as well as a current timestamp;

The token described in step 3 consists from two parts: unique in system id of the follower that is assigned by the leader and expiration time stored in UTC format. This token may or may not have duration limitation depending on a group type. If private group is open only for a limited amount of time then this field is filled, otherwise it is empty. After keys exchanging and authentication processes are complete the follower can connect to other followers using connection information received in the last step. For accomplishing connection establishment between peers they must exchange their tokens and check their validity. As the token signed by the leader with its private key that other peers don't know it

makes forgery nearly impossible if use long-length keys. And at the same time validity of the token could be easily checked by the leader's public key that every peer already has. In the proposed approach we use a classical RSA scheme with 2048-bit length keys and SHA224 hashing algorithm for the digital signature that provides reasonable level of security, low overhead and high encoding throughput. However depending on application requirements these values could be changed.

In case when the token has an expiration time the receiving side also compares this with current system time converted to the leader's one and consider to disconnect the peer if it is already invalid. The converting is possible due to receiving leader's current timestamp in the step 3. While this time is not precise it is still useful for determination expiration time with accuracy equal to a half round-trip time between the follower and the leader that is usually not more than hundreds of milliseconds. In addition to the previous connection establishment time check the follower schedules an expiration check task that has timeout equal to that time. Such approach guarantees that peers will shuffle off expired neighbors even if they silently live in the network. The whole process of connection establishment described in a figure 1 below:

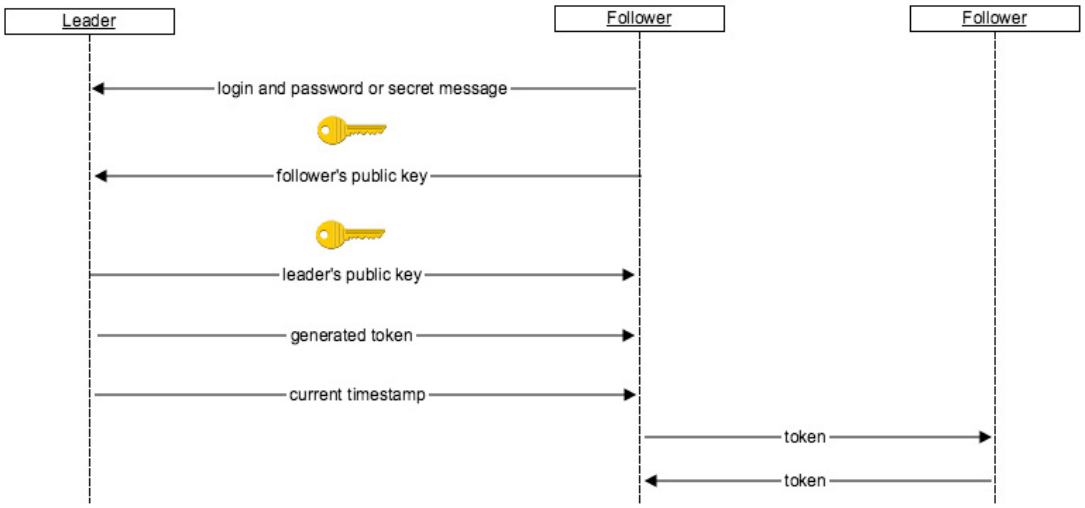


Figure 1. Connection establishment protocol between participants of the network.

Management processes and data dissemination in the private group

As it was previously mentioned proposed system is built on top of Tailcast [Hordiichuk, 2013] topology (figure 2). This topology contains of chain topology, where every peer has a connection with a successor node and at the same time it holds relations with all other peers at distances $2^k, k = \overline{1 \dots n}$, where n is a total amount of users in the network. Such approach is specially designed for low-delay

data dissemination due to ability of every peer reach nearby and far neighbors at the same time. Another important feature of this topology is a clear one-way directed path for data propagation algorithm that gives opportunity to push data without worrying of possible duplications. There are different types of data that could be distributed among peers in such network:

1. Video and audio data including live and on demand streaming;
2. Files of any type;
3. Text messages.

In this topology the leader has a unique ability of a swarm management. The main feature is secure data dissemination. It works as following: every message signed with the private key of the leader and whenever peers receive any data message it can validate it with the public key. It makes this process secure independently of an actual sender of the message. In all cases the source of these data is always the leader or a promoted follower that stands at the same network level in topology as the leader, for further simplicity we call this node “sender”. In newly created group there exists only one sender – the leader, but it can promote any follower by an appropriate command that is distributed among other peers in the network. As it was mentioned in the previous section during connection establishment process between the leader and the follower, the exchange their public keys. So for accomplishing promoting task the leader needs to distribute the public key of that peer that also should be signed by the leader’s private key. After peers receive public keys they can ensure that all messages from the promoted user are valid. In case of the opposite task when the leader wants to refuse in access it can execute a similar process and send a new command that will forfeit promotion. Both of these commands are completely distributed and there is no need to have direct connection between the leader and the promoted follower.

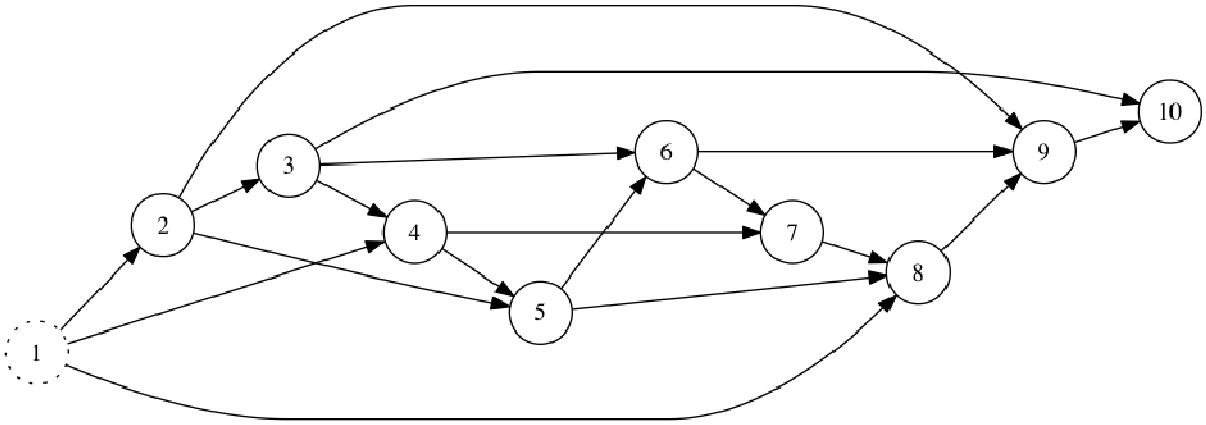


Figure 2. The Tailcast topology. Dotted node represents the leader and solid nodes represent followers.

Another important functions that should have any owner of the private group are banning and kicking users. It is achieved by a similar approach, where the leader sends a signed message to other participants in the network. As it was described in the previous section, during the handshaking process peers also pack their unique ids into the token that help them to identify each other. With this knowledge it also becomes possible to implement ban and kick command. When the follower receives one of these commands and if corresponding id exists in its neighborhood list, it immediately closes connection with that peer. In case when this is the ban command, its receiver also put this id in a ban list and if someone in future will try to connect with the same token it will silently dismiss this proposition and drop the connection. As well as other commands these ones also execute in completely distributed manner.

All information in the Tailcast is distributed using internal stream entity. An elementary information unit is a chunk with a length not more than 1300 bytes that is a typical minimal of MTU (Maximum Transmission Unit) in the Internet. Tailcast data dissemination algorithm guarantees that all chunks will be processed in a correct order and exactly one time. Therefore in this system we pack commands into such chunks. An assurance in order correctness in turn guarantees that all commands will be correctly executed on every peer. However in order to implement distributed chat function we cannot use this approach, as the source of this data could be every peer in the swarm and it is obvious that all of them can't be promoted followers at one time due to the fact that the topology becomes invalid. So for avoiding this problem peers use simple gossip protocol with signing their messages using their private keys. By gossip protocol we mean following conventions between all participants in the network:

1. The peer that is a source of the message generates a random id for it and signs it with own private key. After that peer sends the message to all known neighbors;
2. A receiver of the message proxies it to other peers in its own neighborhood except the sender and put in its history list. In case when there exists another message with the same id in the history list it just ignores it that means both processing and resending avoidance. Every message in history has a time-to-live limitation that is equal to 10 minutes (configurable parameter).
3. Every participant of the network is programmatically limited in its possible sending rate that is equal to 1 message per second (configurable parameter). If the user wants to send with a higher rate than it is alerted with corresponding message about sending rate excess;
4. In case when someone exceeds the sending rate, the receiver side silently drops that connection and does not transmit last message to other peers.

These conventions guarantee that every chat message will be delivered securely and avoid possibility of distributing spam. It is obvious that messages could appear in different order on different computers due to network delay. While it is possible to avoid this problem by using leader's clock information that every

peer knows and delaying messages before displaying them on monitor for previous fetching, it also introduces noticeably delay that significantly impacts on user experience. That is why in our system we display all messages right after they received. Also all gossip protocols have “at least once” message delivery that on the one hand guarantees delivery and on the other introduce transmission overhead at every node that is equal to a number of relations with other peers. However we believe that is a reasonable overhead due to a sending rate limitation that will not impact on system performance comparing with video and file data that is distributed in the network.

Implementation details

While there exists lot of other protocol stacks like BitTorrent’s UTP or even raw UDP sockets that gives ability to implement this system with a minimum overhead and maximum flexibility, all of them need installing additional software on your computer. As it was previously mentioned in the beginning of the paper this system is implemented using WebRTC stack, which makes possible to run a system inside a web page of a browser. This feature is obviously very important for integrating into any modern e-learning system and that is why we have chosen exactly WebRTC and JavaScript as a language. At the same time this technology has limitations. First of all this is still a young technology and currently only the latest versions of Firefox and Chrome browsers support it. Also one of the most important behavior of WebRTC client is bidirectional connection establishing process called SDP (Session Description Protocol) that is impossible without a helper server or node. In our system the leader helps to establish connection with first peers in the system and after that every follower independently discovers the network using neighbors as helpers. This pattern is implemented in P framework (http://ozan.io/p/) that can establish connection using both WebRTC and WebSocket as helper signaling servers and that is why we use it in our system. For WebSocket signaling server case we have implemented a node.js backend application that helps to find the leader of the group.

Also we have faced with a problem that all browsers do not have built-in support of RSA algorithms as well as SHA hashing that makes implementation of this system more difficult. But fortunately for us there exists open-source projects jsrasign (http://kjur.github.io/jsrsasign/) and Javascript Cryptography Toolkit (http://ats.oka.nu/titaniumcore/js/crypto/readme.txt) that contain signing and hashing functionality as well as capabilities for private and public key generation. It should be mentioned that WebRTC protocol provides encrypted message data layer and thus there is no need to additionally encrypt all messages for defending from man in the middle attack.

Conclusion

In this paper proposed a new peer-to-peer system on top of the Tailcast topology that is designed for a secure private group creation that could be integrated to existing e-learning system. Unlike existing approaches of creating secure peer-to-peer networks that rely on peer's reputation, this system uses public key and token exchanging protocol that helps to verify commands from the teacher and establish connections only with those peers that were previously authorized. It guarantees that all data will be delivered only to authorized peers and at the same time malicious peers could not substitute data that provides a certain level of privacy. On top of this protocol different management commands implemented including kicking and banning users as well as granting other peers rights to run these commands. Separately considered function of chat messages dissemination that is based on the gossip protocol with strict sending rate restrictions. Combining these approaches on the one hand guarantee that all messages will be delivered to all recipients and on the other hand it has strong defense from possible spam attacks.

We attempted to implement a system that is secure, distributed, scalable and at the same time can provide reasonable level of privacy. An execution process of all commands is completely distributed that makes this system scalable and usage of digital signage approach provides privacy. Combining these benefits with that fact this system can ran in modern browsers opens the possibility of creating new type e-learning systems.

