Mathematical methods for assessing information security risks

Alexsander Sobol and Viktor Kochyn
Center of Information technologies
Belarussian State University
Minsk, Belarus
Email: sobolam@bsu.by, kochyn@bsu.by

Natalia Grakova
Department of Intelligent Information Technologies
Belarusian State University of Informatics and Radioelectronics
Minsk, Belarus
Email: grakova@bsuir.by

***Abstract*—The article discusses international standards for assessing information security risks, as well as mathematical methods. The semantic model of information security risk assessment of the organization is described. For each element the calculation of the value is given.**

***Keywords*—risk analysis, information security, mathematical model**

I. Introduction

Nowadays, more and more organizations are exposed to cyberattacks. In order to reduce the impact of cyber attacks on the organization, it is necessary to assess information security risks. Although there are different approaches to assessing these risks, all methods require human involvement in any case.

The purpose of a risk assessment system is to establish an objective measurement of the level of risk that allows organizations to understand the business risks associated with critical information and assets, both qualitatively and quantitatively. Ultimately, risk assessment systems provide the tools necessary to make business decisions regarding investments in people, processes, and technology in order to reduce risk to an acceptable level.

This paper presents an overview of various current methodologies and models for information security risk assessment (ISRA). Particular attention is paid to game-theoretic and probabilistic-graphic methods and the construction of a semantic model of risk assessment, depending on the mathematical method used. The purpose of this article is to establish the rules of assessment, the objectives for the actors involved, the terminology used to describe risk, and the quantitative and qualification criteria [1]. In addition, the risk assessment methodology allows the comparison of risk degrees and defines the documentation to be collected and prepared based on the results of the assessment and follow-up.

II. Classic security risk assessment methodologies

To determine the necessary evaluation criteria, let's review the international standards related to risk assessment and use them to formulate the necessary criteria for assessing information security risks.

A. ISO 31000

ISO 31000 is a security risk assessment standard whose universal approach makes it applicable to a wide range of organizations and systems, regardless of their type or size [2].

The ISO 31000 process consists of several steps, as shown "Fig. 1".

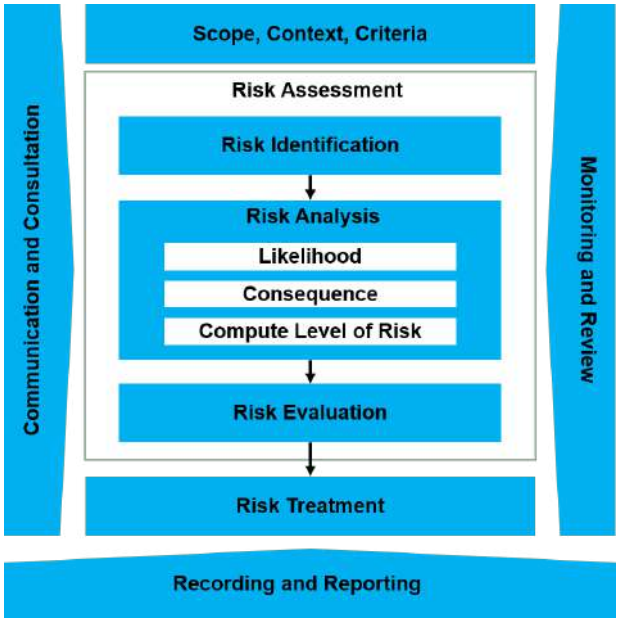

Figure 1. Risk management process.

Let's define each step:

- Establishing the context. This step identifies the internal and external contexts. The internal context defines the management, organizational structure, processes, roles and responsibilities, policies, project objectives, assets and other characteristics of the organization. The external context includes social, cultural, political, legal, regulatory, financial, technological, economic and natural aspects. They are used to build an understanding of the interests of stakeholders inside and outside the organization,

determine the purpose of the risk assessment, and identify risk criteria (what risks to consider and how to assess them).

