# Calculation of the Probabilistic Safety Analysis and Reliability by the Fault Trees and Event Trees Methods

M.A. Berberova[1], A.V.Dmitriev[1], A.V.Golubkov[1], A.I.Elizarov[2]
maria.berberova@gmail.com | avdv@list.ru | sgo@mail.ru | eiao8lzrv@mail.ru
[1]International Nuclear Safety Center, Moscow, Russia
[2]Open Joint Stock Company «All-Russian Research Institute for Nuclear Power Plants Operation», Moscow, Russia

*One of the main requirements for ensuring a high level of safety and economic efficiency of nuclear power units at all stages of the life cycle - designing new ones, operating existing power units and decommissioning them - is a probabilistic safety analysis of nuclear power units. The most widely used method for probabilistic safety analysis is the fault tree method.*

*NPP power units are a complex system consisting of a large number of units of equipment, systems and units that are interconnected functionally and affect each other. In addition, to increase the adequacy of the developed probabilistic model of a power unit, it is necessary to take into account equipment failures for general reasons and the human factor. The resulting in-depth probabilistic models of power units can contain tens of thousands of fault trees and, as a result, hundreds or more of thousands of minimum sections and require lengthy calculations to obtain acceptable accuracy of the results. This complicates the application of this method, especially when monitoring risk in real time, when it is necessary to promptly make changes to the model and assess the impact of these changes on the current risk. The novelty of the project is the use of a modified modularization method, which significantly accelerates the generation of many minimal sections.*

***Keywords**: probabilistic safety analysis, NPP, fault trees, event trees.*

## 1. Introduction

Probabilistic safety analysis of a nuclear power plant (PSA) is a system safety analysis of a nuclear power plant unit, during which probabilistic models are developed and probabilistic safety indicators are determined, and the results of which are used for qualitative and quantitative assessments of the level of safety of a nuclear power plant unit and development of decisions during design and operation unit of a nuclear power plant [1].

The main requirements for the implementation of PSA are given in [2-6].

A detailed description of the «Risk» and «RISK-SPECTRUM» Software tools is given, respectively, in [7] and [8].

To determine the unavailability of primary events in the PSA model development, probabilistic reliability models of elements of the following types are used:

- constantly monitored, restored element (type 1),
- periodically checked item (type 2),
- an element with constant unavailability over time, characterized by a refusal of a requirement (type 3),
- element with a fixed working time (type 4),
- an event characterized by a constant frequency (type 5),
- non-recoverable item (type 6).

Table 1 shows the parameters used as input data, and the corresponding parameters of the formulas used to calculate the unavailability of elements.

**Table. 1.** Parameters used as input

| Formula Options | Description | Codes |
|---|---|---|
| Q | The probability of failure on demand | q |
| λ | Failure rate | r |
| F | Frequency | f |
| W | Failure Flow Parameter | W |
| μ | Recovery flow parameter (frequency) | 1/TR |
| TR | Average recovery time | TR |
| TI | Test Interval | TI |
| TF | First check time | TF |
| TM | Work time | TM |

## 2. Calculation models

1. Constantly monitored, restored element (type 1). Unavailability Q (t) of this type element is calculated by the formula

$$Q(t) = qe^{-\mu t} + \left(\frac{\lambda}{\lambda+\mu}\right) \cdot \left(1 - e^{-(\lambda+\mu)t}\right). \quad (1)$$

Required Parameters: λ, μ(r,TR).
Optional parameters: q.

2. Periodically checked item (type 2)
Required Parameters: λ, TI(r,TI).
Optional parameters: q, TR, TF.

The required parameters characterize the traditional model of a periodically controlled element. For such model, the unavailability of this type element Q(t) is calculated by the formula

$$Q(t) = 1 - e^{-\lambda(t-TI)}, \text{TI} = 0, TI, 2TI, \ldots \quad (2)$$

3. An element with constant unavailability over time, characterized by a refusal of a requirement (type 3). This is the simplest and most frequently used model, using the only q parameter - the probability of the request failure. In this case, the formulas are used

$$Q(t) = q, Q_{mean} = q, \quad \text{W(t)=0.} \quad (4)$$

4. Element with a fixed working time (type 4)
Required Parameters: λ, TM.
Optional parameter: q.
The following formulas are used

$$Q(t) = q + 1 - e^{-\lambda TM}, Q_{mean} = q + 1 - e^{-\lambda TM}, W(t) = 0. \quad (5)$$