Bibliography

[Hordiichuk, 2013] O.V. Hordiichuk. Tailcast — A Distributed Multicast System with Low End-User Delays. In: Theoretical and Applied Aspects of Cybernetics. Proceedings of the 3rd International Scientific Conference of Students and Young Scientists — Kyiv: Bukrek, 2013. 279-286.

[Maymounkov, 2002] Maymounkov, Petar, and David Mazieres. "Kademlia: A peer-to-peer information system based on the xor metric." Peer-to-Peer Systems. Springer Berlin Heidelberg, 2002. 53-65.

[Stoica, 2001] Stoica, Ion, et al. "Chord: A scalable peer-to-peer lookup service for internet applications." ACM SIGCOMM Computer Communication Review 31.4 (2001): 149-160.

[Magharei, 2009] Magharei, Nazanin, and Reza Rejaie. "Prime: Peer-to-peer receiver-driven mesh-based streaming." IEEE/ACM Transactions on Networking (TON) 17.4 (2009): 1052-1065.

[Xiong, 2004] Xiong, Li, and Ling Liu. "Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities." Knowledge and Data Engineering, IEEE Transactions on 16.7 (2004): 843-857.

[Zhao, 2013] Zhao, Huanyu, and Xiaolin Li. "VectorTrust: trust vector aggregation scheme for trust management in peer-to-peer networks." The Journal of Supercomputing 64.3 (2013): 805-829.

[Can, 2013] Can, Ahmet Burak, and Bharat Bhargava. "Sort: A self-organizing trust model for peer-to-peer systems." Dependable and Secure Computing, IEEE Transactions on 10.1 (2013): 14-27.

[Gupta, 2003] Gupta, Minaxi, Paul Judge, and Mostafa Ammar. "A reputation system for peer-to-peer networks." Proceedings of the 13th international workshop on Network and operating systems support for digital audio and video. ACM, 2003.

[Hoßfeld, 2008] Hoßfeld, Tobias, and Andreas Binzenhöfer. "Analysis of Skype VoIP traffic in UMTS: End-to-end QoS and QoE measurements." Computer Networks 52.3 (2008): 650-666.

Authors' Information

Oleh Hordiichuk *– postgraduate student in Taras Shevchenko National University of Kyiv, faculty of information technologies, Kyiv, Ukraine; e-mail: oleg.gordichuck@gmail.com*

Major Fields of Scientific Research: Peer-to-peer networks, distributed computing, networking and e-learning

Oleksiy Bychkov *– docent, PhD in physics and mathematics, deputy dean of academic affairs in Taras Shevchenko National University of Kyiv, faculty of information technologies, Kyiv, Ukraine; e-mail: bos.knu@gmail.com*

Major Fields of Scientific Research: E-learning, theory of programming, mathematical foundations in information technologies

ИСПОЛЬЗОВАНИЕ МЕТОДОВ ТЕОРИИ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ УСОВЕРШЕНСТВОВАНИЯ ПРОЦЕССА СИНТЕЗА СЕТЕЙ ДОСТУПА

Галина Гайворонская, Мария Хильчук

Аннотация*: Проанализирован процесс синтеза сетей доступа и возможность использования методов теории принятия решений для решения отдельных задач этого процесса. Выбраны и обоснованы методы теории принятия решений, наиболее целесообразные для повышения эффективности процесса синтеза сетей доступа.*

Ключевые слова*: синтез сетей доступа, методы теории принятия решений. топологическая структура сети, технологии передачи информации*

ACM Classification Keywords*: H. Information Systems – H.1 Models and Principles, E. Data – E.0 General.*

Введение

Создание сетей доступа (СД) в настоящее время является одной из важнейших задач сферы инфокоммуникаций. Стандартизацией и разработкой рекомендаций в области синтеза СД занимаются ведущие мировые организации, наиболее известными из которых являются: Международный союз электросвязи (МСЭ) [ITU G.902], институт инженеров по электронике и электротехнике [IEEE 802], Европейский и Американский институты по стандартизации в области телекоммуникаций и другие. Каждой из этих организаций уже разработан ряд рекомендаций, связанных с созданием СД, но несмотря на это осталось еще много нерешенных вопросов. Концепция, определяющая суть СД, сформирована в рекомендации МСЭ G.902, согласно этой концепции предполагается создание единой сети, обеспечивающей доступ ко всем базовым сетям с целью предоставления пользователям всего спектра инфокоммуникационных услуг (ИКУ) по одной линии доступа (ЛД) с гарантированным уровнем качества обслуживания [ITU G.902]. Актуальность реализации концепции СД обусловлена тем, что существующие абонентские линии отдельных базовых информационных сетей не справляются с задачей обеспечения гарантированного качества обслуживания пользователей, требования к которому в современных условиях стремительного расширения спектра ИКУ постоянно возрастают. Поскольку методы синтеза СД в полной мере еще не разработаны, в связи с тем, что сама

концепция СД появилась сравнительно недавно их разработка весьма важна и актуальна. В работе предложен подход, предусматривающий для этой цели применение методов теории принятия решений. Синтез СД предусматривает решение множества задач выбора, к которым в частности относятся выбор: топологической структуры сети, технологий передачи данных, телекоммуникационного оборудования, программного обеспечения и т.д. Решение этих задач предполагает рассмотрение и анализ большого количества альтернатив, что во многом и определяет трудоемкость и слабую формализацию процесса синтеза СД. Теория принятия решений (ТПР) включает способы и процедуры формализации процесса принятия решений, под которым понимается определенный вид человеческой деятельности, ориентированный на установление наилучшего варианта действий [Черноморов, 2002]. Целью данного исследования является повышения эффективности процесса синтеза СД путем применения методов ТПР. Объект исследования – процесс синтеза СД, предмет – методы теории принятия решений.

Анализ процесса синтеза сети доступа

Процесс синтеза СД представлен на Рис. 1 в виде алгоритма [Гайворонская, 2012]. Первый этап является, в некотором виде, подготовительным, здесь определяется перечень ИКУ, которые могут затребовать потенциальные пользователи синтезируемой сети, затем все пользователи сети распределяются по группам с одинаковым перечнем предоставляемых ИКУ. На втором этапе формируются требования к сети, выдвигаемые пользователями для предоставления всего спектра затребованных ими ИКУ. Эти требования зависят от класса ИКУ и регламентируются на основании отечественных и международных нормативных документов. Согласно концепции качества обслуживания (Quality of Service, QoS), класс ИКУ нормирует значения времени задержки, вариации времени задержки, доли потерянных пакетов и пакетов с ошибками, кроме того определен приоритет предоставления ИКУ (например, услуги класса А предоставляются в первую очередь) [ITU E.360.4; ITU E.361]. На третьем этапе выделяются фрагменты территории, на которых расположены пользователи, относящиеся к отдельным секторам. Здесь под сектором понимается территория, на которой расположены пользователи одной группы. При этом сектор может состоять из отдельных фрагментов территории не имеющих общих границ, а фрагменты территорий различных секторов могут накладываться друг на друга. Информационные потоки от отдельных пользователей к различным базовым сетям концентрируют узлы доступа (УД) [Гайворонская, 2008]. Путем технико-экономического анализа вариантов топологии СД принимается решение о целесообразности организации двухуровневой структуры проектируемой сети, предусматривающей подключение пользователей к узлам, предоставляющим обслуживание (УПО), через два последовательно соединенных УД с целью обеспечения минимизации длины локального сегмента ЛД (ЛСЛД).

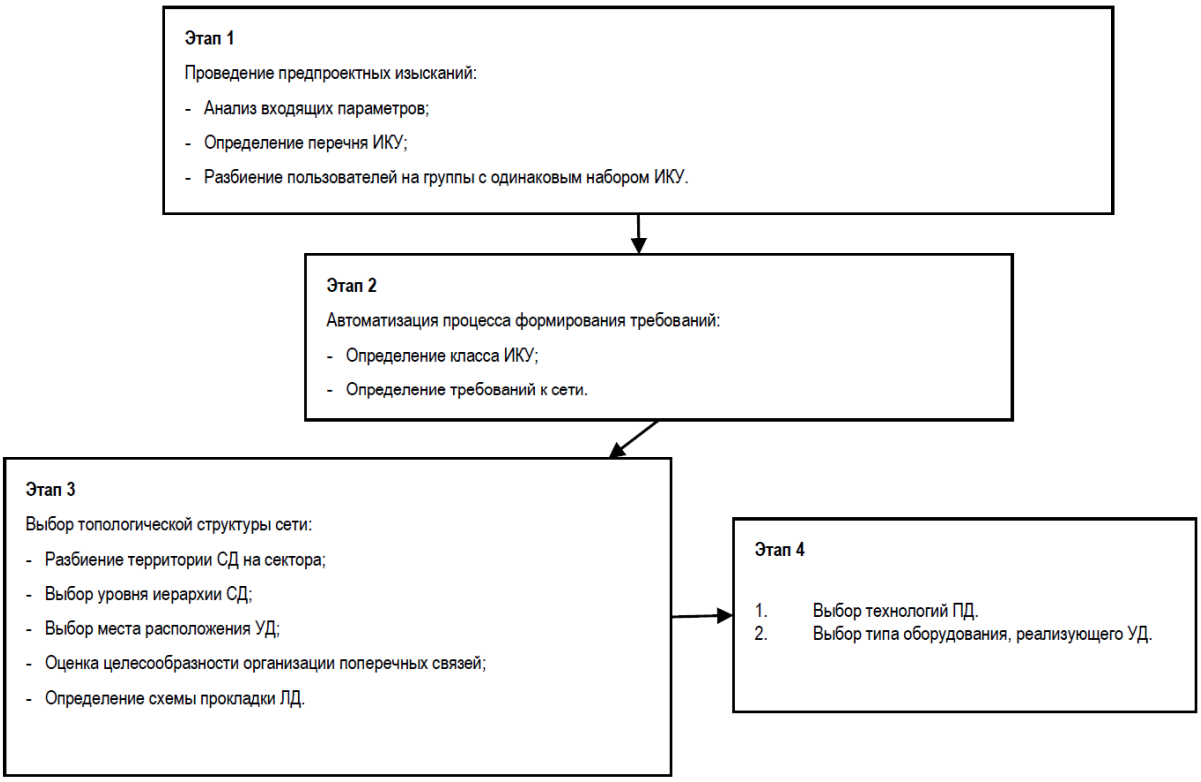


Рисунок 1. Алгоритм проектирования сети доступа

Начиная с четвертого этапа целесообразно применять методы ТПР, так как на нем, на основании технического задания и с учетом прогнозируемых параметров синтезируемой СД, формируется структурная и функциональная схемы сети. Для этого необходимо выполнить выбор технологии передачи информации, оборудования для её реализации и типа УД, концентрирующего информационные потоки от отдельных пользователей к различным базовым сетям [Гайворонская, 2008]. Основная задача на этом этапе: выбрать наилучший вариант структуры СД из всех возможных, а для этого необходимо рассмотреть и проанализировать достаточно большое количество альтернатив. При применении ТПР этот процесс можно сделать менее трудоемким, определив цель, которая в конечном результате должна обеспечиваться, параметры сети (показатели приемлемости) и упорядочив перечень альтернатив.

Путем анализа задач, решение которых необходимо при создании СД, можно сделать вывод, что методы ТПР целесообразно использовать на завершающих этапах синтеза СД. К задачам синтеза СД, для решения которых целесообразно применить методы ТПР, можно отнести:

- Определение топологии сети;
- Выбор технологии транспортировки информации по линиям доступа;
- Выбор типа оборудования, реализующего узлы доступа.

