# Methodological Recommendations for the Cyber Risks Management*

Alexsandr A. Petrenko[1], Sergei A. Petrenko[2] [0000-0003-0644-1731], Krystina A. Makoveichuk [3] [0000-0003-1258-0463], Alexander A. Olifirov [3] [0000-0002-5288-2725]

[1] Russian Technological University (MIREA), Moscow, Russia
[2] Innopolis University, Kazan, Russia
[3] V.I. Vernadsky Crimean Federal University, Simferopol, Russia
s.petrenko@rambler.ru
christin2003@yandex.ru

**Abstract.** The task complexity of the cyber risks, as well as their components (threats and vulnerabilities) identification, depends on the requirements for the mentioned detailing. At the basic level (*third level of organization maturity*), there are generally no specific requirements for detailing, and it is sufficient to use the standard list of cyber risks classes. At the same time, the amount of risk assessment is not considered, which is acceptable for some types of basic level techniques. For example, the *German BSI Standard*[1] contains a catalog of typical cyber-threats for component-information infrastructure. The advantage of such lists is the acceptable completeness level: classes, usually, are few (*dozen*), they are quite wide and consciously cover all existing sets of cyber risks. The disadvantage is the difficulty in assessing the cyber risk level and the effectiveness of countermeasures for a wide class since it is more convenient to make settlements of the narrower (*specific*) risk classes. For example, "*router malfunction*" risk class can be divided into many subclasses, including possible types of malfunction (*vulnerability*) of the software of the particular router and equipment malfunction.

**Keywords:** Digital Transformation, Digital Economy, Cyber Resilience, Manageability Capability, Self-Organization, Proactive Cybersecurity and Adaptability, Models and Methods of Artificial Intelligence, Cognitive Computing, Big Data, Robotics, Internet of Things IIoT/IoT.





[1] https://www.bsi.bund.de/EN/Publications/SecuritySituation/SecuritySituation_node.html

## 2 Cyber risks assessment

The cyber risk assessment recommends considering the following aspects:

– Cyber risk measurement scales;

– Assessing the likelihood of events;

– Measurement methods for cyber risks.

To *measure* a property, you have to select a *scale*. Scales can be *direct (natural) or indirect (derivative)* [1, 5, 6]. Examples of the direct scales are the physical quantity measurement scales, for example - liters to measure volume, meters for length measurement, and so on. In some cases, the direct scales do not exist, it is necessary to use direct scales of other properties in our interest, or to identify new scales. An example is a scale to measure the subjective property "*value of an information resource*". It can be measured in *derived scales*, such as the cost of the *resource recovery, resource recovery time*, etc. Another option is to define a scale for obtaining an *expert assessment*, for example, having three values:

–*Low-value information resource*: critical tasks do not depend on it and it can be restored with a small investment of time and money

– *Resource of average value*: some important tasks depend on it, but in the event of its loss it can be restored in less time than critical, the cost of restoration is high

– *A valuable resource*: critical tasks depend on it, in the event of loss the recovery time exceeds the critical, or the cost is extremely high.

There is no natural scale for measuring cyber risks. Risks can be assessed by *objective or subjective criteria*. An example of objective criteria is the failure probability of any equipment, such as a firewall, in a limited time. An example of subjective criteria is the information resource owner's assessment of the firewall failure risk. To this end, a qualitative scale is usually developed with several gradations, for example: *low, medium, high level* [2-6]. Risk analysis methods, generally, use the subjective criteria, measured in qualitative scales, since:

The assessment should reflect the subjective point of view of the information resources owner.

Various aspects should be taken into account, not only technical but also organizational, psychological, etc.

You can use a direct expert assessment, or define a function that reflects objective data (*probability*) on a *subjective risk scale* to obtain a *subjective assessment*. Subjective scales can be *quantitative and qualitative*, but in practice, generally, the qualitative scales with **3-7** gradations are applied. On the one hand, it is simple and convenient, on the other hand, it requires a competent approach for data processing.