5. An event characterized by a constant frequency (type 5). This model is used when the event is well described by the Poisson process, i.e. when events occur at a constant frequency. In this case, the only parameter f.

$$Q(t) = 0, Q_{mean} = 0, \quad \text{W(t)=f.} \quad (6)$$

6. Non-recoverable item (type 6).
Required Parameter: λ(r).
Optional parameter: q.

$$Q(t) = q + 1 - e^{-\lambda t}, \text{W(t)} = \lambda(1\text{-Q}(t)). \quad (7)$$

For each calculation option, an analysis of the minimum cross sections is carried out.

The uncertainty analysis is carried out in addition to the point estimate obtained in the analysis of the minimum cross sections. The uncertainty analysis is based on a simple version of the Monte Carlo method.

The parameters of the reliability models of primary events have their own (regardless of primary events) record in which the developer sets a point (average) value of the reliability parameter and, if the uncertainty of the parameter is taken into account, the distribution of uncertainty. Distributions are used such as:

- Lognormal – fig. 1;
- Gamma – fig. 2;
- Beta – fig. 3;
- Normal – fig. 4;

– Uniform – fig. 5;
– Log-uniform – fig. 6;
– Discrete - fig. 7.

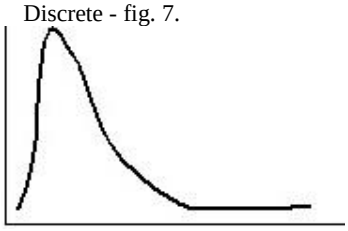

**Fig. 1.** Lognormal Distribution Example

**Fig. 2.** Gamma Distribution Example

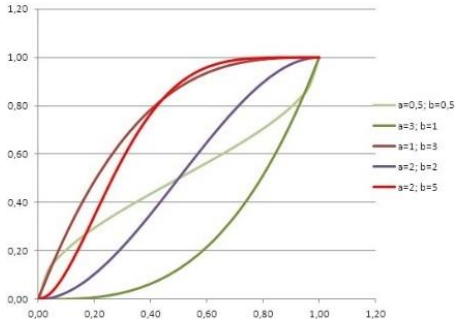


**Fig. 3.** Beta Distribution Example

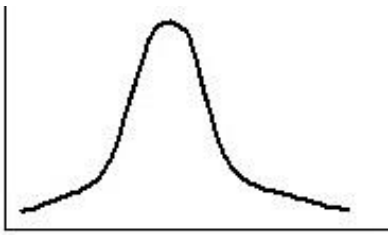

**Fig. 4.** Normal Distribution Example

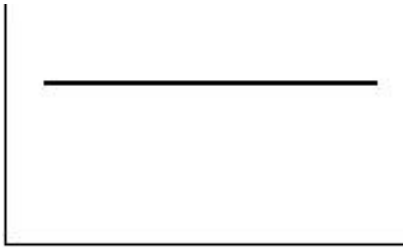

**Fig. 5.** Uniform Distribution Example

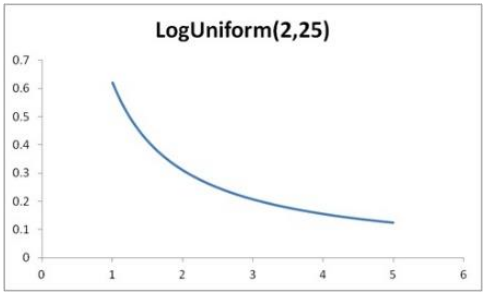


**Fig. 6.** Log-uniform Distribution Example

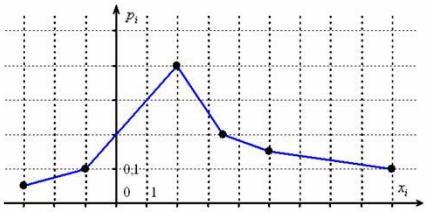


**Fig. 7.** Discrete Distribution Example

## 3. Unavailability indicators calculation for simple structures

1. Logical operator «OR». In terms of fault trees, such a structure corresponds to logic of the «OR» type, i.e. at least one input event occurs (Fig. 8). In mathematical expressions, the operator «OR» is indicated by the symbol «∪« or the sign «+».