При решении этих задач необходимо учитывать множество параметров как СД, так и пользователя. К параметрам СД (Π_M), в рамках данного исследования относятся:

1. Географическое размещение разных групп пользователей (χ_{Gp}).
2. Длина (L) и пропускная способность (PS_{ld}) ЛД.;
3. Количество (N_{YD}), место размещения (χ_{YD}) и пропускная способность (PS_{YD}) УД.
4. Качество предоставления услуг (Ψ):
   - Коэффициент ошибок (k_o);
   - Время задержки (t_z);
   - Время отклика сети (t_{ot});
   - Информационная скорость (ν_i);
5. Тип передаваемой информации (θ_i);
6. Суммарная нагрузка, создаваемая всеми пользователями сети (Y);
7. Расходы на проектирование и эксплуатацию сети (R).

$$\Pi_M\left(\chi_{Gp}, L, PS_{ld}, N_{YD}, \chi_{YD}, PS_{YD}, \Psi\left(k_o, t_z, t_{ot}, \nu_i\right), \theta_i, Y, R\right) \quad (1)$$

Параметры пользователя (Π_p) учитывают:

1. Местонахождение (координаты) пользователя (K_p);
2. Удельную нагрузку, создаваемую пользователем (Y_p);
3. Перечень услуг, которые будут предоставляться пользователю (V_y);
4. Пропускную способность ЛСЛД, необходимую для предоставления ИКУ (PS_p).

$$\Pi_p\left(K_p, Y_p, V_y, PS_p\right) \quad (2)$$

Согласно этим характеристикам формируется цель, которой должен удовлетворять оптимальный метод решения конкретной задачи синтеза СД.

Анализ методов теории принятия решений

Поскольку существует большое количество методов ТПР, а каждая из задач синтеза СД имеет свои особенности, не все методы могут применяться в рамках любых задач синтеза СД и давать результат, удовлетворяющий цели исследования. Поэтому необходимо провести анализ существующих методов ТПР и определить, какие методы целесообразно использовать в рамках каждой из задач синтеза СД. В связи с этим, следующим этапом проведения исследования является решение задач выбора методов ТПР с помощью лексикографического критерия, позволяющего учитывать в качестве дополнительной информации важность каждого показателя приемлемости, имеющих разное влияние на результат в рамках решения каждой из поставленных задач. Для каждой из задач синтеза СД изначально формируется цель, которой должен удовлетворять результат выбора. Далее все методы анализируются на предмет соответствия поставленной цели, и выбирается наиболее подходящий из них.

Для применения в рамках задач, возникающих в процессе синтеза СД, анализируется 25 методов ТПР [Волошин, 2006].

1. Минимаксный критерий (*MM*).
2. Критерий Байеса-Лапласа (*BL*).
3. Модальный критерий (*Mod*).
4. Критерий Севиджа (*S*).
5. Критерий Гурвица (*G*).
6. Критерий Ходжа-Лемана (*HL*).
7. Критерий Гермейера (*Gr*).
8. Критерий произведений (*D*).
9. Критерий минимизации дисперсии оценки (D_{min}).
10. Критерий максимизации вероятности (P_{max}).
11. Метод анализа иерархий (*MAI*).
12. Метод дерева решений (*MDR*).
13. Критерий оптимальности за Слейтером (*C*).
14. Критерий оптимальности за Парето (*P*).
15. Аддитивный критерий (*Ad*).
16. Мультипликативный критерий (*Mp*).
17. Лексикографический критерий (*Lex*).

18. Метод идеальной точки (*MIT*).
19. Метод выбора за количеством доминирующих критериев (*Dk*).
20. Метод последовательных уступок (*PY*).
21. Метод последовательного ввода ограничений (*PO*).
22. Метод желаемой точки (*ZT*).
23. Метод удовлетворенных требований (*YT*).
24. Метод векторной релаксации (*VR*).
25. Метод динамического программирования (*DP*).

Для оценки целесообразности их использования в процессе синтеза СД в качестве показателей приемлемости альтернатив определены следующие характеристики методов ТПР:

- Тип входящих параметров (численный или качественный);
- Тип метода (графический или численный);
- Наложение условий на количество входящих данных (в случаях, когда необходимо анализировать множество альтернатив);
- Возможность реализации решения бесконечное число раз;
- Зависимость результата работы метода от отброшенных альтернатив;
- Учет состояний внешней среды;
- Условия, в которых принимается решение;
- Структурированность задачи;
- Допустимость риска для результата работы (при этом под риском понимается возможная вероятность отклонения значений характеристик предоставления ИКУ от показателей QoS, определенных в нормативной документации, и зависящих от класса ИКУ).

Множество этих характеристик можно выразить выражением:

$$P = \{r; T_{Пвх}; T_D; T_V; T_R; S; US; DA; R; E; F; T_M\} \quad (3)$$

Выбор методов ТПР для задачи синтеза топологической структуры сети доступа

На первом этапе анализа методов ТПР определяются характеристики, которым должен удовлетворять выбранный метод ТПР и степень их важности для решения данной задачи. Для решения задачи синтеза топологической структуры сети доступа правило выбора сформировано следующим образом:

- Входящие данные качественного и количественного типа $(T_{Пвх} = "Kach / Kol")$;
- Принятие решения может происходить в условиях: определенности $(T_D = "+")$, неопределенности $(T_V = "+")$ и в условиях риска $(T_R = "+")$;
- Задача является плохо структурированной $(S = "-", US = "+")$;
- Необходимо учитывать состояние внешней среды $(E = "+")$;
- В этой задаче риск не допустим либо допустим в незначительной степени $(F = "-")$, ведь для синтеза СД важным показателем является качество предоставления всего спектра ИКУ пользователю, поэтому при проектировании топологической схемы сети необходимо учитывать этот показатель и обеспечить его выполнение;
- Метод может использоваться неоднократно и характеристики альтернатив не должны изменяться $(R = "+")$;
- Вариантов схемы прокладки ЛД достаточно много, но ограничением по количеству входящих параметров $(r = "H / O")$ для метода принятия решения в данной задаче можно пренебречь, поскольку входящие альтернативы можно разбить на несколько групп и таким образом уменьшить количество входящих параметров;
- При применении метода могут учитываться или не учитываться отброшенные альтернативы $(DA = "+ / -")$;
- Метод может быть как количественного, так и графического типа $(T_M = "Kol / G")$.

Общее правило выбора для первой задачи имеет вид:

$$P_1 = \{Kach / Kol; +; +; +; -; +; +; -; +; H / O; + / -; Kol / G\} \quad (4)$$

Этому правилу полностью удовлетворяют три метода: анализа иерархий, динамического программирования и дерева решений. Это значит, что для оптимизации процесса синтеза СД можно использовать любой из этих трех методов ТПР.

Выбор методов ТПР для задачи выбора технологии транспортировки информации по линиям доступа

Характеристики правила выбора для этой задачи:

- Значение показателя приемлемости не должно ограничивать количество входящих параметров, т.к. выбор технологий обычно осуществляется из большого количества альтернатив $(r = "H")$;
- Входящие параметры должны быть количественного типа $(T_{Пвх} = "Kol")$;
- Выбор может осуществляться в условиях определенности $(T_D = "+")$ и неопределенности $(T_V = "+")$, принятие решения в условиях риска в данном случае не допускается $(T_R = "-")$;
- Задача является плохо структурированной $(S = "-", US = "+")$;
- Риск для результатов работы метода не допускается или, если и допускается, то незначительный $(F = "-")$;
- Необходимо учитывать состояние внешней середы $(E = "+")$;
- Метод может использоваться по несколько раз для одной и той же альтернативы $(R = "+")$;
- Результат может зависеть или не зависеть от отброшенных альтернатив $(DA = "+/-")$;
- Метод может быть как количественного, так и графического типа $(T_M = "Kol / G")$.

Все показатели приемлемости упорядочены по важности в том порядке, в котором они были охарактеризованы. В результате общее правило для задачи выбора технологии передачи информации имеет вид:

$$P_2 = \{H; Kol; +; +; -; -; +; -; +; +; -/+; Kol / G\} \quad (5)$$

Путем сравнения альтернатив выбраны два метода, удовлетворяющие сформированной цели: последовательного ввода ограничений и идеальной точки.

Определение методов ТПР для задачи выбора типа оборудования, реализующего УД

Для этой задачи правило выбора составляется таким же образом, как и для предыдущих задач, и имеет следующие характеристики:

- Входящие параметры должны быть количественного типа $(T_{Пвх} = "Kol")$;
- Выбор может осуществляться и в условиях определенности $(T_D = "+")$ и в условиях неопределенности $(T_V = "+")$, условия риска не допускаются $(T_R = "-")$;
- Задача является хорошо структурированной $(S = "+", US = "-")$;
- Риск для результата сравнения альтернатив не допускается $(F = "-")$;
- Состояние внешней среды может не учитываться $(E = "-")$;
- Ограничения на количество входящих параметров может, как накладываться, так и не накладываться, ведь альтернатив среди оборудования не очень много $(r = "H / O")$;
- Результат может зависеть или не зависеть от отброшенных альтернатив $(DA = "+ / -")$;
- Параметр реализации решения бесконечное число раз не влияет на результат решения $(R = "+ / -")$;
- Метод может быть как количественного, так и качественного типа $(T_M = "Kol / G")$.

Исходя из этого, правило для этой задачи имеет вид:

$$P_3 = \{Kol; +; +; -; +; -; -; -; H / O; - / +; - / +; Kol / G\} \quad (6)$$

Требованиям задачи выбора типа оборудования, реализующего УД удовлетворяет только один метод ТПР – метод выбора по количеству доминирующих критериев.

Анализ метода идеальной точки для применения в процессе выбора технологии передачи информации

Анализ применения одного из выбранных методов ТПР в процессе синтеза СД, а именно метода идеальной точки для задачи выбора технологии передачи информации по ЛД, выполнен на следующем примере. Создаётся СД в поселке городского типа площадью 10 $км^2$ с радиальной моделью структуры населённого пункта и численностью населения 3000 человек. В поселке расположено озеро, представляющее собой „препятствие", которое необходимо учитывать при синтезе СД. Синтезируемая сеть должна обслуживать 100% территории поселка. Для выбора технологий определен спектр ИКУ, предоставляемых пользователям. Пользователи СД разбиты на пять групп, при этом к одной группе отнесены все пользователи, требующие, один и тот же перечень ИКУ. Для каждой из сформированных групп определено местоположение УД.

Выбор технологий передачи информации по ЛД выполнен для таких альтернативных технологий доступа: VDSL; ADSL; HDSL; Ethernet (10BASE-T); Fast Ethernet (Ethernet 100BASE-T); Gigabit Ethernet (Ethernet 1000BASE-T); GPON (PON); SONET/SDH; WiMax; WCDMA; DECT. Эти альтернативы охарактеризованы следующими параметрами, определяющими выбор показателей приемлемости:

- Скорость передачи данных;
- Длина линии доступа либо область обслуживания при применении беспроводных технологий;
- Тип линии;
- Учет помех (накладывает ли помеха ограничение на организацию сети, реализованной на рассматриваемой технологии);
- Особенности применения технологии для транспортного и локального сегментов доступа: (СТД и СЛД, соответственно);
- Относительная стоимость реализации технологии доступа.

Характеристика альтернатив согласно перечню показателей приемлемости, основанная на анализе источников [Лаборатория; Winncom; Sysadm; Связь комплект; Шоберг; Broadband; Cdma; ПСТМБС], приведена в Табл.1.

Таблица 1. Характеристики технологий передачи информации

Технология	Характеристики					
	Скорость передачи данных	Длина линии передачи	Тип линии передачи	Особенности	Учет помех	Стоимость
1	2	3	4	5	6	7
VDSL (асиметричная)	восходящий поток– 13Мб/с нисходящий поток – 1,6Мб/с восходящий поток – 52Мб/с нисходящий поток. – 2,3Мб/с	до 1,5км до 300м	медный кабель	СЛД	ограничена	невысокая
ADSL	восходящий поток – 8Мб/с нисходящий поток – 1Мб/с	до 100м	медный кабель	СЛД	ограничена	низкая
HDSL	до 2,3Мб/с	6,5км	медный кабель	СЛД	ограничена	невысокая
Ethernet 10BASE-T	10Мб/с	100м	витая пара	СЛД	ограничена	средняя
Ethernet 100BASE-T	100Мб/с	100м	витая пара	СЛД	ограничена	средняя
Ethernet 1000BASE-T	1000Мб/с (1Гб/с)	100м	витая пара	СЛД	ограничена	средняя
GPON (PON)	1200Мб/с (1,2Гб/с)	20км	оптоволокно	СТД	ограничена	высокая

SDH (SONET)	155Мб/с – 2,5Гб/с (в зависимости от иерархии)	20км	оптоволокно	СТД	ограничена	высокая
WiMax	до 75Мб/с	6-10км	радиоканал	СЛД	не ограничена	средняя
WCDMA (CDMA)	до 2Мб/с	4,5км	радиоканал	СЛД	не ограничена	средняя
DECT (WLL)	до 2Мб/с	до 10км	радиоканал	СЛД	не ограничена	средняя

Метод идеальной точки предусматривает наличие идеальных значений показателей приемлемости, которые для рассматриваемой задачи приведены в Табл. 2.