In estimating the probability of events, the following must be taken into account. The term "*probability*" has several different meanings. The most common two interpretations are "*objective probability"* and *"subjective probability*". *Objective (sometimes referred to as physical) probability* means the relative frequency of occurrence of an event in the total amount of observations or the ratio of the number of favorable outcomes to their total number. Objective probability is used in analyzing the results of a large number of past observations, and also as consequences of models describing

some processes. *Subjective probability* is a measure of a person's confidence or confidence in the group of people that the event will take place. As a measure of a person's confidence in the possibility of an event occurring, subjective probability can be formally represented in various ways: *a probability distribution on a set of events, a binary relation on a set of events, not completely defined by a probability distribution or a binary relation and other methods*. Most frequently, subjective probability is a probabilistic measure obtained by an expert way. In modern works, in the system analysis area, subjective probability does not simply represent a measure of confidence on a set of events, but is linked to a decision maker's preferences system (DM), and ultimately to an utility *function reflecting* his preferences on a variety of alternatives. The close link between subjective probability and usefulness is used in constructing some methods for obtaining subjective probability.

The process of obtaining the subjective probability is usually divided into *three stages*: the *preparatory stage, the stage of receiving estimates, the stage of analysis of the obtained estimates*. During the *first stage*, the object of research is formed - a set of events. A preliminary analysis of the properties of this set is given ( dependence or independence of events are established, discreteness or continuity of a random variable generating the given set of events). Based on such an analysis, one of the appropriate methods for obtaining subjective probability is selected. At the same stage, an expert or a group of experts are trained. They are informed of the method and checked by the experts for understanding the task set. The *second stage* is to apply the method chosen in the first stage. The result of this stage is a set of numbers that reflects the subjective opinion of an expert or group of experts on the probability of an event, but it is not always possible to be considered as a final distribution, because it can be contradictory. Finally, the *third stage* consists of studying the survey results. If the probabilities received from the experts do not agree with the axioms of probability, then the experts' attention is drawn to this and the answers are refined to bring them into line with the chosen system of axioms. For some methods of obtaining subjective probability, the third stage is not carried out, since the method consists of choosing the probable distribution obeying the axioms of probability, which in one sense or another is closest to the estimates of experts. The third stage is of special importance in the aggregation of estimates obtained from the expert group. The technology of aggregating the group assessments with risk factors will be discussed in greater detail below.

## 3 Approaches to Measuring the Cyber Risks

Today, there are some approaches to measuring the cyber risks, for example, the *assessment of cyber risks by two and three factors* [5, 6]. In the simplest case, the two-factor cyber risk assessment is applied: the probability of an accident and the severity of possible consequences. It is usually considered that the greater cyber risk is the greater the probability of an accident and the severity of the consequences. The general idea can be expressed by the following equation 1:

$$CYBERRISK = P\ Incidents * LOSS\ PRICE \quad (1)$$

If the variables are quantities, the cyber risk is an estimate of the expectation of loss.

If the variables are qualitative quantities, then the metric multiplication operation is not defined. Thus, this formula should not be used explicitly.

Let us consider the use of qualitative quantities (the most common situation). Scales must be defined first.

The subjective probability scale of events is to be determined:

*A* - Event rarely happens.

*B* - Event rarely happens.

*C* - The probability of an event for the considered period is about 0.5

*D* - Most likely, an event will occur

*E* - Event will almost certainly happen.

In addition, a subjective severity scale is determined:

*N (Negligible)* - Impact can be neglected

*Mi (Minor)* - Minor Incident: the consequences are easily removable, the costs of eliminating the consequences are not great, the impact on the information infrastructure is insignificant.

*Mo (Moderate)* - An event with moderate results: eliminating the consequences is not associated with large costs, the impact on the information infrastructure is not large and does not affect the critical processes.

*S (Serious)* - An incident with serious consequences: the elimination of consequences are associated with significant costs, the impact on the information infrastructure is palpable, significantly affects the critical processes.

*C (Critical)* - An incident leads to an irreversible critical state and the inability to continue the business.