- Risk Assessment. This step involves a complete process of risk identification, analysis, and assessment. Risk identification - defines sources of risk, areas of influence, risk events and their consequences. The main result of this part is a list of all possible risks. The next step is risk analysis. For each item of the list the corresponding probability of occurrence and potential consequences (impact) is defined. Risk analysis focuses on identifying risk sources, communicating with stakeholders to gather the information needed to make a decision, and evaluating risks against risk criteria. Risk analysis can be quantitative, semi-quantitative or qualitative in nature. During the assessment phase, risks are ranked for further processing.
- Risk treatment. This step involves selecting and implementing one or more options to change (mitigate) risks. ISO 31000 identifies a number of possible strategies that include deploying additional safety controls, shifting responsibility for risk mitigation to other organizations, changing the specifics of the organization, and accepting risk as it is. Each step of the assessment should involve communication with stakeholders and subject matter experts. The approach is considered iterative and should be repeated periodically.

ISO 31000 offers a high-level description of the process. This level of precision allows it to be adopted for a large number of different systems/organizations. However, most of the process steps are not detailed and rely solely on stakeholder decision-making and peer review. This standard does not contain any explicit suggestions for possible automation of the decision-making process at each step, nor does it define how to quantify risks. The standard assumes that the relevant relationships between systems and possible post-attack consequences must be taken into account in the risk assessment. However, the standard does not provide a clear procedure or algorithm to be followed.

B. ISO 27005

ISO 27005 [1] belongs to the ISO 27000 family of standards and is an extended risk management process that is specifically adapted to information security requirements. The standard itself contains a description of the ISRA process, which is still applicable in information security and infrastructure security. The ISO 27005 process itself is shown in “Fig. 2”. The first step of the analysis is to establish the context. It identifies the following objects of analysis:

- Definition of impact criteria, such as financial, human or reputational losses. Impact criteria may vary

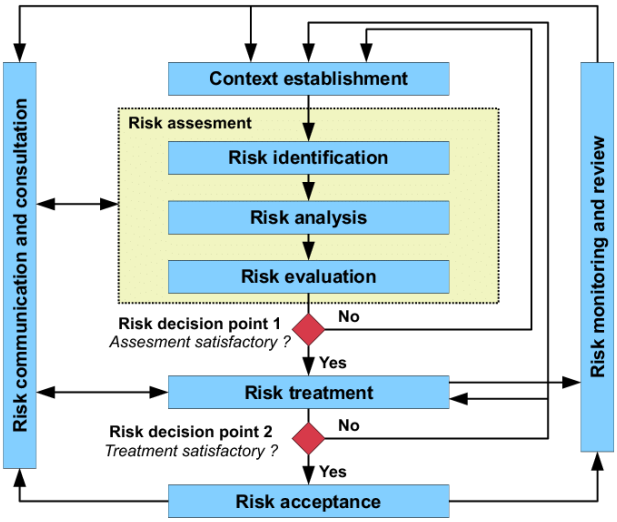

Figure 2. Information security risk management process.

depending on the specifics of the protected system and are defined as real parameters describing the level of damage caused. The usual range of impact criteria is from 0 to 5, where the scale is determined by the security personnel conducting the analysis.
- Defining the scope, which is the organization’s overall view of the assets to be protected. Assets can be both tangible (buildings, computers or personnel) and intangible (data, functions).
- If the assessment is planned as part of some standard process within the organization, it is important to identify the unit responsible for carrying it out.

The next step in the analysis is the risk assessment, which has three parts.

- Risk identification examines what incidents are likely to occur and which ones will result in a loss. This includes both those incidents that are under the organization’s control and those that are based on external influences. Identifying possible threats includes listing critical system assets (which can be tangible or intangible); identifying major vulnerabilities and how they are exploited; creating a set of possible ”controls,” that is, means to mitigate or prevent an attack; identifying the various types of consequences of an attack, such as money, reputation, human loss, or any other relevant criteria.
- Risk analysis analyzes threats in terms of their probability of occurrence and numerically evaluates them against a set of criteria defined in the previous step. Risk analysis can be either qualitative or quantitative, depending on the type of criterion under consideration. For example, some criteria can be defined as an exact numerical value or range of values (financial losses), some criteria can be

characterized using descriptive scales (e.g., ”low,” ”medium,” ”high”). Probability assessment looks at how often a particular threat is likely to occur and how easily the vulnerabilities associated with it can be exploited; it is conducted by experts in the field using an event log.