Таблица 2. Характеристики синтезируемой сети доступа

	Характеристики					
	Скорость передачи данных	Длина линии передачи	Тип линии передачи	Особенности	Учет помех	Стоимость
Группа 1	8,6Мб/с	93м	витая пара	СЛД	озеро	мин.
Группа 2	583кб/с	9км	радиоканал	СЛД	озеро	мин.
Группа 3	5,2Мб/с	111м	витая пара	СЛД	озеро	мин.
Группа 4	4,3Мб/с	100м	медный кабель	СЛД	нет	мин.
Группа 5	8,6Мб/с	69м	витая пара	СЛД	нет	мин.

УД1 –УПО1	267Мб/с	450м	оптоволокно	СТД	нет	мин.
УД1 –УПО2	165Мб/с	320м	оптоволокно	СТД	нет	мин.
УД1 –УПО3	7,4Гб/с	600м	оптоволокно	СТД	озеро	мин.
УД2 –УПО1	169,7Мб/с	550м	оптоволокно	СТД	нет	мин.
УД2 –УПО2	68,9Мб/с	350м	оптоволокно	СТД	нет	мин.
УД2 –УПО3	67,2Мб/с	650м	оптоволокно	СТД	озеро	мин.
УД3 –УПО1	453,3Мб/с	600м	оптоволокно	СТД	нет	мин.
УД3 –УПО2	2Гб/с	700м	оптоволокно	СТД	нет	мин.
УД4 –УПО1	53,8Мб/с	300м	оптоволокно	СТД	нет	мин.
УД4 –УПО2	32Мб/с	350м	оптоволокно	СТД	нет	мин.
УД4 –УПО3	1,1Гб/с	500м	оптоволокно	СТД	нет	мин.
УД5 –УПО1	209,1Мб/с	800м	оптоволокно	СТД	нет	мин.
УД5 –УПО2	93,7Мб/с	1100м	оптоволокно	СТД	озеро	мин.
УД5 –УПО3	8,8Гб/с	200м	оптоволокно	СТД	нет	мин.

После определения параметров СД, которые должны соответствовать поставленной цели, в результате использования выбранной альтернативы выполнено сравнение параметров альтернатив на соответствие параметрам „идеальной” точки („идеальным” параметрам), для этого определяем расстояние между параметрами „идеальной” точки и параметрами

рассматриваемой технологии. Расстояние в метрическом пространстве определяется по формуле [Волошин, 2006]:

$$\rho_s(y,a)=\left(\sum_{i=1}^{m}|y_i-a_i|^s\right)^{\frac{1}{s}}, \quad (7)$$

где ρ_s - расстояние в метрическом пространстве между „идеальной" точкой и альтернативой;

y_i - параметры альтернатив;

a_i - параметры „идеальной" точки;

s - значение метрики, выбирается в зависимости от предметной области, в данном случае $s=1$, ведь характеристики имеют не только численные значения и учитываются все характеристики с одинаковым уровнем важности для принятия правильного решения, поэтому расстояние до „идеальной" точки определяется как суммарное несвязанное по всем критериям.

Таким образом, скаляризованная задача может быть представлена выражением [Волошин, 2006]:

$$\min\sum_{i\in M}|y_i-a_i|=\max\sum_{i\in M}y_i \quad (8)$$

Так как критерии задачи имеют разные шкалы (единицы измерения), то их необходимо свести их к безразмерной шкале [0,1, ...] следующим образом:

1. Длина сегмента линии доступа: 1000м = 1км.
2. Тип линии передачи:
   - Медный кабель – 1;
   - Витая пара – 2;
   - Оптоволокно – 3;
   - Радиоканал – 4.
3. Особенности:
   - СЛД – 1;

- СТД – 2.

4. Препятствия:

4.1. Для альтернатив:

- Ограничено – 2;
- Не ограничено – 1;

4.2. Для проектируемой СД:

- Озеро – 1;
- Нет – 2;

4.3. Если для организации ЛД для группы пользователей нет препятствий, то коэффициент равен 0.

5. Стоимость:

- Низкая, минимальная – 1;
- Невысока – 2;
- Средняя – 3;
- Выше средней – 3,5;
- Высокая – 4.

6. Скорость передачи данных: 1000Мб/с = 1Гб/с (только для СТД).

Затем определяем расстояние до „идеальной” точки отдельно для каждой из групп пользователей и отдельно для каждого фрагмента СТД. Для определения оптимальной альтернативы решения задачи находимо рассчитать минимальное расстояние к „идеальной” точке. При определении оптимального варианта решения задачи важным является тот факт, что значение скорости передачи информации и длины сегмента линии доступа должны быть не меньше, чем определенное для синтезируемой СД, но может быть больше, поэтому, если альтернатива удовлетворяет „идеальным” параметрам каждой из этих характеристик, то для обеих характеристик коэффициент расстояния приравнивается к 0. Согласно рассчитанным характеристикам синтезируемой СД для первой группы пользователей, приведенным в табл. 2, и после перехода к безразмерным значениям характеристик определяется расстояние до „идеальной” точки для каждой из альтернатив в соответствии с формулой. Для первой группы пользователей:

VDSL: $\rho_s = |2,3-8,6| + 0 + |1-2| + |1-1| + |2-1| + |2-1| = 9,3;$

ADSL: $\rho_s = |1-8,6| + 0 + |1-2| + |1-1| + |2-1| + |1-1| = 9,6;$

HDSL: $\rho_s = |2,3-8,6| + 0 + |1-2| + |1-1| + |2-1| + |2-1| = 9,3;$

10BASE-T: $\rho_s = 0 + 0 + |2-2| + |1-1| + |2-1| + |3-1| = 3;$

100BASE-T: $\rho_s = 0 + 0 + |2-2| + |1-1| + |2-1| + |3-1| = 3;$

1000BASE-T: $\rho_s = 0 + 0 + |2-2| + |1-1| + |2-1| + |3-1| = 3;$

GPON: $\rho_s = 0 + 0 + |3-2| + |2-1| + |2-1| + |4-1| = 6;$

SDH: $\rho_s = 0 + 0 + |3-2| + |2-1| + |2-1| + |4-1| = 6;$

WiMax: $\rho_s = 0 + 0 + |4-2| + |1-1| + |1-1| + |3-1| = 4;$

WCDMA: $\rho_s = |2-8,6| + 0 + |4-2| + |1-1| + |1-1| + |3,5-1| = 11,1;$

DECT: $\rho_s = |2-8,6| + 0 + |4-2| + |1-1| + |1-1| + |3,5-1| = 11,1.$

После определения расстояний между значениями характеристик „идеальной” точки и альтернатив, определяется минимальное расстояние до „идеальной” точки. Альтернатива, имеющая минимальное расстояние, выбирается в качестве лучшего варианта. Для данной задачи наименьшее расстояние имеют сразу три альтернативы: 10BASE-T, 100BASE-T, 1000BASE-T. Исследователь может выбрать любую из них. Для этого ему необходимо учесть, что при реализации выбранной технологии их стоимость будет отличаться между собой: наиболее дешевой будет технология 10BASE-T, которая полностью удовлетворяет требованиям к синтезируемой сети. Если же в будущем планируется увеличение необходимой пропускной способности, то можно выбрать одну из более высокоскоростных технологий 100BASE-T или 1000BASE-T, стоимость которых будет несколько выше.

На основании тех же принципов происходит выбор технологи передачи для всех остальных сегментов СД, в результате чего получаем:

- Для первой, третьей и пятой группы пользователей для организации передачи данных пользователей к УД лучше применить технологии семейства Ethernet: 10BASE-T, 100BASE-T, 1000BASE-T;

- Для удовлетворения потребностей второй группы пользователей лучше выбрать технологию WiMax, поскольку она способна обеспечить покрытие всей обслуживаемой территории с соблюдением требований к качеству передачи данных;

- По техническим условиям на проектирование этой СД, для четвертой группы пользователей передача данных на локальном сегменте ЛД должна быть организована на основании использования существующей абонентской сети по медным парным телефонным линиям. Поэтому определено, что оптимальной технологией для организации доступа пользователей этой группы к ИКУ являются технологии VDSL и HDSL, хотя согласно результату применения метода идеальной точки для этой цели подходят также технологии 10BASE-T, 100BASE-T и 100BASE-T, которые не удовлетворяют условиям, а именно обеспечивают передачу информации только в цифровой форме и имеют более высокий параметр вариации задержки. При выборе конкретной технологии передачи следует заметить, что при решении задачи рассмотрена технология VDSL асимметричного типа, при этом выбор основан на более низкой скорости восходящего потока, скорость к пользователю значительно выше. Технология HDSL является симметричной, то есть имеет одинаковую скорость в обоих направлениях;

- Для организации сегмента транспортного доступа для всех групп пользователей, кроме четвертой, определена концепция GPON. Хотя, можно также использовать и технологию SDH, ведь при их сравнении за основу скорости передачи данных для этой технологии взята минимальная скорость, которая может быть увеличена на высших уровнях иерархии скоростей передачи.

Проведя анализ результатов использования метода идеальной точки целесообразно заметить, что его применение упрощает процесс выбора технологии передачи данных, используемых на линиях доступа проектируемой сети. При этом нет необходимости анализировать полностью все альтернативы, необходимо только определить показатели приемлемости и их значения для „идеальной” технологии и для всех рассматриваемых. К недостаткам метода, исходя из этого примера, можно отнести то, что с его помощью может быть определена не одна конкретная альтернатива, а несколько, удовлетворяющих поставленной цели. Также следует заметить, что в

процессе применения метода выбирается альтернатива, которая максимально удовлетворяет показатели приемлемости, но они могут быть удовлетворены не полностью.

Выводы

При проведении исследования определены задачи процесса синтеза СД, для решения которых целесообразно применять методы ТПР. При этом выбрано три задачи: определение топологической схемы сети, выбор технологии транспортировки информации по линиям доступа и выбор типа оборудования, реализующего узлы доступа. Для каждой из задач определены методы ТПР, которые лучше всего подходят для решения конкретных задач и учитывают особенности процесса синтеза СД. Выбрано шесть методов ТПР: анализа иерархий, динамического программирования и дерева решений для задачи выбора топологической структуры СД; метод последовательного ввода ограничений и метод идеальной точки для задачи выбора технологии передачи данных по ЛД и метод выбора по количеству доминирующих критериев для задачи выбора типа оборудования, реализующего УД. На конкретном примере рассмотрено применение метода идеальной точки для решения задачи выбора технологии передачи информации и определены его преимущества и недостатки. Применение всех, определенных в ходе исследования, методов может облегчить процесс синтеза СД при условии правильного и точного определения характеристик СД, которые необходимо учитывать при ее синтезе.

Литература

[ITU E.360.4] International Telecommunication Union ITU [Электронный ресурс] Режим доступа: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=5591. Дата обращения: 01.10.2014

[ITU E.361] International Telecommunication Union ITU [Электронный ресурс] Режим доступа: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=6246. Дата обращения: 01.10.2014

[ITU G.902] International Telecommunication Union ITU [Электронный ресурс] Режим доступа: http://www.itu.int/rec/T–REC–G.902–199511–I/en. Дата обращения: 01.10.2014

[Sysadm] Sysadm.pp.ua [Електронный ресурс] Режим доступа: http://sysadm.pp.ua/internet/standarty-ethernet.html. Дата обращения: 30.04.2015

[Winncom] Winncom Technologies [Електронный ресурс] Режим доступа: http://www.winncom.com.ua/upload/iblock/ 7c6/%20vqdenrfrgiaxtrdizg% 20DSL.pdf; Дата обращения: 29.04.2015

[Broadband] Broadband.org.ua [Електронный ресурс] Режим доступа: http://www.broadband.org.ua/tekhnologii-bystrogo-interneta/1311-chto-takoe-wimax-printsipy-raboty-wimax. Дата обращения: 02.05.2015

[Волошин, 2006] А.Ф. Волошин и С.О. Мащенко, "Модели и методы принятия решений", Научное пособие Издательско–полиграфический центр „Киевский университет", Киев, 2006.