To assess the cyber risks, a scale of three values is determined:

– Low Cyber Risk

– Medium Cyber Risk

– High Cyber Risk

The cyber-risk associated with a particular event depends on two factors and can be defined as follows (see Table 1):

**Table 1.** The definition of cyber risk depending on two factors.

| | Negligible | Low risk | Low risk | Medium risk | Medium risk |
|---|---|---|---|---|---|
| A | Low risk | Low risk | Low risk | Medium risk | High risk |
| B | Low risk | Low risk | Medium risk | Medium risk | High risk |
| C | Low risk | Medium risk | Medium risk | Medium risk | High risk |
| D | Medium risk | Medium risk | Medium risk | Medium risk | High risk |
| E | Medium risk | High risk | High risk | High risk | High risk |

The scales of the cyber risk factors and the table itself can be defined differently, have a different number of levels. Such an approach to assessing cyber risks is quite common. In developing (using) cyber risk assessment techniques, the following features should be considered:

– The scale values should be clearly defined (verbal description) and should be understood in the same way by all participants in the peer-review procedure.

– Justification of the selected table is required. It is necessary to make sure that different incidents characterized by the same combinations of cyber risk factors have the same level of cyber risks from the expert's point of view. There are special verification procedures for that [5-10]. Such techniques are widely used in the analysis of cyber risks, the so-called basic or initial level.

In the case of higher requirements than the base level, as a rule, a cyber risk assessment model is used with three factors: threat, vulnerability, cost of loss. In this case, the threat and vulnerability are defined as follows:

*Threat* - a set of conditions and factors that can cause a violation of cyber resistance (cybersecurity).

*Vulnerability* - weakness in the system of protection, which makes possible the threat realization.

The probability of an incident, which in this approach can be an objective or subjective value, depends on the levels (probabilities) of threats and vulnerabilities:

$$P\ incident = P\ threat * P\ vulnerability \quad (2)$$

Accordingly, the cyber risk is defined as follows:

$$CYBER\text{-}RISK = P\ threat * R\ vulnerabilities * LOSS\ PRICE \quad (3)$$

This expression can be considered as a mathematical formula if the quantitative scales are used, or as a formulation of a general idea, if at least one of the scales is qualitative. In the latter case, various tabular methods are used to determine the risk depending on three factors.

For example, the cyber risk is measured on a scale from 0 to 8 with the following definitions of risk levels:

**1** – cyber-risk is almost absent. Theoretically, the situations in which an event occurs are possible, however, in practice, this happens rarely and the potential damage is relatively small.

**2** – cyber-risk is very small. This kind of event happens quite rarely, in addition, the negative effects are relatively small.

**8** - Cyber Risk is large enough. The event is likely to come, and the consequences will be extremely complex.

The matrix can be defined as follows (Table 2)

**Table 2.** Determining the cyber risk level based on three factors.

| SI severity | Threat level | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Low | | | Moderate | | | High | | |
| | Vulnerability level | | | Vulnerability level | | | Vulnerability level | | |
| | H | C | B | H | C | B | H | C | B |
| Negligible | 0 | 1 | 2 | 1 | 2 | 3 | 2 | 3 | 4 |
| Minor | 1 | 2 | 3 | 2 | 3 | 4 | 3 | 4 | 5 |
| Moderate | 2 | 3 | 4 | 3 | 4 | 5 | 4 | 5 | 6 |
| Serious | 3 | 4 | 5 | 4 | 5 | 6 | 5 | 6 | 7 |
| Critical | 4 | 5 | 6 | 5 | 6 | 7 | 6 | 7 | 8 |

In Table 2 the H, C, C levels of vulnerability mean respectively: low, medium, and high. Such tables are used both in "paper" versions of cyber risk assessment methodologies and in various kinds of tools for cyber risk analysis. In the latter case, the matrix is set by the developers of the corresponding software and, as a rule, is not subject to adjustment. This is one of the factors limiting the accuracy of this kind of toolkit.

## 4 Assessment Method of Threats and Vulnerabilities

As a rule, for assessing threats and vulnerabilities may be involved:

– Expert evaluation.
– Statistical data.
– Consideration of factors affecting the levels of threats and vulnerabilities.

