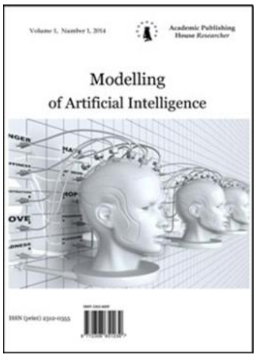

Published in the Russian Federation
Modeling of Artificial Intelligence
Has been issued since 2014.
ISSN: 2312-0355
E-ISSN: 2413-7200
2017, 4(2): 78-85

DOI: 10.13187/mai.2017.2.78
www.ejournal11.com

The Methodology of Risk Analysis in Assessing Information Security Threats

Andrey S. Kopyrin [a], Simon Zh. Simavoryan [a, *], Arsen R. Simonyan [a], Elena I. Ulitina [a]

[a] Sochi state university, Russian Federation

Abstract

Information security is not an IT problem and cannot be reduced to the IT department. Effective preservation of confidentiality, integrity and availability must be anchored throughout the organization. To meet this challenge efficiently, a risk-based approach is required. First, the organizational context must be determined. When implementing the risk management process, the quality of the risk identification is crucial. Risks that are not identified here are missing in the subsequent risk analysis and valuation and thus also in the risk treatment. There are several approaches to methodological risk identification, two of which are presented: the predominantly impact-based event-based approach and the cause-based approach based on values, threats and vulnerabilities. In order for the implementation of risk identification to be successful in practice, various prerequisites must be fulfilled. The decisive factor is that the top management performs its leadership role effectively and effectively. The key challenge is to keep the scope of risk identification manageable. For this purpose, the procedures of focusing and coarsening have proven themselves in practice. Finally, through the process of continuous improvement, an initially crude but unambiguous image of information security risks can be refined step by step and adapted to current requirements and threats.

Keywords: risk-analysis, data protection services, security threats.

1. Introduction

It is undisputed that adequate and effective protection of the confidentiality, integrity and availability of information about business processes, support processes, employees, customers, suppliers, etc. has a great importance to all organizations. It does not matter in what form the information is available or tangible: it can be printed or written on paper, stored electronically, sent by post or e-mail, transmitted by electronic means, shown on photos, in videos or films, and so on.

If information gets into unauthorized hands, it can have very far-reaching consequences for the business, such as reputational damage, loss of competitive advantage, loss of technology leadership, lawsuits and penalties, breach of contractual obligations in service level agreements, etc., all the way to complete business cessation.

This raises the question of how information can best be adequately and effectively protected. First of all, it has to be said that this is not an IT problem and certainly not a matter that can be restricted to the IT department, as it completely shuts out those responsible for business processes and support processes as well as the risk owners. The information security risks to which the organization is exposed must therefore be comprehensively and sufficiently identified throughout

[*] Corresponding author
E-mail addresses: simsim58@mail.ru (S.Zh. Simavoryan)

the organization. Only then they can be analyzed in terms of their size and evaluated according to their importance to the organization.

If an organization has poorly identified its information security risks, it has a poor foundation for choosing appropriate information security measures. As a result, the proposed information security risk treatment may be ineffective or inefficient, and thus inappropriately expensive.

It is the aim of this article to present the identification of information security risks from a methodological point of view and to provide guidance on how to do so in practice.

2. Discussion

ISO 31000: 2009 describes a risk management process. Its subprocesses have the following content:

– Communication and consulting: supports defining and adapting the context as well as the continuous improvement of the other sub-processes during all phases of the risk management process.

– Defining the context: Defines the objectives of the organization for the implementation of the risk management process, determines the external and internal issues as well as the needs and expectations of external and internal interested parties

– Risk identification: Identifies the information security risks associated with the loss of confidentiality, integrity and availability of information within the scope of the Information Security Management System (ISMS) and identifies the risk owners.

– Risk analysis: estimates the possible consequences of the identified risks, estimates the realistic probabilities of occurrence of the identified risks and determines the risk levels.

– Risk Assessment: compares the results of the risk analysis with defined risk criteria and prioritizes the risks analyzed for the risk treatment.

– Risk treatment: selects one or more appropriate risk treatment options, taking into account the results of the risk assessment, and sets out all measures necessary to implement the chosen risk treatment option (s).