[Гайворонская, 2008] Г.С. Гайворонская, "Сети и системы абонентского доступа", Часть 1, Технология информационных систем, Учебное пособие, Одесса, 2008.

[Гайворонская, 2012] Г. С. Гайворонская и А. А. Бондаренко. Задача выбора топологической структуры сети доступа, Problems of Computer Intellectualization. Kyiv–Sofia: National Academy of Sciences of Ukraine V.M.Glushkov Institute of Cybernetics, ITHEA, 2012, №28, pp. 252 – 261

[IEEE 802] Institute of Electrical and Electronics Engineers IEEE [Электронный ресурс], Режим доступа: http://standards.ieee.org/about/get/802/802.html. Дата обращения: 08.10.2014

[Лаборатория] Лаборатория „Обработки и передачи данных"„ [Електронный ресурс], Режим доступа: http://opds.sut.ru/old/electronic_manuals/sde/t6sde/xdsl_texn.htm. Дата обращения: 29.04.2015

[ПСТМБС] Портал о современных технологиях мобильной и беспроводной связи [Електронный ресурс], Режим доступа: http://1234g.ru/blog-of-wireless-technologies/46-dect/171-o-standarte-dect. Дата обращения: 02.05.2015

[Cdma] Информационный портал: Cdma.ru [Електронный ресурс], Режим доступа: http://www.cdma.ru/technology/ standart/cdma/. Дата обращения: 02.05.2015

[Связь комплект] Связь комплект [Електронный ресурс], Режим доступа: http://www.skomplekt.com/technology/ethernet.htm. Дата обращения: 30.04.2015

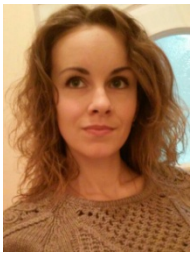
[Черноморов, 2002] Г.А. Черноморов, "Теория принятия решений", Научное пособие, Новочеркаск, 2002.

[Шоберг] Страница для студентов А. Шоберга Сети ЭВМ и Телекоммуникации [Електронный ресурс], Режим доступа: http://network-evm.narod.ru/lections/physicallayer/SDH/SDH.pdf. Дата обращения: 01.05.2015

Информация об авторах

Галина Гайворонская *– д.т.н., профессор, заведует кафедрой информационно-коммуникационных технологий факультета информационных технологий и кибербезопасности Института холода, криотехнологий и экоэнергетики им. В.С. Мартыновского ОНАПТ; ул. Дворянская, 1/3, Одесса-26, 65026, Украина; тел. (048)-720-91-48; e-mail: gsgayvoronska@gmail.com*

Главные области научных исследований: оптимизация переходных периодов при эволюции информационных сетей. Потоки вызовов, нагрузка и межузловое тяготение в сетях. Проблемы создания перспективных сетей доступа.



Мария Хильчук – магистр кафедры информационно-коммуникационных технологий факультета информационных технологий и кибербезопасности Института холода, криотехнологий и экоэнергетики им. В.С. Мартыновского ОНАПТ; ул. Дворянская, 1/3, Одесса-26, 65026, Украина; тел. (048)-720-91-48; e-mail: mariahilchyk@mail.ru

Главные области научных исследований: использование методов теории принятия решений в перспективных сетях доступа.

Using Decision Theory Methods to Optimize the Access Networks Synthesis Process

Galina Gaivoronskaya, Maria Hilchyk

Abstract*: Using the methods of the theory of decision-making to optimize the synthesis of access networks. Analyzed the synthesis of access networks and the use of decision theory for optimization. Choose the optimum method of decision theory, which may be used to facilitate the synthesis of access networks.*

Keywords*: access network, synthesis access networks, decision theory, decision theory methods.*

ПРИМЕНЕНИЕ СКАЛЯРНЫХ КРИТЕРИЕВ ВЫБОРА ДЛЯ ОПРЕДЕЛЕНИЯ СТРУКТУРЫ МНОГОЗВЕННОЙ КОММУТАЦИОННОЙ СХЕМЫ ДЛЯ КОММУТАЦИИ ОПТИЧЕСКИХ СИГНАЛОВ

Гайворонская Г.С., Рыбалов Б.А.

***Аннотация**: Предложен подход к выбору оптимальной коммутационной схемы, основанный на скалярных критериях выбора, и решена задача определения структуры многозвенной системы коммутации, характеризующаяся строгой неблокируемостью, не требующей ремаршрутизации при использовании любой процедуры установления соединения. Полученные результаты могут быть применены при проектировании пространственных систем коммутации оптических сигналов, позволяющих повысить эффективность функционирования оптических телекоммуникационных сетей за счет повышения быстродействия процессов коммутации в этих сетях.*

***Ключевые слова**: коммутация оптических сигналов, система коммутации оптических сигналов, коммутационная схема, скалярные критерии выбора.*

***Ключевые слова классификации ACM**: B.6 LOGIC DESIGN – B.6.3 Design Aids, B.4 INPUT/OUTPUT AND DATA COMMUNICATIONS - B.4.3 Interconnections (subsystems).*

***Conference topic**: Informational Modelling.*

Введение

Создание сетей следующего поколения – *Next Generation Network (NGN*) – является наиболее актуальной задачей на современном этапе развития телекоммуникаций. Концепция *NGN* предусматривает предоставление неограниченного количества инфокоммуникационных услуг, что обуславливает рост требований к пропускной способности этой сети. Одним из возможных способов, позволяющих решить задачу существенного повышения пропускной способности телекоммуникационных сетей (ТС), является создание полностью оптических сетей – *All-Optical Networks* (*AON*), позволяющих повысить пропускную способность сети до нескольких Пбит/с за счет применения полностью оптических технологий обработки информационного сигнала.

Основной задачей, требующей решения при создании полностью оптических сетей, является задача реализации коммутации оптических сигналов. Анализ состояния вопроса в области

создания оптических сетей [Каток В. Б., 2006; Иванов А.Б., 1999; Каток В.Б., 1999; Шарварко В.Г., 2006; Убайдуллаев Р.Р., 2001] показал, что на данный момент принципы функционирования волоконно-оптических систем передачи, изучены достаточно хорошо. В то же время вопросы реализации систем коммутации оптических сигналов (СКОС) рассмотрены поверхностно и требуют проведения дальнейших исследований. В настоящее время существуют лишь общие концептуальные подходы к построению СКОС, требующие развития и тщательного анализа.

Существующие методы коммутации оптических сигналов [Гайворонская Г.С. (1), 2011] предусматривают необходимость предварительного преобразования оптического излучения, несущего информацию, в электрическую форму (*O/E*), коммутацию электрического сигнала и обратное электрооптическое преобразование (*E/O*) с последующим усилением мощности оптического излучения. На рисунке 1 представлена обобщенная структурная схема системы коммутации *O/E/O*.

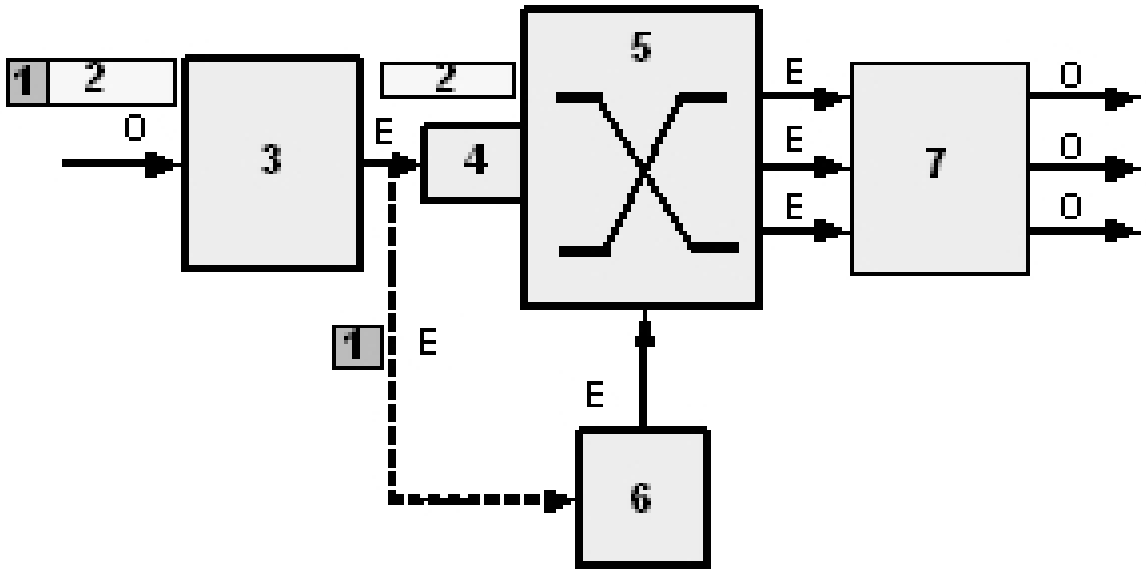


Рисунок 1 – Структурная схема системы коммутации *O/E/O*:

1 – служебная информация, 2 – полезная информация,

3 – блок оптоэлектрического преобразования,

4 – электронная буферная память, 5 – электронное коммутационное поле,

6 – электронный блок управления коммутацией, 7 – блок электрооптического преобразования

Такой подход к коммутации оптических сигналов накладывает ограничения на пропускную способность системы коммутации (СК) и ее емкость. Осуществление двукратного преобразования информационного сигнала, во-первых, существенно ограничивает пропускную способность СК (до 2,5 Гб/с), а, во-вторых, характеризуется чрезмерным энергопотреблением, что повышает стоимость эксплуатации системы коммутации. Более того, повышенное энергопотребление и наличие перекрестных помех приводит к ограничению емкости подобных СК, которая не превышает 32x32. [Гайворонская Г.С. (2), 2011; Гайворонская Г.С. (3), 2011].

Следовательно, электронно-оптические СК становятся узким местом ТС и являются сдерживающим фактором при наращивании её пропускной способности. Для устранения этого недостатка необходима разработка модели системы коммутации оптических сигналов, не только коммутирующей сигналы в оптической форме, но и обеспечивающей управление процессом коммутации с помощью оптического излучения. Под оптическим управлением процессом коммутации понимается управление переносом информации между оптическими каналами, реализуемое исключительно с использованием оптических технологий и позволяющее совершить переход к пентабитным скоростям передачи информации в ТС.

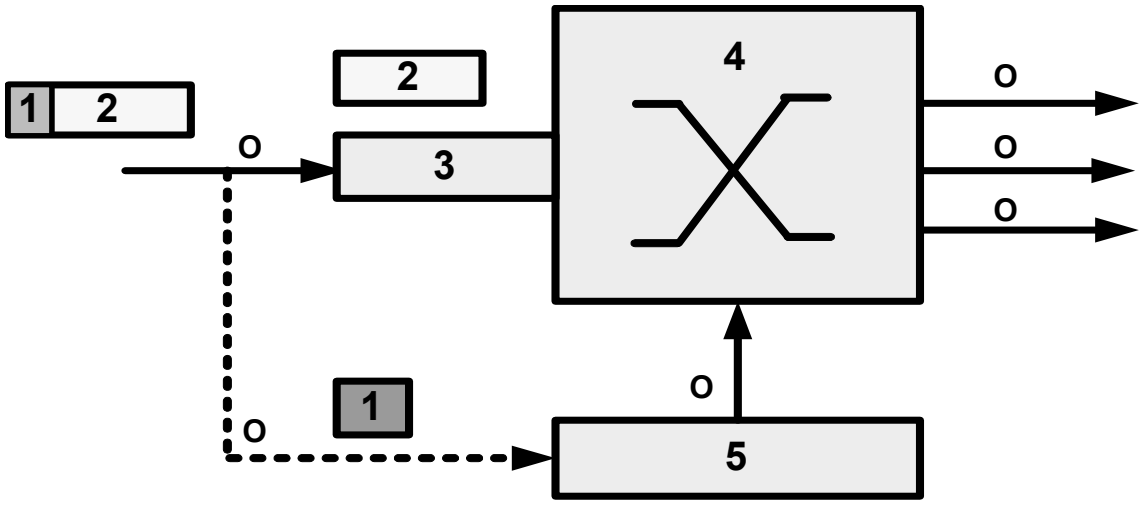


Рисунок 2 – Архитектура полностью оптической системы коммутации:

1 – служебная информация,

2 – полезная информация,

3 – оптический буфер,

4 – оптическое коммутационное поле,

5 – блок оптического управления коммутацией

На рисунке 2 приведена архитектура полностью оптической системы коммутации.