Here, one of the possible approaches is the accumulation of statistical data on actual incidents, the analysis, and classification of their causes, the identification of the factors on which they depend. The threats and vulnerabilities of the critical information infrastructure can be assessed based on this information [5, 6, 8-12].

The practical difficulties in this approach implementation are as follows. First, very extensive material on incidents should be collected in this area. Secondly, the use of this approach is not always justified. If the information infrastructure is large enough (contains many components, located on a vast territory), has a long history, then this approach is most likely applicable. If the system is relatively small, it uses the latest information technologies (for which there are no reliable statistics yet), the threat and vulnerabilities estimates may be unreliable.

A more common approach is currently based on various factors affecting the levels of threats and vulnerabilities [5, 13-15]. Such an approach allows one to abstract from the insignificant technical details, to take into account not only program-technical but also other aspects. For example, the well-known *CCTA Risk Analysis and Management Method, CRAMM Version 5.0*.[2] for the class of cyber risks: "*The use of someone else's*

[2] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html

*identifier by employees of the organization ("masquerade") "offers to select the following indirect factors for threat assessment*:

– Statistics on the recorded incidents.

– Trends in statistics for similar violations.

– The presence of information useful to potential internal or external violators in the system.

– The moral quality of staff.

– Ability to benefit from changes in the information processed in the system.

– Availability of alternative ways to access information.

– Statistics on similar violations in other information systems of the organization.

The following indirect factors are proposed for assessing vulnerabilities :

– The number of jobs (users) in the system.

– The size of the working groups.

– Management awareness of the actions of employees (various aspects).

– The nature of the equipment and software used in the workplace.

– The user rights.

Further, according to indirect factors, there are some questions and several fixed answers, which *"cost*" a certain number of points. The final assessment of the threat and vulnerability of this class is determined by summing up the scores (Table 3).

**Table 3.** Threat level according to the number of points.

| Points | Threat level | Vulnerability level |
|---|---|---|
| Till 9 | Very low | Low |
| From 10 to 19 | Low | Medium |
| From 20 to 29 | Medium | |
| From 30 to 39 | High | High |
| 40 and more | Very high | |

The advantage of this approach is the possibility of taking into account a variety of indirect factors (not just technical ones). The technique is simple and gives the information resource owner a clear idea of how the final grade is obtained and what needs to be changed to improve the scores.

*Disadvantages*: Indirect factors and their values depend on the scope of the organization, as well as on some other circumstances. Herefore, the technique always requires an adjustment to a specific object. In this case, the completeness proof of the selected indirect factors and the correctness of their values (the task is slightly formalized and complex) is solved in practice by expert methods (checking the conformity of the results obtained by the method with those expected for test situations).

Such techniques, as a rule, are developed for organizations of a certain profile (departments), are tested, and then used as a departmental standard. *CRAMM* developers also took this path, creating about a dozen versions of the method for various departments (*Ministry of Foreign Affairs, Ministry of Defense, government*, etc.) [6-9].

Let us note that the assessments of cyber risks and vulnerabilities in the considered example are qualitative values. However, such methods can also be used to obtain quantitative estimates that are necessary for calculating residual risks and solving optimization problems. For this purpose, some methods, which make it possible to establish a distance system on an ordered set of estimates, are applied. Obtaining objective quantitative risk assessments is also relevant for insurance agencies involved in insuring information risks. In practice, insurance agencies use quality assessments in most cases. Simple techniques, without a lengthy and expensive survey, allow us to assign the key components and services of the company's information infrastructure to a particular group of cyber risks (according to the classification of the insurance company) based on interviews with some officials. In such techniques, indirect factors are also recorded and analyzed.

## 5 Methods for Subjective Probability

Generally, the necessity of obtaining subjective probability arises in the following cases: when the objective probability is defective; if it is assumed that the obtained conformities and objective probability won't be observed in the future; when there is no objective observation data in the past.