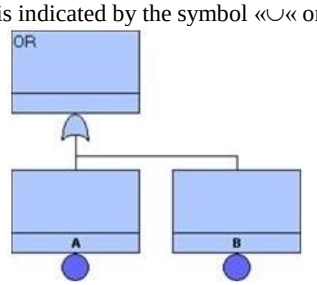


**Fig. 8.** Example of a fault tree with the logical operator «OR»

According to the formula of total probability, the probability of the event AB (P(AB)) will be equal to:

$$P(AB) = P(A) + P(B) - P(AB). \quad (8)$$

2. Logical operator «AND». In terms of fault trees, such a structure corresponds to logic of the «AND» type, i.e. all input events occur (Fig. 9). In mathematical expressions, the operator «AND» is indicated by the symbol «∩» or the sign «•».

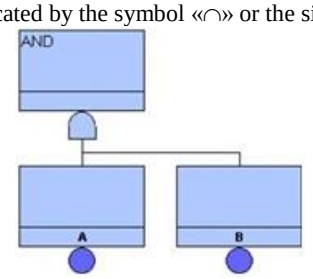


**Fig. 9.** Example of a fault tree with the logical operator «AND»

By the multiplication theorem, the probability of the event AB (P(AB)) will be equal to:

$$P(AB) = P(A) \cdot P(B). \quad (9)$$

3. Logical operator «K from N» (K / N). For such a system, the failure criterion is the failure of any K elements from N (for example, two elements from three). In this case, a logical operator of type K / N is used in the fault tree (Fig. 10).

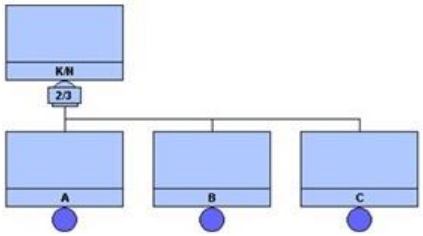


**Fig. 10.** Example of a fault tree with the logical operator «K/N»

According to the formula of total probability and the multiplication theorem, the probability of the event ABC (P(ABC)) will be equal to:

$$P(ABC) = P(AB) + P(BC) + P(AC) - P(ABBC) - P(BCAC) - P(ABAC) - P(ABBCAC). \quad (10)$$

4. Logical operator «NOR». In terms of fault trees, such a structure corresponds to the logic of the «Not OR» type, i.e. denial of OR or none of the events occur (Fig. 11).

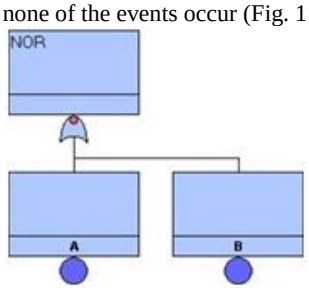


**Fig. 11.** Example of a fault tree with the logical operator «NOR»

According to the multiplication theorem, the probability of the event $\overline{AB}$ ($P(\overline{AB})$) will be equal to

$$P(\overline{AB}) = (1 - P(A)) \cdot (1 - P(B)). \quad (11)$$

5. Logical operator NAND. In terms of fault trees, this structure corresponds to the logic of the «Not and» (NAND) type, i.e. denial of AND or not all events occur (Fig. 12).

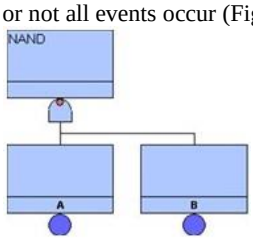


**Fig. 12.** Example of a fault tree with the logical operator «NAND»

According to the formula of total probability, the probability of the event $\overline{AB}$ ($P(\overline{AB})$) will be equal to:

$$P(\overline{AB}) = P(A) + P(B) - P(\overline{AB}). \quad (12)$$

6. Logical operator XOR. In terms of fault trees, this structure corresponds to the logic of the type «OR only» (XOR), i.e. strictly one of the input events occurs (with the exception of the OR operator) (Fig. 13).