В этой системе информационный оптический сигнал, переносящий некоторый блок информации (БИ), одновременно запоминается в оптическом буфере (ОБф) и поступает на вход блока оптического управления (БОУ), который выполняет анализ БИ, выделяет адресную информацию и после ее обработки генерирует оптический сигнал управления точкой коммутации оптического коммутационного поля (ОКП). Затем оптический сигнал извлекается из ОБф и, следуя по коммутационному пути, поступает на выход СК. После усиления мощности сигнал передается по оптическому волноводу к следующему узлу коммутации.

Несмотря на преимущества полнооптического подхода к построению систем коммутации, его применение вызывает ряд сложностей. В первую очередь, это касается реализации БОУ, использующего оптические процессоры, применяемые в военной промышленности и ядерной энергетике, стоимость которых в десятки раз превышает стоимость их электронных аналогов [Жувикин Г., 2003].

Еще одним препятствием для построения СКОС является сложность создания оптического буфера с произвольным доступом (*Optical RAM*). Существующие на сегодняшний день линии оптической задержки – *Fiber Delay Line* (*FDL*) – способны накапливать оптический сигнал лишь ограниченный промежуток времени, что обуславливается чрезвычайно быстрым затуханием оптического излучения в миниатюрных петлях задержки.. В связи с этим актуальной задачей является создание гибридной модели системы коммутации оптических сигналов на переходный период, которая, реализуя концепцию «коммутации на лету» (“*cut through”*) [Ершова Э.Б., 2009] без буферизации, позволит повысить эффективность функционирования оптических сетей. Такая модель СКОС должна быть лишена электрооптического преобразования информационного сигнала, а управление коммутацией может быть реализовано электронным способом. Это позволит решить проблему большого энергопотребления и сложности построения СК большой емкости путем применения технологии микроэлектромеханических систем (*MEMS)* [Гайворонская Г.С., 2010], используя для управления ОКП доступные по цене высокопроизводительные электронные процессоры. При этом одной из актуальных задач при проектировании СКОС емкостью более 1024 портов является определение структуры коммутационной схемы (КС). Эта статья посвящена решению задачи выбора КС для построения квадратных многозвенных СКОС.

Основная часть

При построении пространственных систем коммутации оптических сигналов функциональную пригодность и эффективность СКОС оценивают с помощью следующих показателей [Слепов Н.Н., 2000; Слепов Н.Н., 1999]:

– характеристики блокировки;

– требуемое количество базовых элементов (БЭ);

– однородность коммутации;

– пересекаемость связующих волноводов.

Под характеристиками блокировки СК понимают возможность установления соединения между любой парой свободных портов на входе и выходе СК ($X_{ВХ}, Y_{ВЫХ}$). В зависимости от этой характеристики выделяют неблокирующие и блокирующие коммутационные схемы [Иванова О.Н., 1978]. Неблокируемость КС является ключевым требованием к системам пространственной коммутации оптических сигналов. При этом неблокирующие коммутационные схемы, в свою очередь, делятся на:

– неблокирующие в строгом смысле;

– неблокирующие в широком смысле;

– неблокирующие перестраиваемые.

Неблокирующие в строгом смысле КС – это такой тип схем, который не требует ремаршрутизации какого-либо соединения при использовании любой процедуры установления соединения.

Неблокирующие в широком смысле КС характеризуются отсутствием необходимости ремаршрутизации уже существующих соединений только при условии использования определенной процедуры установления связи.

Именно первые два типа неблокирующих КС на сегодняшний день могут быть эффективно использованы для построения СКОС. Это вызвано тем, что неблокирующие перестраиваемые КС требуют ремаршрутизации существующих соединений, что является проблематичным по причине необходимости буферизации оптического сигнала.

Стоимость системы коммутации определяется количеством используемых базовых элементов. Под базовым элементом (БЭ) многозвенной КС будем понимать коммутационный прибор с

параметрами 2x2 либо 1x2. Следовательно, на стадии проектирования КС необходимо стремиться к минимизации количества используемых БЭ, что позволит уменьшить стоимость разрабатываемого устройства. Пересекаемость связующих волноводов необходимо минимизировать либо вовсе исключить, поскольку она обуславливает возникновение потерь мощности оптического излучения и переходные потери в результате взаимодействия световых потоков.

Под однородностью СК понимается равенство минимального и максимального количества базовых элементов, которые пройдет оптический сигнал, прежде чем достигнет выхода системы коммутации. Учитывая тот факт, что каждый базовый оптический элемент вносит затухание сигнала, при проектировании СКОС необходимо стремиться к тому, чтобы, во-первых, количество БЭ, через которые проходит оптический сигнал, было минимальным, а, во-вторых, минимальные и максимальные потери сигнала должны быть тождественны. Среди существующих схем комбинирования коммутационных приборов, удовлетворяющих условию неблокируемости, можно выделить следующие: матричную, схему Бенеша, схему Шпанке и схему Шпанке-Бенеша [Иванова О.Н.,1978]. Основные характеристики неблокирующих КС приведены в таблице 1.

Таблица 1 – Характеристики неблокирующих коммутационных схем $N \times N$

Схемы / Показатели	**Матричная**	**Бенеша**	**Шпанке-Бенеша**	**Шпанке**
Неблокируемость	В широком смысле	С перестройкой	С перестройкой	В строгом смысле
Количество БКЭ	N^2	$\frac{N(2\log_2 N - 1)}{2}$	$\frac{N(N-1)}{2}$	$2N(N-1)$
Максимум потерь	$2N-1$	$2\log_2 N - 1$	N	$2\log_2 N$

Минимум потерь	*1*	$2\log_2 N - 1$	$\frac{N}{2}$	$2\log_2 N$
Однородность коммутации	Нет	Да	Нет	Да
Пересекаемость	Нет	Да	Нет	Да

Пусть задано множество КС Ω, состоящее из отдельных вариантов ω_i так, что каждый отдельный вариант $\omega_i \in \Omega$ рассматривается как точка в пространстве показателей приемлемости, а множество возможных вариантов Ω определяется областью их существования: $\Omega = \{\omega_i\}, i = \overline{1,N}$.

Альтернативные варианты в однородном множестве Ω представляются минимальными конечными описаниями, представляющими собой набор характеристик коммутационной схемы $P = \{p_j\}, j = \overline{1,J}$, в достаточной степени полно описывающий каждый из вариантов однородного множества Ω. Множество характеристик $\{p_j\}$ для коммутационных схем $\Omega = \{\omega_i\}$ состоит из подмножества показателей приемлемости $\{k_l\}$ и подмножества условий $\{Y_z\}$. Множество альтернатив, удовлетворяющих совокупности условий $\{Y_z\}$, т. е. требованиям по допустимости C_d, является допустимым множеством Ω_d.

Учитывая, что ключевым условием реализации системы коммутации оптических сигналов является требование неблокируемости КС, множество Ω_d составляют следующие КС: матричная W_1, Бенеша W_2, Шпанке-Бенеша W_3 и Шпанке W_4.

Задача выбора сводится к тому, чтобы среди множества допустимых коммутационных схем Ω_d выбрать вариант, обладающий лучшими значениями k_l с точки зрения принятой критериальной постановки.

Прежде чем сформулировать критериальную постановку $K = \{k_1,...,k_M\}$ необходимо отобразить характеристики КС на числовую шкалу. Для отображения качественных характеристик (тип

неблокируемости, однородность коммутации) использована порядковая шкала, а для количественных характеристик (количество БЭ, максимум и минимум потерь) – абсолютная шкала.

Пусть k_1 – это тип неблокируемости КС, k_2 – количество БКЭ, k_3 – максимум потерь, k_4 – минимум потерь, k_5 – однородность коммутации, k_6 – пересекаемость волноводов. Тогда критериальная постановка K будет иметь следующий вид:

$$K = \{k_1 \to \max, k_2 \to \min, k_3 \to \min, k_4 \to \min, k_5 \to \max, k_6 \to \max\} \quad (1)$$

Учитывая тот факт, что характеристики КС имеют различные физические размерности, необходимо выполнить нормирование исходных значений. При этом влияние каждого нормированного показателя на результирующую функцию будет сопоставимо, если диапазоны возможных изменений каждого из них окажутся общими. Для этого использовано следующее выражение (2):

$$k_l = \frac{k_l - k_l^*}{k_l^{**} - k_l^*}, \quad (2$$

где $k_l^* = \min k_l \in \{k_l\}$,

$k_l^{**} = \max k_l \in \{k_l\}$.

С помощью этого выражения для каждой характеристики k_l получены характеристики неблокируемых КС после нормирования.

Важным этапом при решении задачи выбора является определение используемого критерия выбора. Векторные критерии (критерии по Парето и Слейтеру) позволяют отбросить лишь заведомо худшие варианты и выявить нехудшие – эффективные по Парето и Слейтеру. Главной чертой векторных критериев является их объективность, так как показатели качества в таких критериях являются независимыми [Гайворонська Г.С. (4), 2011]. Учитывая, что сформулированная постановка задачи выбора предусматривает наличие зависимых показателей приемлемости (в частности, однородность коммутации зависит от числа минимальных и максимальных потерь), то применение векторных критериев не представляется

целесообразным. Более того, одним из главных требований к применению критериев по Парето и Слейтеру является свойство сравнимости вариантов. Варианты сравнимы, если значения всех показателей качества одного варианта меньше (или больше) значений показателей качества другого варианта. Поскольку предварительный анализ исходного множества допустимых вариантов Ω_d показывает присутствие малого числа сравнимых вариант, то напрашивается вывод о неэффективности использования векторных критериев для решения поставленной задачи. Особенностью скалярных критериев является возможность получения единственного варианта решения, однако вместе с тем скалярные критерии содержат большую долю субъективности лица принимающего решения (ЛПР).

В случае решения задачи выбора КС функция выбора задается как некоторый функционал – комплексный показатель приемлемости, отражающий суммарный целевой эффект. Следовательно, для решения поставленной задачи целесообразным является применение интегрального критерия сравнения альтернатив.

Для назначения экспертных оценок весовых коэффициентов использован метод ранжирования, поскольку он предусматривает возможность достаточно точной оценки важности каждого из показателей выбираемого варианта. Суть метода ранжирования заключается в оценке показателей приемлемости по шкале относительной важности (например, в диапазоне от 1 до 10). Согласно этому методу, для M показателей весовые коэффициенты определяются по следующей формуле:

$$a_l = \frac{\lambda_l}{\sum_{l=1}^{M} \lambda_l}, \tag{3}$$

где λ_i – оценка значимости фактора l.

При этом для M весовых коэффициентов a_l должно выполняться выражение:

$$\sum_{i=1}^{M} a_i = 1, \quad a_i \geq 0, \quad \overline{i = 1, M} \tag{4}$$

Оценка показателей приемлемости по десятибалльной шкале относительной важности приведена в таблице 2.