- The risk assessment re-examines the list of threats given the assessed criteria and probabilities. Based on the expert assessment, risks are ranked and a list of priority threats is compiled.

The next step in the process is risk treatment, described as a complex step consisting of four possible options: risk modification, risk retention, risk avoidance, and risk sharing. These options are not mutually exclusive; a combination of strategies is possible. Risk modification involves choosing (new) controls to reduce risk. This decision must be made in the light of available resources. The remaining strategies identify different measures to transfer responsibility for handling risk to another strategy or to accept low-impact risks as they are.

The final step in the analysis is risk acceptance, where all identified risks are reassessed against the chosen treatment strategies and accepted or not based on residuals (estimated exposure levels after treatment). ISO 27005 provides a high-level risk assessment algorithm and defines the vocabulary and basic elements of the ISRA process. It is more detailed than ISO 31000, defining the exact types of entities to be analyzed during the contextualization phase. However, it does not define a meaningful approach for quantifying risks - the standard relies heavily on expert judgment at each stage of analysis and provides no suggestions or guidance for detailed formalization of attacks or any means for automating decision-making during risk identification and risk analysis. identification and risk analysis.

III. ISRA CRITERIA

Based on the international standards considered, the following features can be identified, which are important for the assumed mathematical model of ISRA. The described criteria are considered as necessary conditions, for simplicity of simplification of experts in the field of ISRA.

1. General description of the system. The approach must be applicable to any type of system and must interact with heterogeneous entities, which can be adjusted according to the information security expert’s area of interest.

2. General descriptions of attacks. The approach should allow the description of arbitrary threat scenarios and attack types. Attacks can be interdependent, and the scenario can include several stages of development.

3. Versatility of protection description. The approach must be capable of implementing a variety of information security controls and information protection tools.

This list is not necessarily sufficient for a quality ISRA. However, meeting these requirements will allow the model to be technically applied to ISRA problems. Many additional constraints and requirements can be added, such as the need to explicitly model sequential countermeasures, deflect simultaneous attacks, and consider different types of exposure. Fulfilling these criteria will require a certain level of simplification compared to models that consider specific attacks on a particular system. In addition to defining the modeling criteria, it is necessary to describe the specific application of the model being developed (i.e., the group of end users and the qualifications required). The end users of the model are information security personnel and specialists who perform ISRA.

IV. ISRA MATHEMATICAL METHODS

The mathematical methods used for ISRA are diverse. They cover a wide range of methods, including formalized techniques [3], evolving into intermediate expert assessments with supporting formal structures (e.g., attack trees and correlation diagrams), [4] and converging to fully expert decision tree methods used to classify or quantify security levels.

A. Main Families of Models

The main methods of applied mathematics in the field of ISRA are: big data analysis and statistical learning, algorithms of operations research and statistical graph models. Let us consider them in more detail.

1. Data manning and statistical learning. These methods have been successfully applied in intrusion detection. The methods developed are usually formalized as anomaly detection problems, solved by methods such as principal component analysis [5], single-class support vector machines (SVMs) [6], or kernel density estimators [7]. The advantage of these methods is that there is no need to develop a detailed system model, since the training procedure aims to adapt the parametric model depending on the specifics. However, these algorithms are used for specific tasks with a narrow domain, and exploitation is performed at the system component level using special equipment (e.g., network analyzers, protocol scanners and malware detectors or botnets). Algorithms based on statistics depend on the training data and on the structure of the chosen algorithm, which significantly narrows the scope of their application. An exception in this case may be self-learning online models that can adjust to new data. Nevertheless, these methods still require the data to be presented in the standard format of generic descriptive information security ”trait-vectors”, which is a separate problem that needs to be solved. Another problem with statistical methods, especially the more complex examples (e.g., deep neural networks), is the poor interpretation of results and difficult error analysis/debugging.