– Monitoring and review: identifies changes in the external and internal issues, the needs and expectations of external and internal interested parties, scope and risk criteria; provides further information to improve risk identification, analysis and evaluation; analyzes and gains insights from events, changes, trends, successes and mistakes; identifies emerging risks; recognizes the effectiveness and efficiency of the entire risk management process.

Let's describe the process of preparation for risk identification according to Hans-Peter Königs, 2013; Decker, Karsten M., 2017:

1. Setting the context

First, the context needs to be specified. This must include all topics relevant to the purpose of the organization, the interested parties relevant to the ISMS and their information security requirements be determined. If these considerations are made too narrowly or too superficially, essential elements are disregarded and, as a consequence, risk identification will inevitably be incomplete.

1.1. Defining the external context

The external context encompasses all relevant topics, interested parties and their requirements outside the sphere of influence of the organization. Examples that apply to organizations of all kinds include legislators and legislators, suppliers, contractors, competitors, and customers.

1.2. Defining the internal context

The internal context encompasses all relevant topics, interested parties and their requirements within the sphere of influence of the organization. Examples that apply to organizations of all kinds include goals, strategies and policies for their achievement, structure and leadership, including roles and responsibilities, employees, processes and procedures, and skills in the form of resources and knowledge (capital, time, persons, Processes, systems, technologies).

2. Determining the scope

On the basis of the considerations described above, it is necessary to determine exactly where the risk management process should apply and where not. To do this the limits and applicability of the ISMS are determined. That concerns the:

- functions of the organization (products and services);
- processes of organization;
- areas of the organization;
- the interfaces and dependencies between the activities carried out by the organization itself and activities carried out by other organizations are determined.

The scope of the risk management process may alter from the scope of the ISMS. This is the case, for example, when an external organization performs or carries out a function, process or activity completely or in part. This organization is outside the scope of the ISMS, although the outsourced function, outsourced process or outsourced activity is within the scope of the ISMS scope. However, as the associated responsibilities remain with the organization, the risks associated with the spin-off must be part of the risk management process.

3. Risk criteria

The description of the possible consequences of security events for the organization's business activities regarding the confidentiality, integrity and availability of information may in principle vary greatly between different persons and when repeating the risk identification process. In order to meet the requirements of consistency, comparability and reproducibility of the results of this process these descriptions must be structured and standardized. This is done with the help of follow-up criteria, which must be specified in detail and with sufficient accuracy before the risk identification process begins.

Some risk impacts are shown in Table 1.

The follow-up criteria are of key importance to the risk analysis process, which follows the risk identification process.

Table 1. Risk consequences

Consequences for confidentiality	Consequences for integrity	Consequences for availability
Violation of the privacy of internal or external users	Incorrect delivery due to contradictory data	Service degradation of services
Loss of competitive advantages	Impossibility to produce a correct annual statement	Unavailability of services
Loss of technology leadership	Inability to fulfill legal obligations	Business interruption

4. Risk identification

The next stage is risk identification. It is the process of finding, recognizing and describing risks. Risk is defined as the effect of uncertainty on goals (ISO 31000:2009). The goal of risk identification is to create a comprehensive list of risks based on those events that cause, enhance, prevent, mitigate, accelerate or delay the achievement of goals.

The risk identification process must be based on sufficiently detailed methods and tools so that repeated risk identifications lead to consistent, comparable and reproducible results.

Repeated applications of the risk identification process can help to identify problems with the chosen methods and tools.

Regardless of the methods and tools have been chosen, the risk identification process must ensure that:

- all risks are considered with the required level of detail;
- the results are consistent and reproducible, so third parties can understand them;
- the results are the same when different people identify the risks in the same context;
- the results of repeated risk identifications are comparable.

Regardless of the chosen risk identification approach, the starting points are the information security objectives, the context of risk identification and their scope of application.

There are two approaches, which are commonly used to identify risks:

- an event-based approach;
- an approach based on the identification of values, threats and vulnerabilities.

Both approaches are consistent with the principles and general guidelines for the ISO assessment of ISO 31000: 2009.

Other approaches can be used, but are only recommended if they can ensure the requirements mentioned above. If ISMS is the target that meets the requirements of ISO/IEC 27001:2013, ensuring these requirements are essential. Let's consider both approaches in more detail

a) The event-based approach

The event-based approach identifies risks by looking at events and their consequences. Considered events may have happened in the past or may be expected for the future. In the first case they can include historical data, in the second case they can be based on theoretical analyzes, expert opinions and expert opinions as well as needs of interested parties.