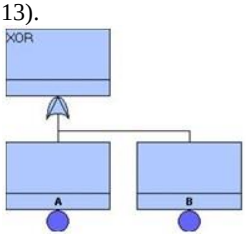


**Fig. 13.** Example of a fault tree with the logical operator «XOR»

According to the formula of total probability and the multiplication theorem, the probability of the event AB (P(AB)) will be equal to:

$$P(AB) = P(A) \cdot \big(1 - P(B)\big) + \big(1 - P(A)\big) \cdot P(B) - \\ -((1 - P(A)) \cdot (1 - P(B)). \quad (13)$$

7. Logical operator XAND. In terms of fault trees, such a structure corresponds to the logic of the «And Only» (XAND) type, i.e. exactly one event does not occur (Fig. 14).

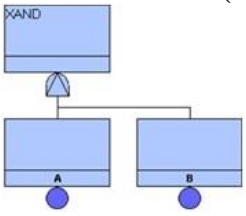


**Fig. 14.** Example of a fault tree with the logical operator «XAND»

According to the formula of total probability and the multiplication theorem, the probability of the event AB (P(AB)) will be equal to:

$$P(AB) = P(A) \cdot P(B) + \Big(P(A) \cdot \big(1 - P(B)\big)\Big) + \\ +((1 - P(A)) \cdot P(B) - P(AB). \quad (14)$$

8. Logical operator NXOR. In terms of fault trees, such a structure corresponds to the logic of the «NON-EXCLUSIVE OR» (NXOR) type, i.e. no event takes place (denial of XOR) (Fig. 15).

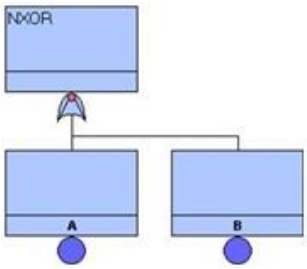


**Fig. 15.** Example of a fault tree with the logical operator «NXOR»

According to the formula of total probability and the multiplication theorem, the probability of the event AB (P(AB)) will be equal to:

$$P(AB) = \big(1 - P(A)\big) \cdot P(B) + \Big(P(A) \cdot \big(1 - P(B)\big)\Big) - P(AB). \quad (15)$$

9. Logical operator NXAND. In terms of fault trees, such a structure corresponds to the logic of the type «NON-EXCLUSIVE AND» (NXAND), i.e. only one event is realized (negation of XAND) (Fig. 16).

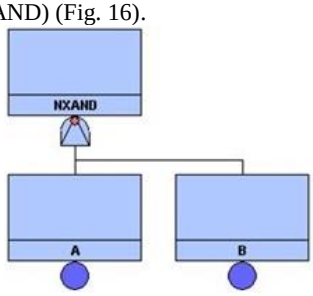


**Fig. 16.** Example of a fault tree with the logical operator «NXAND»

According to the formula of total probability and the multiplication theorem, the probability of the event AB (P(AB)) will be equal to:

$$P(AB) = \big(1 - P(A)\big) + (1 - P(B)) \cdot \big(1 - P(A)\big) + \\ +P(B)) \cdot \big(1 - P(B)\big) + P(A) - P(AB). \quad (16)$$

10. Logical operator NOT. NOT - the operator «NOT» (ie, the negation operator) (Fig. 17).

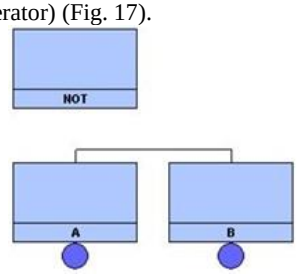


**Fig. 17.** Example of a fault tree with the logical operator «NOT»

## 4. Calculation of unavailability indicators for systems of medium complexity

An example of a fault tree is shown in Fig. 18. Comparative results and calculation results are given in tables 2-4 and in fig. 19-21.