Таблица 2 – Оценка показателей приемлемости по шкале относительной важности

Показатели качества	**Относительная оценка**
Тип неблокируемости, a_1	10
Количество БЭ, a_2	3,51
Минимум потерь, a_3	1
Максимум потерь, a_4	1,49
Однородность коммутации, a_5	2
Пересекаемость, a_6	1,8

После расчета весовых коэффициентов для каждого показателя приемлемости с помощью применения интегрального критерия выбора аддитивного типа решена задача выбора КС.

$$W = \sum_{i=1}^{M} a_i k_i, \ \overline{I = 1, M} \tag{5}$$

На рисунке 3 приведены результаты расчета интегрального критерия выбора для каждой КС W_i.

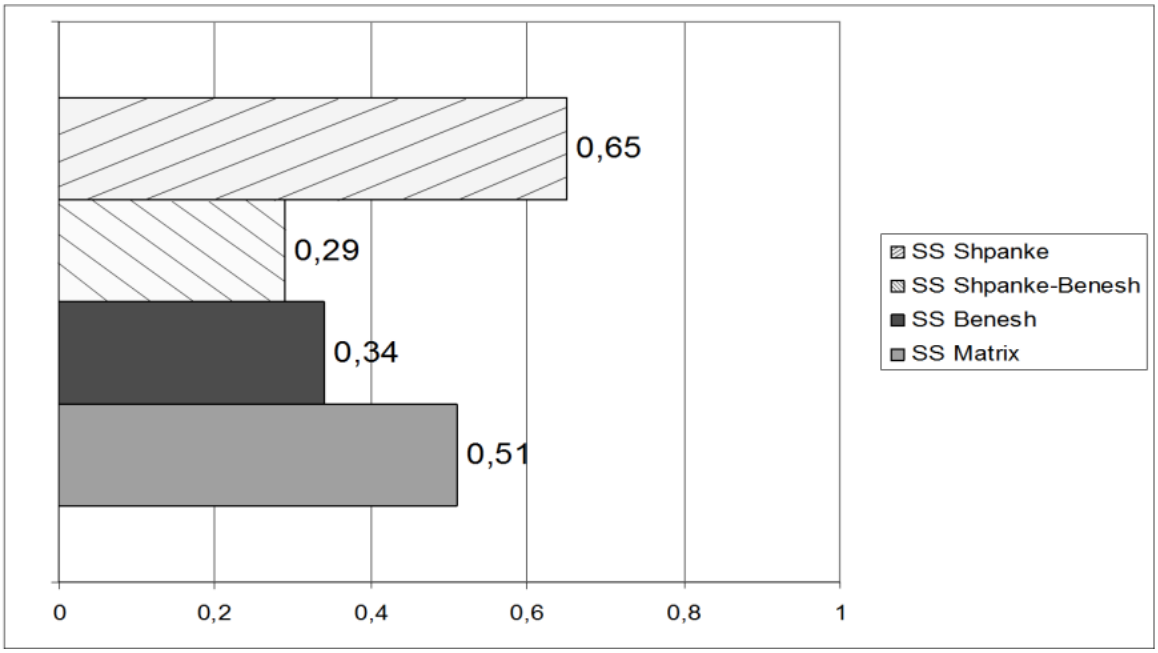


Рисунок 3 – Показатели интегрального критерия выбора для неблокирующих КС

На основании решения задачи выбора, наиболее приемлемым вариантом для построения СКОС является альтернатива W_4 – коммутационная схема Шпанке, удовлетворяющая условию строгой неблокируемости.

Заключение

Предложенный в статье подход к выбору коммутационной схемы для построения системы коммутации оптических сигналов позволяет однозначно утверждать, что решение таких задач характеризуется большой долей субъективизма ЛПР, и зависит от его подготовленности и профессионализма. Решение задачи с применением интегрального критерия выбора позволило выбрать структуру коммутационной схемы Шпанке для построения квадратных систем коммутации оптических сигналов большой емкости. Несомненным достоинством коммутационной схемы Шпанке является характеристика строгой неблокируемости, однако для ее реализации необходимо большое количество коммутационных приборов 1x2. Другие коммутационные схемы, рассмотренные при решении задачи выбора, могут быть использованы при построении многокаскадных СКОС лишь тогда, когда будет решена проблема оптической реализации перестройки существующих соединений.

Благодарности

Настоящая работа выполнена при поддержке интернационального проекта ITHEA XXI Института информационных теорий и их приложений FOI ITHEA и Ассоциации ADUIS Украина (Ассоциация разработчиков и пользователей интеллектуальных систем).

The paper is published with financial support by the project ITHEA XXI of the Institute of Information Theories and Applications FOI ITHEA (*www.ithea.org*) and the Association of Developers and Users of Intelligent Systems ADUIS Ukraine (*www.aduis.com.ua*).

Литература

[Каток В. Б., 2006] Аналіз характеристик передачі одномодових волокон для мереж зв'язку / В.Б. Каток, О.Б. Омецинская, М.В. Шаповалов // Тези доповідей МНПК «Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій».– Запоріжжя. – 2006. – С.18-19.

[Иванов А.Б.,1999] Волоконная оптика: компоненты, системы передачи, измерения. – М.: Сайрус системс, 1999. – 664 с.

[Каток В.Б.,1999] Волоконно-оптичні системи зв'язку. – Київ.: *Lucent Technologies*, 1999. – 483 с.

[Шарварко В.Г.,2006] Волоконно-оптические линии связи: Учебное пособие. – Таганрог: Изд-во ТРТУ, 2006. – 170 с.

[Убайдуллаев Р.Р.,2001] Волоконно-оптические сети. – М.: Эко-Трендз, 2001. – 267 с.

[Гайворонская Г.С. (1), 2011] Особенности применения оптических коммутаторов в современных информационных сетях / Г.С. Гайворонская, А.В. Рябцов // *Applicable Information Models*. – Sofia: *ITHEA, 2011*. – № 22. – P. 169-181.

[Гайворонская Г.С. (2), 2011] Проблема обеспечения полностью оптической коммутации в конвергентных сетях / Г.С. Гайворонская // Збірник тез V МНТК «Проблеми телекомунікацій». – Київ. – НТУУ «КПІ». – 2011. – С.39

[Гайворонская Г.С. (3), 2011] Тенденции развития оптических коммутаторов / Г.С. Гайворонская, А.В. Рябцов// Збірник тез V МНТК «Проблеми телекомунікацій».– Київ.– НТУУ «КПІ».– 2011.– С.99

[Жувикин Г., 2003] Светит ли нам оптический компьютер? / Г. Жувикин // М.: Компьютерра. – 2003. – №2. – Режим доступа: *http://offline.compu-terra.ru/2000/332/2877/*

[Ершова Э.Б.,2009] К вопросу построения оптических сетей / Э.Б. Ершова, Э.М. Вакс // Спецвыпуск «Технологии информационного общества». – Москва. – 2009. – С. 14 – 18.

[Гайворонская Г.С., 2010] Метод повышения быстродействия оптических коммутаторов в информационных сетях / Г.С. Гайворонская, А.В. Рябцов // Холодильна техніка і технологія. – Одеса: ОДАХ, 2010. – №4 (126). – С. 70-72.

[Слепов Н.Н., 2000] Современные технологии цифровых оптоволоконных сетей связи / Н.Н. Слепов // М.: Радио и связь, 2000. – 468 с., ил.

[Слепов Н.Н., 1999] Оптические кросс-коммутаторы. Принципы реализации и архитектура / Н.Н. Слепов // М.: Связь и телекоммуникации. – 1999. – №6. – Режим доступу: *http://www.electronics.ru/issue/1999/6/3*

[Иванова О.Н.,1978] Автоматические системы коммутации / О.Н. Иванова, М.Ф. Копп // М.: Связь. – 1978.– 624 с.

[Гайворонська Г.С. (4), 2011] Оптимальний синтез інформаційних мереж: навчальний посібник для магістрів / Г.С. Гайворонська // Одеса: ОДАХ. – 2011. – 94 с.

Информация об авторах

Гайворонская Галина Сергеевна *– Институт холода, криотехнологий и экоэнергетики им. В.С. Мартыновского, факультет информационных технологий и кибербезопасности ОНАПТ, д.т.н., профессор, зав. кафедрой информационно-коммуникационных технологий, советник ректора по инфокоммуникациям; Украина, Одесса, 65026, ул. Дворянская, 1/3; тел. (048)-720-91-48; e-mail: gsgayvoronska@gmail.com*

Области научных исследований: оптимизация переходных периодов при эволюции телекоммуникационных сетей. Потоки вызовов, нагрузка и межузловое тяготение в сетях. Проблемы создания сетей доступа. Проблема построения полностью оптических сетей и систем коммутации.

Рыбалов Борис Александрович *– Институт холода, криотехнологий и экоэнергетики им. В.С. Мартыновского, факультет информационных технологий и кибербезопасности ОНАПТ, старший преподаватель кафедры информационно-коммуникационных технологий; Украина, Одесса, 65026, ул. Дворянская, 1/3; тел.(067) 93 29 677; e-mail: borisr@ukr.net*

Основные направления научных исследований: задачи создания полностью оптических сетей, коммутация оптических сигналов.

SCALAR CHOICE CRITERIA'S USAGE FOR DETERMINATION OF THE OPTIMUM SWITCHING CIRCUIT FOR OPTICAL SIGNALS' SWITCHING SYSTEM

Galina Gayvoronska, Borys Rybalov

Abstract: *An approach to the optimum switching scheme's choice is proposed. It is based on the scalar choice criteria. Problem of the multistage switching system's structure's determination is solved. Such system is characterized by strict non-blocking and doesn't require rerouting at the usage of any connection establishment procedure. Obtained results can be applied at the design of spatial optical signals' switching systems, allowing improvement of the optical telecommunications networks' functioning by increasing the performance of switching operations in these networks.*

Keywords: *optical signals' switching, optical signals' switching system, switching scheme, scalar choice criteria.*

АНАЛИЗ ИСПОЛЬЗОВАНИЯ ПРОПУСКНОЙ СПОСОБНОСТИ КАК ПОКАЗАТЕЛЯ КАЧЕСТВА ОБСЛУЖИВАНИЯ ПОЛЬЗОВАТЕЛЯ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Евгений Кушниренко, Галина Гайворонская

***Аннотация**: Проанализировано влияние пропускной способности на удовлетворение требований пользователей различных услуг с разнящимся типом передаваемой информации с целью включения показателя пропускной способности в ряд параметров качества обслуживания пользователя в телекоммуникационной сети.*

***Ключевые слова:** телекоммуникационная сеть, качество обслуживания, пропускная способность, корреляция, показатель качества.*

***ACM Classification Keywords**: C.4 Performance of systems, C.2. Computer-communication networks, H. Information Systems - H.1 Models and Principles*

Введение

Концепции качества обслуживания уделяется большое количество внимания в сфере информационных сетей. По мнению производителей сетевого оборудования, качество обслуживания отвечает возможности сети предоставлять гарантированные значения сетевых параметров при предоставлении различных услуг и наличия высокой нагрузки в базовых сетях, включая те, которые построены на технологии ретрансляции кадров, асинхронного режима передачи, *Ethernet,* а также сетях, которые используют маршрутизацию по протоколу *IP*.

Согласно определению, которое дано международным союзом электросвязи (МСЭ) в рекомендации *E.800*, качество обслуживания – совокупность характеристик инфокоммуникационных услуг, которые определяют уровень удовлетворения потребностей пользователя инфокоммуникационных услуг (ИКП). Также указано, что качество обслуживания сочетает эффективность сетевых и несетевых параметров. К параметрам сети, например, можно отнести частоту ошибок, пропускную способность, задержку и т. д., к несетевым параметрам – время простоя, время восстановления, диапазон тарифов и время решения проблем

технического характера. Список критериев качества обслуживания для практической реализации зависит от услуг и их актуальности для разных типов пользователей [Cisco, 2009]. Определение качества обслуживания со стороны производителей сетевого оборудования можно дать следующим образом: качество обслуживания – это набор технологий, которые позволяют программным приложением производить запросы и получать прогнозированные уровни обслуживания, обеспечивая определенные параметры пропускной способности, задержки и ее вариации [ITU, 2008].