*Classification of methods of subjective probability*

Methods of subjective probability can be classified depending on the *form* of *issues* posed to the experts or on the *event characteristics and random variables* and also depending on the *number of experts* involved in obtaining the probabilities. For cyber risk assessment of the tasks in a context of uncertainty, it is required to make a probability (possibility) estimate of environmental conditions (unidentified factors). Since the external environment can assume only one value from a given set usually the methods for sets of incompatible events for estimation of subjective probabilities are applied. Among methods designed for probabilities estimate in case of finite sets of incompatible events, more practical value was obtained by the following methods: *direct probability assignment method, ratio technique, and eigenvalue method*, in case of infinite sets of incompatible events - *variable interval method and the fixed interval method* [6 - 10].

The detailed elaboration and adaptation of the above-mentioned methods are required for practical implementation and solving issues of cyber resilience and cybersecurity. It is also required to develop and implement the specific algorithms for interviewing experts in these methods. In addition to algorithms, implementing the specified methods it is necessary to create graphical representation procedures on the data obtained from the expert. This will allow the experts to make necessary adjustments in their previous estimates based on the overall picture. The procedures for probabilities aggregation should be established for the processing of probabilities, obtained from several experts. They can be based on the *weighted sum method*. To improve the expert assessments consistency, an iterative examination procedure based on *the Delphi technique* is usually developed.

Conventionally, methods for obtaining subjective probability can be divided into the following three groups: *direct, indirect, and hybrid*. *The first* and the largest group of methods is the *direct methods* where the expert answers the question about the probability of an event. These methods include *a variable interval method, fixed interval method, ratio technique, diagram method, eigenvalue method, estimating method of distribution parameters,* and other methods. Regardless of the specific method of this group, an expert should directly estimate the event probability. *The second group* of methods - the methods, when the event probability is derived *from the experts' decisions* in a particular hypothetical situation. The examples would be *a lottery method and also an equivalent basket method.* Conventionally speaking, an application of methods from the second group requires an expert to compare not the probabilities as such, but the useful alternatives in which the outcome depends on the implementation of a random variable. Many experts note the increasing complexity of the questions and more significant errors in applying these methods in comparison to the methods of the first group. *The third group* of methods - *the hybrid methods* where the experts answer the question both about probability and utility value. Some varieties of the *lottery method* [6, 11 - 14] fall into the category of hybrid methods.

*Obtaining the subjective probability problem statement*

The problem statement is the requirement to develop probability distribution on a finite set of incompatible (exclusive) events [5, 7, 12] by interviewing the experts.

1) *Direct assessment of event probabilities*

In this method, an expert or a group of experts is provided with a list of all events. An expert shall consistently specify the probability of all the events. The method may have various modifications. In one of the modifications, it is proposed to firstly select the most probable event from the proposed list, and then to evaluate its probability. After that, this event is removed from the list and the same procedure is applied to the remaining list. The sum of all obtained probabilities must be equal to one.

2) *Ratio technique*

In this method, the expert is supposed to select the most probable event. The unknown probability is attributed to this event $P_1$. Then the expert shall evaluate the probabilities ratio of all other events to the $P_1$ probability of the selected event (coefficients $C_2 \ldots C_N$). Because the probabilities sum is equal to **1**, the following equation is composed:

$$P1(1 + C2 + C3 + \ldots + CN) = 1 \qquad (4)$$

Having solved this equation and finding the value of $P_1$, one can calculate the sought probabilities.

3) *Eigenvalue method*

The eigenvalue method is based on the fact that the unknown probability vector $(P_1, \ldots P_n)$ is the eigenvector of some specially designed matrix, corresponding to its largest eigenvalue. Firstly, the expert is asked which one of the two events is more probable. Assuming that the most probable event is $S_1$**.** Secondly, comes the question of what fold the $S_1$ event is more probable than the $S_2$ event. The ratio obtained from the expert is written in the relevant place in the matrix.

4) *Equivalent basket method*

This method allows obtaining a probability based on the expert comparison of the alternative utility. Assuming that it is required to calculate the probability of some $S_1$ event. Let us choose two any wins, for example, cash prizes, which are significantly different, e.g. the first is **1** thousand *$*, and the second is **0** *$*, and offer the expert a choice to participate in one of two lotteries. In the first lottery, the expert gets the cash prize (**1** million*$*) if the $S_1$ event takes place, and gets the second prize (**0** *$* rub.) if the event does not occur. To arrange the second lottery let us imagine a hypothetical basket filled with white and black balls, initially in equal proportions, for example, **50** balls of each color. If the participant picks the white ball, he/she receives a cash prize in the amount of **1** thousand *$*, if the black one - **0***$*.