First, by considering the questions "Who?", "What?", "Where?", "When?" and “Why?" possible events are described. To support the determination of events, in practice event catalogs are used. For example, the Basel Committee on Banking Supervision drew up a detailed catalog for the banking sector (Basel, 2006).

It identifies the root causes of these events to gain a deeper understanding of the risks and to gain insight into the underlying threats and vulnerabilities.

Finally, the possible consequences are described for all events. Consequences that can not be attributed to the goals of the organization do not add to the risks and can therefore be ignored. However, if such consequences are perceived as actually contributing to risks, this indicates that there are omissions in the list of goals of the organization that should be corrected.

The advantage of this predominantly cost-oriented approach is that its use is associated with relatively little effort. This makes it suitable for creating a first, rough picture of information security risks. It can be argued that such a focus of risk identification on the critical risks is supported.

The disadvantage is that existing threats and vulnerabilities as possible causes of the events are not necessarily determined systematically. This complicates the goal-oriented selection of measures in the subsequent risk treatment process. Another disadvantage is that risks can be overlooked.

b) The value, threat and vulnerability based approach

This approach identifies risks by looking at values, threats, vulnerabilities, and related consequences. These consequences arise when threats exploit vulnerabilities in a value or group of such assets and thus cause harm to an organization.

A value is anything that is valuable to an organization and therefore needs protection. Two types of values can be distinguished: primary values and supporting values.

The primary values are made up of business processes and activities, as well as information that is central to the organization's purpose. These are the values that must be considered first in risk identification.

The supporting values can be classified in hardware, software, network, personnel, location and organization. They may be considered containers in a broader sense to process, store, archive, or otherwise process or handle the primary values. Supporting values typically have vulnerabilities that can be exploited by threats designed to harm the primary values.

For each value, should be named a person who is responsible for the handling of the asset as well as its maintenance and safety. This person is often the most suitable one to estimate the value.

A threat is one possible cause of an incident that can cause harm to a system or organization.

Threats can exploit the vulnerabilities of one or more values. They can be based on natural phenomena, accidental, accidental or intentional and therefore conscious and deliberate origin.

Threats can be classified by type. ISO/IEC 27005: 2011 suggests e.g. the following classification:

- physical damage;
- natural events;
- loss of utilities;
- disturbance due to radiation;
- compromising information;
- technical failures;

- unauthorized actions;
- compromise tasks.