Проблемой обеспечения качества обслуживания, методами ее оценки, и определением параметров качества обслуживания занимается исследовательская комиссия (ИК, англ.: *Study Group*, SG) МСЭ №12, название которой „Показатели работы, качество обслуживания и пользовательская оценка качества услуг". Основные серии рекомендаций, которые были разработаны данной комиссией и вступили в силу в качестве международных рекомендаций, включают документы серий *E* (Общая эксплуатация сети, телефонная служба и человеческий факторы), *G* (Системы и среда передачи, цифровые системы и сети), *P* (Качество телефонной передачи, телефонное оборудование, сети местных линий), *И* (Цифровые сети интегрального обслуживания), *Y* (Глобальная информационная инфраструктура, проблемы протокола интернет (*ИР*) и сетей следующего поколения) [ITU]. Другими словами, можно констатировать, что на примере проблем, которые рассматриваются МСЭ, качество обслуживания, параметры и методы обеспечения и оценки качества являются обязательной составляющей полноценной базы стандартов и рекомендаций для построения телекоммуникационных сетей.

Рекомендация *E.800* определяет качество обслуживания, как, совокупность характеристик услуг электросвязи, которые устанавливают уровень удовлетворения потребностей пользователя услуг. Это определение не раскрывает методов объективного оценивания, однако оно дает возможность на основе анализа рабочих характеристик применений выбрать объективные показатели качества обслуживания.

Вместе с рекомендациями *Y.1540, Y.1541, Y.1561*, рекомендация *G.1010* определяет некоторые ключевые параметры качества обслуживания, однако выделяет те, которые самым значительным образом влияют на пользователя. К таким параметрам, относятся: задержка, вариация задержки и потеря информации. При этом рекомендация допускает, что с точки зрения конечного пользователя, количество параметров, которое влияет на качество предоставленных ИКП значительно больше. В частности, указано: *„С точки зрения пользователя, понятие задержки также включает в себя эффекты других сетевых параметров, таких как пропускная способность…"* [ITU, 2001].

Постановка задачи корреляционного анализа пропускной способности

В сложившийся ситуации с помощью методов многомерного статистического анализа решено проанализировать, как пропускная способность (которая является теоретическим максимумом значений таких параметров, как скорость передачи, или скорость доступа к глобальной сети) влияет на удовлетворение потребностей пользователей телекоммуникационных сетей, а также, – как пропускная способность влияет на востребованность различных типов услуг. Многомерным статистическим анализом является раздел математической статистики, который анализирует методы сбора и применения многомерных статистических данных, их систематизацию и обработку с целью выявления характера и структуры взаимосвязи между компонентами исследуемого многомерного признака, получения практических выводов. Результатом такого анализа будет вывод о корреляции разных типов показателей между собой [Wikipedia].

Формирование входных данных корреляционного анализа пропускной способности

В работе в качестве сферы исследования выбраны услуги, которые предоставляются международной глобальной сетью Интернет. Такой выбор можно объяснить чрезвычайной популярностью, наибольшей распространенностью, а также наибольшим списком услуг и приложений, которые предоставляются через Интернет на сегодняшний день. В качестве предмета исследования выбраны данные, касательно количества пользователей таких порталов, как *YouTube* (согласно данным [Audience] – самого популярного портала потокового видео в Украине) и *Wikipedia* (один из самых популярных в мире энциклопедичных ресурсов) и показатели средней скорости доступа к Интернет в Украине, начиная с первого квартала 2012 г., заканчивая вторым кварталом 2014 г.

Данные касательно средней скорости доступа к Интернет в Украине взяты из международного статистического ресурса „*Statista"* [Statista], объем ежегодной выборки ресурса составляет 1-3 млн. пользователей сети Интернет из Украины. Данные касательно популярности услуг сети Интернет среди украинской аудитории взяты из ресурса „Интернет аудитория Украины" [Audience], объем выборки составил 16 млн. пользователей Интернет, которые, ориентировочно, составляют полную численность пользователей сетью Интернет в Украине (Таблица 1).

Таблица 1. Входные данные анализа многомерной выборки

Квартал и год	Популярность услуги		Средняя скорость доступа к сети Интернет в Украине, Кбит/с
	YouTube, чел.	*Wikipedia,* чел.	
I.2012	6423485	4633574	4378
II.2012	6374042	5139617	4540
III.2012	6949117	5558722	4586
IV.2012	7326927	5792115	4792
I.2013	7115078	5440411	5717
II.2013	6623731	5349923	6767
III.2013	7483400	5456211	7978
IV.2013	7823921	5812469	7325
I.2014	8536108	5837990	8130

Решение задачи корреляционного анализа пропускной способности

Корреляция между скоростью доступа к сети Интернет и количеством пользователей соответствующих услуг определяется, по следующей методике.

Сначала определяется, коррелируют ли между собой средняя скорость доступа к сети Интернет в Украине и количество украинских пользователей портала потокового видео *YouTube*. После чего, определяется наличие корреляции между средней скоростью доступа к сети Интернет в Украине и количеством украинских пользователей энциклопедического ресурса *Wikipedia*. Наличие корреляции устанавливается при помощи коэффициента корреляции, Спирмена, Фехнера и Кендалла для каждого из двух случаев. В Таблице 1, приведены входные данные, которые используются для расчета коэффициентов корреляции [Studopedia], то есть математической мери зависимости двух случайных величин

$$r = \sum_{i=1}^{n} \frac{(x_i - \overline{x})(y_i - \overline{y})}{n * \delta_x * \delta_y} \quad (1)$$

где $\overline{x}$, $\overline{y}$ – математическое ожидание, δ – среднеквадратическое отклонение, n – количество наблюдений.

Результат расчета этого коэффициента приведено в Таблицах 2 и 3 соответственно для каждой пары выборок.

Коэффициент Фехнера – это оценка степени согласованности направлений отклонений индивидуальных значений факторных и результативных признаков от средних значений факторных и результативных признаков [Studopedia]. Для определения коэффициента Фехнера воспользуемся формулой:

$$K_{ф} = \frac{C - H}{C + H} \quad (2)$$

где C, H – количество случаев для которых по паре признаков X, Y наблюдается соответственно совпадение (C) или расхождение (H) знаков отклонения для средних уровней.

Результат расчета этого коэффициента приведен в Таблицах 2 и 3 соответственно для каждой пары выборок.

Коэффициент ранговой корреляции Спирмена является непараметрической мерой статистической зависимости между двумя переменными. Он оценивает насколько точно можно описать отношения между двумя переменными при помощи монотонной функции [Studopedia]. Для определения коэффициента Спирмена использовано формулу:

$$K_c = 1 - \frac{6\sum d^2}{n(n^2 - 1)} \quad (3)$$

где $\sum d^2$ – сумма квадратов разных рангов, n – число парных наблюдений.

Результат расчета этого коэффициента аналогично приведен в Таблицах 2 и 3 соответственно для каждой пары выборок.

Коэффициент корреляции Кендалла – мера линейной связи между случайными величинами. Корреляция Кендалла является ранговой, то есть для оценки силы связи используются не численные значения, а соответствующие им ранги. Коэффициент инвариантный по отношению к любому монотонному преобразованию шкалы измерения [Studopedia]

$$K_k = \frac{2S}{n(n-1)} \tag{4}$$

где n – количество наблюдений, $S = Q - P$.

При расчете S учитывается частота нарушения порядков следования по признаку y, при условии, что по признаку x ранги следуют один за другим строго упорядочено.

Следовательно, проведя все необходимые вычисления, мы получили результаты, предоставленные в Таблицах 2 и 3.

Таблица 2. Результаты вычисления коэффициентов между средней скоростью доступа к сети Интернет в Украине и количеством украинских пользователей *YouTube*

Коэффициент корреляции	Коэффициент Фехнера	Коэффициент Спирмена	Коэффициент Кендалла
0,848	0,8	0,988	-0,956

Таблица 3. Результаты вычисления коэффициентов между средней скоростью доступа к сети Интернет в Украине и количеством украинских пользователей *Wikipedia*

Коэффициент корреляции	Коэффициент Фехнера	Коэффициент Спирмена	Коэффициент Кендалла
0,574	0,2	0,988	-0,956

Согласно полученным данным, можно сделать вывод, что в первом случае показатели корреляции очень высоки (больше 0,7 по модулю) и имеет место быть зависимость одного

показателя от другого, а именно количество украинских пользователей услугой потокового видео *YouTube* действительно зависит от средней скорости доступа к сети Интернет в Украине. Во втором же случае, корреляция является менее выраженной из-за малых значений показателей коэффициента корреляции и коэффициента Фехнера (меньше 0,7 по модулю) и поэтому мы не можем однозначно утверждать про то, что количество украинских пользователей энциклопедического сервиса *Wikipedia* однозначно зависит от средней скорости доступа к сети Интернет в Украине.

Заключение

Результаты анализа свидетельствуют о том, что с увеличением показателя пропускной способности сети, пользователи стремятся к получению более требовательных к производительности сети услугам, которые при меньших значениях пропускной способности не могли удовлетворить потребности всех пользователей сети. Следовательно, для дальнейшего повышения общего качества обслуживания в телекоммуникационных сетях, а также для дальнейшего побуждения всё большего числа клиентов к пользованию требовательными услугами, следует рассматривать параметр пропускной способности как один из самых основных, формирующих как итоговую оценку качества обслуживания, так и аудиторию пользователей телекоммуникационной сети.

Литература

[Audience] Интернет аудитория Украины, http://www.audience.com.ua

[Cisco, 2009] Cisco QoS Frequently Asked Questions, http://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/22833-qos-faq.html

[ITU, 2001] ITU G.1010 “End-user multimedia QoS categories”// ITU Recommendation, 2001

[ITU, 2008] ITU E.800 „Quality of telecommunication services: concepts, models, objectives and dependability planning – Terms and definitions related to the quality of telecommunication services”// ITU Recommendation, 2008.

[ITU] Международный союз электросвязи, http://www.itu.int/ru/ITU-T/groups/Pages/default.aspx

[Statista] Statista, http://www.statista.com/

[Studopedia] Студопедия, Методы стохастического анализа, http://studopedia.net/10_1152_metodi-stohastichnogo-korelyatsiynogo-faktornogo-analizu.html

[Wikipedia] Свободная энциклопедия Википедия, http://uk.wikipedia.org/wiki/Кореляция

Информация об авторах

Евгений Кушниренко *– факультет информационных технологий и кибербезопасности ОНАПТ, магистр кафедры информационно-коммуникационных технологий;; Украина,Одесса, 65026, ул. Дворянская, 1/3; тел. (093)-159-48-74; e-mail: betreyer@yandex.ru.*

Области научных исследований: качество обслуживания в телекоммуникационных сетях: модели, механизмы, параметры

Галина Гайворонская *– факультет информационных технологий и кибербезопасности ОНАПТ, д.т.н., профессор, зав. кафедрой информационно-коммуникационных технологий, советник ректора по инфокоммуникациям; Украина,Одесса, 65026, ул. Дворянская, 1/3; тел. (048)-720-91-48; e-mail: gsgayvoronska@gmail.com*

Области научных исследований: оптимизация переходных периодов при эволюции телекоммуникационных сетей. Потоки вызовов, нагрузка и межузловое тяготение в сетях. Проблемы создания сетей доступа. Проблема построения полностью оптических сетей и систем коммутации.

Analysis of Usage of Throughput as a Parameter of Quality of Service of User of Telecommunication Network

Yevhen Kushnirenko, Galyna Gayvoronska

Abstract: *Analyzed impact of throughput on demands satisfaction of users of different services with different types of information transmition with the purpose to include throughput in a number of quality of service parameters of user of telecommunication network.*

Key words*: telecommunication network, quality of service, throughput, correlation, quality index.*

TABLE OF CONTENTS OF IJ IMA VOL.4, NUMBER 1

TABLE OF CONTENTS OF IJ IMA VOL.4, NUMBER 2

TABLE OF CONTENTS OF IJ IMA VOL.4, NUMBER 3

TABLE OF CONTENTS OF IJ IMA VOL.4, NUMBER 4