2. Algorithms for information security problems based on operations research. They are usually developed for large-scale information security systems. These methods take as inputs a formal description of the system, a set of asset variables to be optimized (e.g., security control allocation), and one (potentially multiple) objective function. The target function must be optimized for the model variables. The adversary is usually represented explicitly as an entity, and its goals can be explicitly modeled using formalization by means of game theory or decision theory. Existing methodologies may vary depending on the asset and system variables modeled, but within operations research (and game theory in particular) provides a general concept that can be used to support decision making during ISRA in large-scale systems. In addition, the explicit definition of the target function simplifies the interpretation of the results.

3. A family of statistical graph models [8]. This method can be understood as a combination of statistical analysis and operations research algorithms. They are used in security tasks to identify failures of subsystems [9], as well as for cybersecurity [10]. In contrast to big data analysis models, statistical graph models have a preliminary design phase that aims to capture the specifics of the system being described. The models establish an explicit probabilistic relationship between the data observed during operation and the description of the system state (e.g., the failure of certain modules or the possible presence of an attack). Thus, graph models allow, for example, to derive a probabilistic distribution of system state variables depending on the observed data.

It should be noted that in recent years, the aforementioned distinction between the use of operations research methods and big data analysis has become increasingly flexible. One of the main reasons for this is related to the developing field of generative adversarial networks (GANs) [11]. GANs can be thought of as a combination of operations research methods and data mining. Some theoretical settings simulate a zero-sum game between a generator and a classifier [12], the intention being to teach the generator to produce objects that are indistinguishable from the ”real” training dataset. However, this does not explicitly aim to model the behavior between the attacker and the defender, nor does it address the problem of poor interpretation. In addition to the methods already discussed, there are a number of approaches to solve general information security problems, including general attack detection methods, as presented in [13].

B. Semantic assessment of information security risks

The semantic model of information security risk assessment can be represented as the following function:

$$R = f(V, T, I) \tag{1}$$

where: V — probability of threat occurrence; T — severity of consequences; I — cost of risk reduction.

This function takes as input the three components of the model and calculates the information security risk borne by the system or a component of the system. Appropriate functions can be used to calculate each component, which can be determined from experience and statistical data.

The function for calculating the probability of the threat is as follows:

$$V = V(P, C, E) \tag{2}$$

where: P — theoretical threat probability (this value from 0 to 1 depends on the formula we choose: Bayesian, Monte Carlo, etc.); C — the degree of possibility of the threat occurrence (this value from 0 to 10 can be obtained based on the vulnerabilities of information systems, which are evaluated according to the CVSS metric); E — the motivation of the attacker.

The motivation can be varied, for example financial, political, hacking, revenge, or sabotage. All of these motivations can take different forms and manifest themselves in different types of cyber attacks. To defend against cyber threats more effectively, it is necessary to understand the motivations of attackers and take them into account when developing an information security strategy. In general, it can be difficult to formalize an assessment of an attacker's motivation using mathematical methods, because motivations can be very diverse and are often social, political or psychological in nature. However, the use of machine learning algorithms and big data analysis can help automate the process of assessing the motivation of attackers. An attacker's motivation score can be expressed as a numerical value on a particular scale, such as 0 to 10, where 0 is no motivation and 10 is the maximum motivation. A numerical estimate of motivation can be derived from an analysis of various factors affecting the attacker, such as:

- the potential benefit of successfully executing the attack (e.g., financial gain, gaining a competitive advantage, revenge, etc.);
- complexity of the attack (e.g., skills, tools available to the attacker, etc);
- whether the attacker can be detected and punished (e.g., the probability that the attack will be detected and the attacker will be eliminated);
- value of the target to the attacker (e.g., value of sensitive data, company reputation, etc.).

itemize Based on the analysis of these factors, a motivation factor can be determined to represent the numerical value of the attacker's motivation. For example, a formula to estimate an attacker's motivation might look like this:

$$E = \frac{B * Diff * ValueTarg}{Detect} \tag{3}$$

where: B — the potential benefit of successfully executing the attack; $Diff$ — the difficulty of the attack;

$ValueTarg$ — the value of the target to the attacker; $Detect$ — the probability of identifying and punishing the attacker.