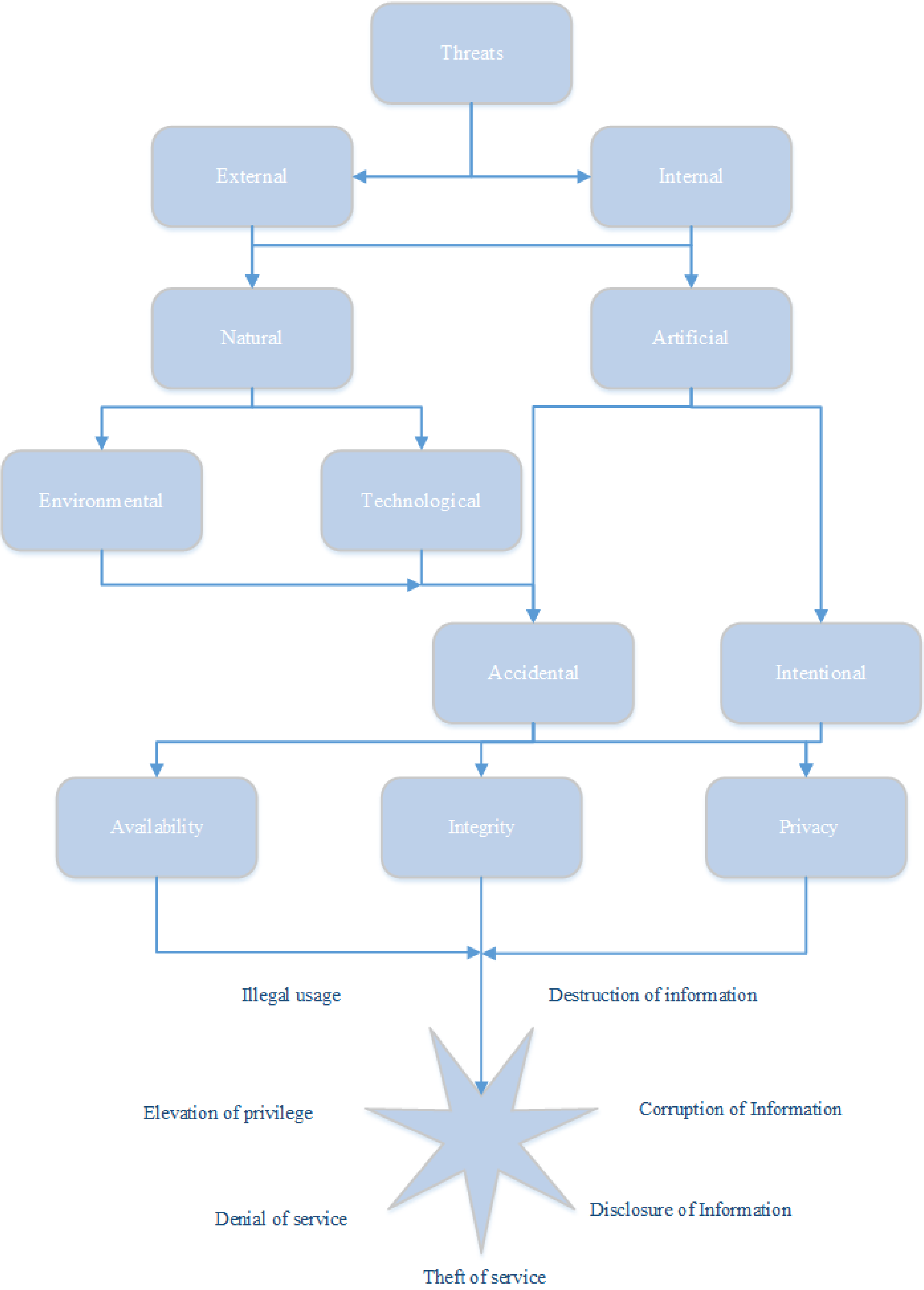

Fig. 1. Multidimensional model of classification of Threats

On another hand this classification can be sufficient for a stable environment (a small organization) where security threats are relatively stable, but in an ever-changing environment, organizations do not protect themselves from insider threats (Geric, Hutinski Z, 2007). In fact, organizations are subject to several threats that affect their reputation, and it is important that they identify all characteristics of threats in order to mitigate their risks. Classification allows an organization to know the threats that affect their assets, and the areas in which each threat can affect and therefore protect their assets in advance. In addition, it helps managers create information systems of their organizations with fewer vulnerabilities. In addition to this, the main problems can be identified in the work of existing threats. In fact, existing classifications do not support the principles of classification (Lindqvist, Jonsson, 1997; Gordon, Lawrence et al, 2005; Tang et al, 2012). At this point, the usual solution is to combine different classifications and create a hybrid. Because of the above results, we propose a hybrid model of classification of threats to the security of the information system, which we called the multidimensional model of classification of threats, intending to respect all principles of threat classification. The main idea of our model is to combine the criteria of threat classification and show their potential impact. The model is shown on the fig. 1.

When determining threats, this classification scheme can ensure that important threats are not forgotten. According to Simavoryan, 2017 malicious actions can be searched by automated means using specialized software. To do this, you need to build a specialized database. The structure of such a database was developed by the authors on the basis of FSTEC, 2015 is shown in fig. 2.

A vulnerability is a weakness of a value or measure that can be exploited by one or more threats.

Weaknesses are thus essential properties of values or measures. These properties do not have to be exclusively negative. For example, the great agility of mobile devices of all kinds (Laptops, netbooks, tablets, smartphones, etc.). On the negative side, however, this agility makes these devices easier to exploit for threats such as theft, eavesdropping or remote espionage. The same applies to values such as removable media.

Analogously, in the case of measures, e.g. be called a weak access control. While these facilitate access to premises and access to systems or applications, on the negative side are the exploitability of threats such as theft or destruction of data media, documents or equipment, the unauthorized use of equipment, the falsification of data or the denial of activities to call.

It is consistent with the logic of the value, threat and vulnerability-based approach to risk identification that a vulnerability itself can not cause harm because a threat must exist to exploit this vulnerability. However, such vulnerabilities need to be identified and monitored because changes in the internal or external environment can re-emerge appropriate threats.