The expert is suggested to give preference to one of two lotteries. If from the expert's point of view the lotteries are equal, it is concluded that the probability of the event $S_1$ equals **0.5.** If the expert prefers the first lottery, a part of black balls is removed from the basket and replaced with the same number of white balls. If the expert gives preference to the second lottery, a part of white balls is replaced with black ones. And again, in both cases, the expert is invited to participate in one of two lotteries. Having changed the ratio of balls in a hypothetical basket, the equivalence of the two lotteries can be achieved. Then the sought probability of the $S_1$ event equals the share of white balls in their total number.

*Methods for obtaining estimates of continuous distributions*

They are used to find the distribution function (or frequency distribution) of subjective probabilities of a continuous random variable. In practice, two methods are applied: *variable interval method and fixed interval method* [5, 6, 12-16].

*Variable interval method*

There are several modifications to this method. However, for all modifications, it is common for the expert to specify the set of values of a random variable such as an interval that the probability that the random variable takes on a value in the specified interval is equal to the specified value. For example, an expert interviewing can be based on the following scheme. At first, the expert specifies such a value of $P_1$ of a random variable that two probabilities become equal: a probability that a random variable takes on a value smaller than $P_1$ and a probability that a random variable takes on a value larger than $P_1$. The second stage starts after the value of $P_1$ is specified by the expert. At this stage, the expert specifies such a value of $P_2$ of a random variable that divides the range of values of larger $P_1$, into two equally probable parts. The same procedure is repeated with the range of values of smaller $P_1$ and evaluate $P_3$. After the second stage, it is possible to carry out the third stage, which consists of finding *median values* for each of the obtained parts. This process should take too long, as the probability of expert errors increases at small intervals. Applying this method, it is usually useful to return to the previously obtained estimates and analyze their consistency. When inconsistencies are found, the expert should change one of his estimates obtained earlier.

In some variations of the *variable interval method,* the expert can be asked to specify two points on the proposed set of values of a random variable, which divides the set into three equally possible parts. In other variants, the method can include the following questions: Specify such a value of a $P_1$ random variable that the probability that the

random variable will take a smaller value than $P_1$ is equal to **0.1.** The estimates obtained in this way are less dependent on each other, i.e. there is no error accumulation. This is their advantage. There are modifications of the method based on the assumption that it is easier for the expert to specify a point dividing the area into two equally probable parts than to specify a point separating the area corresponding to the probability **0.1** from the rest of the set. Thus, applying the variable interval method, it is necessary to choose between the comparison primality and the independence of the obtained estimates.

*Fixed interval method*

In this method, the set of values of a random variable is divided into intervals and the expert is asked to estimate the probability that a random variable will take a value from this interval. Typically, intervals are chosen of equal length, except for the far left and the far right intervals. The number of intervals is chosen, according to the required accuracy and the required distribution type. Once the expert has announced the probability of all intervals, the inspection of the obtained distribution is usually carried out. For example, if the same probability is assigned to two different intervals, the expert can be asked whether these intervals are equally probable. Relating to other intervals, it can be clarified whether one of them is so much more likely than the other, as it follows from the probabilities assigned to these intervals. As a result of such a review, the expert can somehow correct the probabilities. Sometimes the *fixed interval method* is applied in conjunction with the *variable interval method*. For example, first of all, the expert can be asked to determine the median, that is such a value of a random variable that divides the entire set of values into two equally probable sets, and then to single out equal fixed intervals in both directions from the found median.

*Graphical method*

The expert is asked to present in a graph form (in the form of a graph of the *distribution function, probability density function*, in the form of a diagram or graph) his/her idea *of the event probability or a random variable*. Frequently the general view of a graphical chart is specified and the expert is only required to choose the distribution parameters. The graphical method is useful as an auxiliary method in the analysis of probabilities obtained in any other way. For example, *the distribution function* is obtained with the help of *the fixed interval method* and then its *graphical chart*, as well as *the density function graph* is presented to the expert for finalization [5, 6, 17-20].