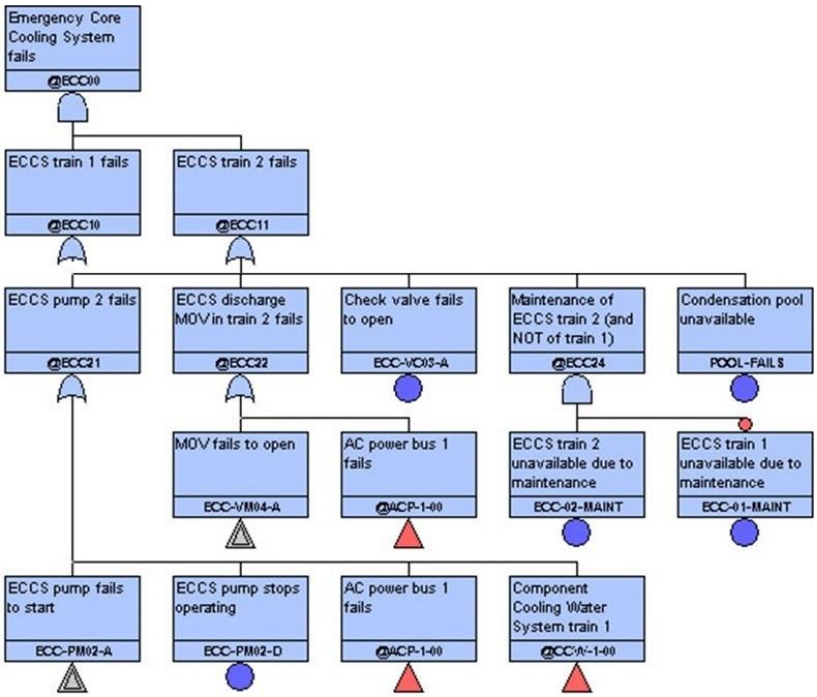


**Fig. 18.** Fault Tree Example

**Table. 2.** Fault trees. Average unavailability rate

| Top event | The number of minimal cutset | RISK SPECTRUM | РИСК |
|---|---|---|---|
| SYS-DPS | 52 | 1.364E-002 | 1.364e-002 |
| SYS-ECCS | 124 | 6.137E-003 | 6.161e-003 |
| SYS-EFWS | 125 | 6.898E-003 | 6.932e-003 |
| SYS-MFWS | 7 | 3.265E-002 | 3.265e-002 |
| SYS-RHRS | 147 | 5.843E-003 | 5.861e-003 |

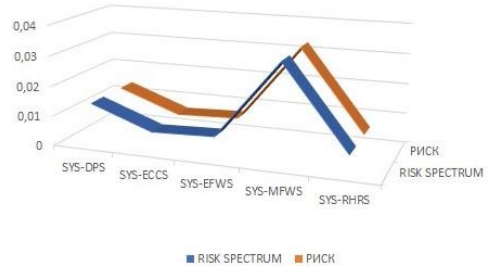


**Fig. 19.** Fault trees. Average unavailability rate

**Table. 3.** Consequences. Event frequency

| Top event | The number of minimal cutset | RISK SPECTRUM | РИСК |
|---|---|---|---|
| CD-ALOCA | 199 | 1.196E-006 | 1.198E-006 |
| CD-TRANS | 141 | 2.021E-004 | 2.022E-004 |
| CORE DAMAGE TOTAL | 3480 | 2.033E-004 | 2.034E-004 |
| CD-FIRES | 3820 | 2.404E-009 | 2.305E-009 |

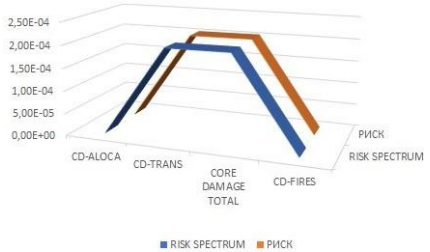


**Fig. 20.** Consequences. Event frequency

**Table. 4.** Sequences. Event frequency

| Top event | The number of minimal cutset | RISK SPECTRUM | РИСК |
|---|---|---|---|
| ALOCA-02 | 92 | 5.802E-007 | 5.811e-007 |
| ALOCA-03 | 82 | 6.098E-007 | 6.112e-007 |
| ALOCA-04 | 201 | 1.098E-008 | 1.092e-008 |
| F-EC001-01 | 1 | 1.000E-006 | 1.000E-006 |
| F-EC001-06 | 11 | 5.248E-010 | 5.248E-010 |
| F-EC001-08 | 0 | 0.000E+000 | 0.000E+000 |
| F-EC001-09 | 0 | 0.000E+000 | 0.000E+000 |
| F-EC001-10 | 3 | 4.434E-012 | 4.495E-012 |
| F-RB001-06 | 26 | 3.378E-010 | 3.323E-010 |
| F-RB001-08 | 0 | 0.000E+000 | 0.000E+000 |
| F-RB001-09 | 0 | 0.000E+000 | 0.000E+000 |
| F-RB001-10 | 0 | 0.000E+000 | 0.000E+000 |
| F-RB002-06 | 13 | 2.440E-010 | 2.432E-010 |
| F-RB002-09 | 0 | 0.000E+000 | 0.000E+000 |
| F-RB002-10 | 0 | 0.000E+000 | 0.000E+000 |
| TRANS-04 | 1776 | 9.761E-006 | 9.817E-006 |
| TRANS-05 | 1654 | 1.014E-005 | 1.021E-005 |
| TRANS-06 | 3017 | 1.825E-004 | 1.825E-004 |
| TRANS-08 | 4967 | 1.325E-007 | 1.304E-007 |
| TRANS-09 | 5270 | 1.376E-007 | 1.355E-007 |
| TRANS-10 | 1819 | 2.496E-006 | 2.496E-006 |