When the vulnerability of a value is exploited by a threat, an immediate impact on information security is first caused. For example, confidential information is disclosed to unauthorized persons, falsified documents are circulated or an information system fails. Such events may eventually trigger consequences for the organization's operations. In the examples mentioned, these may be e.g. breach of contractual agreements or applicable laws, performance degradation or unavailability of services or a complete interruption of operations.

The distinction between immediate information security implications and consequences for the organization's business causes loss of confidentiality, integrity or availability of information. The effects and consequences of each event where a threat exploits a vulnerability of a value must be identified and described with sufficient accuracy.

Vulnerabilities can be classified as threats by type. ISO/IEC 27005: 2011 classify them according to supporting values:

- hardware;
- software;
- network;
- staff;
- location;
- organization.

The most important advantage is that this cause-based approach allows the consequences of events to be systematically linked to the weaknesses of values and measures. This creates the prerequisites for the measures to be selected in a very specific and targeted manner in the subsequent risk treatment process, and for the required scope of implementation and depth to be precisely determined. Thus, both the effectiveness and the efficiency of the ISMS is ensured. Also, this approach can better ensure that all relevant risks are taken into account.

The disadvantage is the potentially great effort for this approach. The identification of relevant values is not always easy. Each value can have one or more vulnerabilities, each of which can be exploited individually by one or more threats. That is why the number of events can increase very quickly in a combinatorial way.

5. Identification of the risk owner

For the process steps following the risk identification, it is important to identify a risk owner for each identified risk. These individuals are responsible for managing these risks, which can also be cross-process. In order to fulfill this responsibility, the necessary resources must be assigned to them by the process owners.