*Some recommendations*

It is known that subjective probability obtained by the expert method significantly depends on the applied method. In particular, the expert often tends to exaggerate the probability of the least probable event, as well as to underestimate the probability of the most probable event or to exaggerate the variance of the estimated random variable.

The following recommendations are proposed to conduct the more correct expert interviewing, using various methods.

1. The expert should be given grounding in the expert procedure assessment as far as it is possible. Especially those experts who have only initial training in probability theory.

2. It is clear that the procedure of expert interviewing is just one element in the whole process of obtaining probabilities. Previous steps for carving out events and selection

of the appropriate method are equally important. The subsequent analysis of the obtained probabilities should not be neglected for their possible adjustments.

3. The objective information about the event probabilities should be used, where possible and relevant, such as how these events have occurred in the past. This information should be notified to the expert. Previously obtained estimates of the expert should be also algebraically processed to compare them with the new estimates of the expert.

4. Any other methods of obtaining subjective probability or even modifications of methods should be used to verify the reliability of the obtained data. Probabilities obtained by different methods should be demonstrated to the expert to clarify his/her estimates.

5. The expert's experience with numerical indices should be taken into account, choosing a particular method. If this experience is insufficient, the fixed interval method is unsuitable, since it requires numerical estimates. The variable interval method is more appropriate here since within this method the expert is only required to make a statement about the equal probability of two intervals. In any case, the usage of the concepts, phrases, questions, and scales, familiar to the expert, contributes to his/her possibility of the numerical representation of probability.

6. Whenever it is possible, one should obtain subjective probability from several experts and then aggregate it somehow into a single one.

7. Elaborate methods which require a lot of effort from the expert, such as the lottery method, should not be used, except when there are compelling arguments for the use of these methods.

These recommendations can significantly improve the probability estimates used for the analysis and cyber risks management, for example, based on *ISO 15408* (Figure 1).

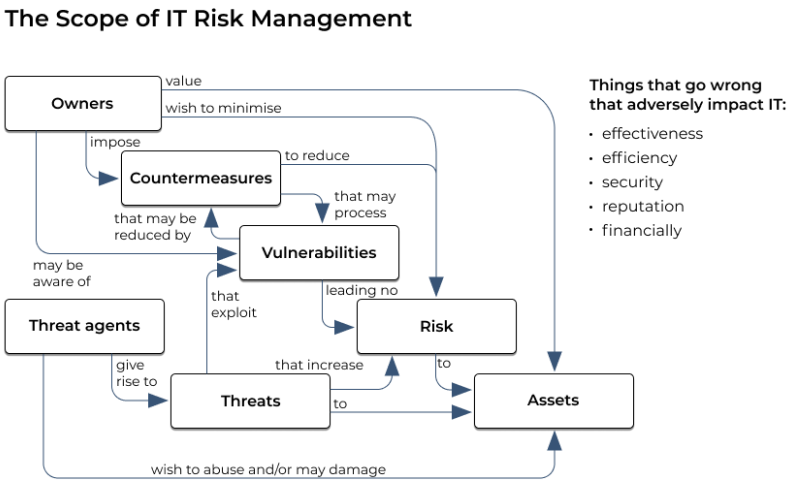


**Fig. 1.** Cyber risk management algorithm, ISO 15408.

## 6 Conclusion

The choice of an acceptable level of cyber risk is associated with the costs of implementing a system of cyber resistance, resiliency, and cybersecurity. At least there are two approaches to choosing an acceptable level of cyber risks. The *first approach* is typical for a basic level of cybersecurity, in which the level of residual cyber risks is not taken into account. Here, the costs of organizational and technical measures necessary to meet the protected information infrastructure with the basic level specifications (*UTM, SOC, SIEM. ME, VPN, IPS/IDS, antivirus software, backup systems, access control systems*) are mandatory, their expediency is not discussed.