A function for calculating the severity of consequences could look as follows:

Calculation of consequence severity (T):

$$T = T(II, A, F) \tag{4}$$

where: II — is the importance of the information that may be stolen, lost, or damaged (importance); A — likelihood of the consequence occurring (likelihood); F — the degree of impact on business processes (impact factor).

Quantifying the importance of information (II) can be done by using mathematical modeling and data analysis techniques. One such method is Business Impact Analysis (BIA).

BIA is a process that is used to assess the importance of information to business processes and to determine the potential consequences of its loss or breach of confidentiality. The evaluation of information importance in BIA is based on two main criteria: business importance and confidentiality.

Different levels of importance can be defined for each criterion, which can be expressed as numbers from 1 to 10. For example, business importance levels may include the following values:

- critically important: 9-10;
- very important: 7-8;
- medium importance: 4-6;
- minor: 1-3.

Similar levels can be defined for the privacy criterion.

Further, for each business process, the importance of each element of information related to the process can be defined. The importance of each element can be expressed by a number from 1 to 10, where 1 is low importance and 10 is high importance.

The final importance of each information can be determined by multiplying the importance of each element by the importance of the business process and the importance of confidentiality. The probability of consequences refers to the likelihood that a particular event or threat will result in undesirable consequences for the system or organization.

Various methods can be used to estimate the probability of consequences, including statistics, expert judgment, and modeling. A quantitative estimate of probability can be expressed as a number, usually on an interval between 0 and 1, where 0 means that probability is impossible and 1 means that probability is absolutely certain.

The degree of impact on business processes can be estimated using the following formula:

$$Impract = \sum_{i=1}^{n} (Asset_i * \frac{Lost_i}{Revenue}) \tag{5}$$

where n is the number of assets, $Asset_i$ is the value of i-th asset, $Loss_i$ is the potential loss when consequences for i-th asset occur, $Revenue$ is the company's annual income. Thus, the value of $Impact$ shows what part of the annual income of the company can be lost as a result of the possible consequences for its assets. The higher the value of $Impact$, the more serious are the consequences for business processes.

The following formula can be used to quantify the probability of a consequence occurring:

$$P = Mot * U * II \tag{6}$$

where Mot is the probability of the attacker's motivation; U is the probability of system vulnerability, and II is the importance of the information.

Each of the components of the formula can be evaluated on an interval from 0 to 1, where 0 means that the probability is impossible and 1 means that the probability is absolutely certain.

Estimating the probability of an attacker's motivation can be done through expert judgment, historical data analysis, or research. An assessment of the likelihood of system vulnerability can be based on statistical data analysis, vulnerability studies, or expert assessments. An assessment of the importance of information can be based on business process analysis, expert evaluations, or data classification. Each of these components can be evaluated based on an analysis of the importance of the data stored in the system, the likelihood of consequences occurring, and the extent to which those consequences affect business processes.

Each of these components can be estimated based on an analysis of the importance of the data stored in the system, the likelihood of the consequences and the impact of these consequences on business processes.

Calculation of risk reduction cost (I):

$$I = I(Cost, RR) \tag{7}$$

where: $Cost$ — the cost of taking risk reduction measures (cost); RR — the probability of risk reduction when taking action (effectiveness).

The cost of taking risk reduction measures can be estimated using the following formula:

$$Cost = \sum_{i=1}^{n} (Asset_i * \frac{Lost_i * Risk_i}{SecurityBudget}) \tag{8}$$

where n is the number of assets, $Asset_i$ is the value of ith asset, $Risk_i$ is the probability of threat occurrence for ith asset, $Loss_i$ is the potential damage when consequences occur for ith asset, $SecurityBudget$ is the budget for information security.

Thus, the value of $Cost$ shows how much money needs to be spent on risk mitigation measures for all company assets. Estimating the cost helps to decide what risk

mitigation measures should be implemented based on the information security budget.

The probability of reducing risk by taking action can be estimated using the following formula:

The cost of taking risk reduction measures can be estimated using the following formula:

$$RR = \frac{Risk_{before} - Risk_{after}}{Risk_{before}} * 100 \qquad (9)$$

where $Risk_{before}$ is the probability of threat occurrence before taking measures, $Risk_{after}$ is the probability of threat occurrence after taking measures.