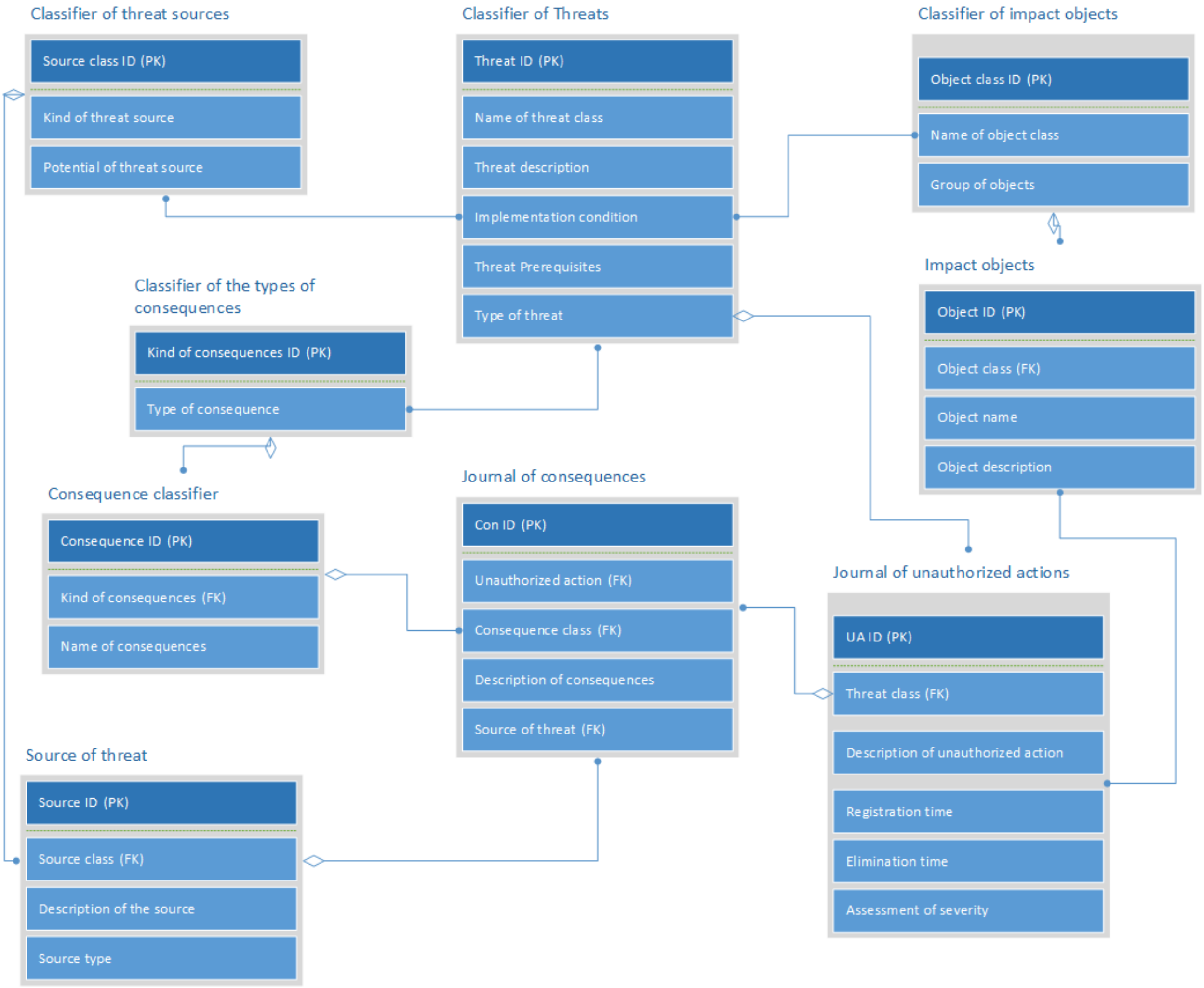

Fig. 2. Database logical model

3. Results

The importance of methodological risk identification for the effective management of information security risks is not recognized in most cases. However, it is essential for an effective risk management process. Without one that is tailored to the specific needs of the organization, the whole process has little value. Any risk that is not identified in this process step is ignored in the subsequent process steps. There are different approaches to risk identification whose respective strengths and weaknesses must be taken into account when defining the process.

In the practical implementation, the fulfillment of various conditions is crucial for the success. However, if risk identification is carried out with due diligence, there are at least two major benefits immediately. On the one hand, the prerequisites are created to prepare and manage not only the selection of measures of any kind in the subsequent processes of risk analysis, assessment and treatment, but in particular, also to determine their scope and depth, to the extent that they are responsible for the Organization is required. The cost-effectiveness of the measures implemented in this way can be (significantly) higher than simply relying on the frequently advertised good practices without further consideration and differentiation. On the other hand, sound risk identification also creates the prerequisite for a discussion with hardware and software suppliers on an equal footing. This can help to save unnecessary costs.

4. Acknowledgement

The reported study was funded by Russian Foundation for Basic Research (RFBR) according to the research project No. 16-01-00527.

References

Basel, 2006 – Basel Committee on Banking Supervision, International Convergence of Capital Measurement and Capital Standards; A Revised Framework, comprehensive Version, June 2006, Bank for International Settlements.

Decker, Karsten, 2017 – *Decker, Karsten M.* (2017). Informationssicherheit–ohne methodische Risikoidentifizierung ist alles Nichts." HMD Praxis der Wirtschaftsinformatik 54.1: 21-36.

FSTEC, 2015 – FSTEC of Russian Federation "Methodology for determining threats to information security in information systems", 2015.

Geric, Hutinski, 2007 – *Geric S, Hutinski Z.* (2007). Information system security threats classifications. Journal of Information and Organizational Sciences; P. 31-51.

Gordon, Lawrence A., et al, 2005 – *Gordon, Lawrence A. et al.* 2005 CSI/FBI computer crime and security survey. *Computer Security Journal* 21.3 (2005): 1.

Hans-Peter Königs, 2013 – *Hans-Peter Königs* (2013). IT-Risikomanagement mit System. Praxisorientiertes Management von Informationssicherheits- und IT Risiken. Springer Verlag, 4. Auflage.

ISO 31000:2009 – ISO 31000:2009, Risk management – Principles and guidelines.

ISO/IEC 27001:2013 – ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements.

ISO/IEC 27005:2011 – ISO/IEC 27005:2011, Information technology – Security techniques – Information security risk management.

Lindqvist, Jonsson, 1997 – *Lindqvist, Ulf, Erland Jonsson* (1997). How to systematically classify computer security intrusions." Security and Privacy, Proceedings., 1997. IEEE Symposium on. IEEE, 1997.

Simavoryan, 2017 – *Simon Zh. Simavoryan, Arsen R. Simonyan, Elena I. Ulitina, Rafik A. Simonyan, Elina A. Pilosyan, Nadezhda A. Kornienko.* (2017). Search Fuzzy Image of the Attacker Based on the Use of Automatic Classification Methods // *Modeling of Artificial Intelligence*, 4(1): 29-38.

Tang et al., 2012 – *Tang J, Wang D, Ming L, Li X.* (2012). A Scalable Architecture for Classifying Network Security Threats. Science and Technology on Information System Security Laboratory.