The additional costs are within reasonable limits and do not exceed **5-15%** of funds for technical support and maintenance of the information infrastructure. The second approach is applied in providing enhanced levels of cybersecurity. The owner of information resources must choose the permissible level of residual cyber risks himself and be responsible for his choice. Depending on the maturity level of the organization, the nature of the main activity, the selection justification for choosing an acceptable level of cyber risk can be carried out in different ways. Here, the cost/effectiveness analysis of various variants of the cybersecurity system architecture is more common, for example, the following tasks are set:

– The cost of the cybersecurity subsystem should be not over 20% of the information infrastructure value. Find a variant of countermeasures that minimize the total level of cyber risks.

– The level of cyber risks in all classes should not be lower than “very low level”. Find a countermeasure option with a minimum cost.

In the case of optimization problems' statement, it is important to choose the right set of countermeasures (list possible options) and evaluates its effectiveness [5, 6, 21, 22].

**Acknowledgment**

The publication was carried out with the financial support of the Russian Foundation for Basic Research (RFBR) and the Government of the Republic of Tatarstan in the framework of the scientific project No. 18-47-160011 “Development of an early warning system for computer attacks on the critical infrastructure of enterprises of the Republic of Tatarstan based on the creation and development of new NBIC cybersecurity technologies ".

## References

1. Ross, R. S.: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (2018).
2. NIST Special Publication 800-160 VOLUME 4. Systems Security Engineering. Hardware Assurance Considerations for the Engineering of Trustworthy Secure Systems – (Draft), (December 20, 2020).
3. NIST SP 800-34. Rev. 1: Contingency Planning Guide for Federal Information Systems Paperback (February 18, 2014).

4. NIST, Framework for improving critical infrastructure cybersecurity, version 1.1, draft 2, (16 April 2018).
5. Petrenko, S.: Big Data Technologies for Monitoring of Computer Security: A Case Study of the Russian Federation, Springer Nature Switzerland AG (2018).
6. Petrenko, S.: Cyber Security Innovation for the Digital Economy: A Case Study of the Russian Federation, River Publishers. (2018).
7. ISO/IEC 27002:2013, Information technology. Security techniques. Code of practice for information security controls. URL: https://www.iso.org/standard/54533.html
8. ISO/IEC 27005:2018, Information technology. Security techniques
9. Kott, A., Linkov, I: Cyber Resilience of Systems and Networks (Risk, Systems, and Decisions), 2019 Springer Nature Switzerland AG, (2019)
10. Mailloux, L. O.: Engineering Secure and Resilient Cyber-Physical Systems (2018).
11. ISO 22301:2012. Societal security. Business continuity management systems – Requirements.
12. ISO 22313:2012. Societal security. Business continuity management systems – Guidance.
13. ISO/TS 22317:2015. Societal security. Business continuity management systems. Guidelines for business impact analysis (BIA).
14. ISO/TS 22318:2015, Societal security. Business continuity management systems. Guidelines for supply chain continuity.
15. ISO/TS 22330:2018, Security and resilience. Business continuity management system. Guidelines for people aspects of business continuity.
16. ISO/TS 22331:2018, Security and resilience. Business continuity management systems. Guidelines for business continuity strategy.
17. NIST Special Publication 800-160 VOLUME 2. Systems Security Engineering. Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems, (March 2018).
18. NIST Special Publication 800-160 VOLUME 3. Systems Security Engineering. Software Assurance Considerations for the Engineering of Trustworthy Secure Systems (December 20, 2019).
19. NIST Special Publication 800-160 VOLUME 4. Systems Security Engineering. Hardware Assurance Considerations for the Engineering of Trustworthy Secure Systems, (December 20, 2020).
20. Graubart, R.: The MITRE Corporation, Cyber Resiliency Engineering Framework, The Secure and Resilient Cyber Ecosystem (SRCE) Industry Workshop Tuesday, (November 17, 2015).
21. Ross, R. S., McEvilley, M., Oren, J. C.: Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems (March 21, 2018).
22. The BCI Cyber Resilience Report, Business Continuity Institute (2018)