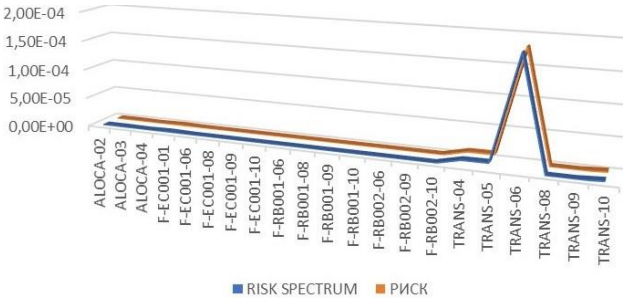


**Fig. 21.** Sequences. Event frequency

## 5. Results

In this article, a comparative calculation of the probabilistic analysis of safety and reliability using the RISK [7] and RISK-SPECTRUM [8].

The sets of minimum sections completely coincided for all fault trees. The probabilities of all the corresponding minimal cross sections also coincided.

In accordance with [9], the error in the PSA calculation results does not exceed 0.15.

## 6. Conclusions

To significantly reduce the calculation time of existing and developed codes and to increase the accuracy of probabilistic safety assessments, including when monitoring the safety of the current state of the power unit in real time (risk monitoring), it is necessary to develop methods and algorithms that accelerate the process of constructing a set of minimum sections for assessing the reliability and safety parameters of complex probabilistic models of nuclear power plants with a large number of fault trees.

## 7. Acknowledgments

The study was carried out within the framework of grants 19-07-00455, 20-07-00577 and 17-07-01475.

## 8. References:

[1] The main recommendations for the development of a probabilistic safety analysis of level 1 for a nuclear power plant unit at initiating events caused by external influences of natural and technogenic origin. Safety Guide RB-021-14, Rostekhnadzor, 2014.

[2] Recommendations on the procedure for performing the reliability analysis of systems and elements of nuclear plants important for safety and their functions. Safety Guide RB-100-15, Rostekhnadzor, 2015.

[3] General provisions for the safety of nuclear power plants. Federal norms and rules in the field of atomic energy use NP 001-15, Rostekhnadzor, 2015.

[4] NUREG/CR-2300, «PRA Procedures Guide», US NRC, January 1983.

[5] NUREG/CR-2815, «Probabilistic Safety Analysis Procedures Guide», US NRC, August 1985.

[6] NUREG/CR-4550. Analysis of Core Damage Frequency from Internal Events: Methodology Guidelines. Volume 1. US NRC, September 1987.

[7] Development of guidelines for the implementation of tasks within the PSA of levels 1 and 2 for all operational states and categories of initiating events of power units of RBMK-1000 NPPs. Guidelines for the development of PSA-1. Guidelines for the development of a database for VAB-1 NPPs with RBMK-1000, taking into account data for equipment aging models. Guidelines for the analysis of personnel reliability. Guidelines for the analysis of the uncertainty, significance and sensitivity of the results of the PSA-1 nuclear power plant with RBMK-1000: research report reg. No. 1562MY09 / Dmitriev A.V., Golubkov A.V., Elizarov A.I., Berberova M.A., Derevyankin A.A. - M .: International Center for Nuclear Safety, 2009. - 287 p.

[8] RiskSpectrum. [Electronic resource] – URL: http://www.riskspectrum.com/

[9] On ensuring the uniformity of measurements: [Federal Law No. 102-FZ dated 06/26/08: adopted by the State Duma on June 11, 2008]. - M., 2008 . - 16 p.