Thus, the value of $RiskReduction$ shows by how much the probability of threat occurrence will decrease when measures to reduce risk are taken. This assessment helps to determine the effectiveness of the measures taken to reduce the risk and decide whether additional measures are needed.

References

Information security risk assessment is an important element of information resource management in any organization, since information security is directly related to its value, confidentiality and integrity. There are many methods of risk assessment, and each of them has its own advantages and disadvantages.

One approach to risk assessment is the use of mathematical methods and formulas. They allow you to assess the likelihood of the threat, the motivation of the attacker, the importance of the information, the impact on business processes, the degree of impact of the consequences and other factors that may affect the security of information.

By using machine learning algorithms, it is possible to automate the risk assessment process and improve the accuracy of the assessment. In this case, machine learning models can be used to analyze large amounts of data, search for hidden patterns, determine parameters and identify dependencies between them. Machine learning can also be used to create predictive models and scenario analyses.

However, despite all the advantages, mathematical methods and machine learning models are not a universal solution to the problem of information security. It is necessary to take into account that each model has its own limitations and shortcomings, and cannot take into account all possible factors that may affect information security.

Therefore, a comprehensive approach to risk assessment is necessary, which includes the use of several assessment methods, analysis of results, regular updating and improvement of models based on new data and improvement of information security practices.

In general, mathematical methods and machine learning models are an important tool for information security risk assessment, but only in combination with other information security methods and practices, such as physical security, access management, personnel training, etc.

References

[1] ISO/IEC 2018. Technical report

[2] A. Dali and C. Lajtha. Iso 31000 risk management: “the gold standard”. EDPACS, 45(5):1–8, May 2012.

[3] M. Brown, B. An, C. Kiekintveld, F. Ordonez and M. Tambe. Multi-objective optimization for security games. In Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems. *International Foundation for Autonomous Agents and Multiagent Systems*, Richland, SC, 2012, Vol. 2, AAMAS ’12, pp. 863–870.

[4] B. Schneier. Attack Trees — Modeling security threats. *Dr. Dobb’s Journal*, 1999.

[5] T. Morita, S. Yogo, M. Koike, T. Hamaguchi, S. Jung, I. Koshijima, and Y. Hashimoto. Detection of cyber-attacks with zone dividing and PCA. Procedia Computer Science, 22:727 – 736, 2013. 17th International Conference in Knowledge Based and Intelligent Information and Engineering Systems — KES2013.

[6] Y. Wang, J. Wong and A. Miner. Anomaly intrusion detection using one class SVM. In Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop, 2004., pp. 358 – 364.

[7] Y. Cao, H. He, H. Man and X. Shen. Integration of Self-Organizing Map (SOM) and Kernel Density Estimation (KDE) for network intrusion detection. Edward M. Carapezza (ed.), Unmanned/Unattended Sensors and Sensor Networks VI, International Society for Optics and Photonics, SPIE, 2009, vol. 7480, pp. 146–157.

[8] C. Borgelt and R. Kruse Graphical Models: Methods for Data Analysis and Mining. *John Wiley and Sons*, Inc., USA, 01 2002.

[9] A. Abdollahi, K. R. Pattipati, A. Kodali, S. Singh, S. Zhang and P. B. Luh. Probabilistic Graphical Models for Fault Diagnosis in Complex Systems, Springer International Publishing, Cham, 2016, pp. 109–139.

[10] P. Xie, J. Li, X. Ou, P. Liu and R. Levy. Using Bayesian networks for cyber security analysis. In 2010 IEEE/IFIP International Conference on Dependable Systems Networks (DSN), 2010, pp. 211–220.

[11] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville and Y. Bengio. Generative adversarial networks. Commun. ACM, 63(11):139–144, 2020.

[12] F. A. Oliehoek, R. Savani, J. Gallego-Posada, E. van der Pol, E. D. de Jong and R. Gross. GANGs: Generative adversarial network games, 2017.

[13] F. Pasqualetti, F. Dörfler and F. Bullo. Attack detection and identification in cyberphysical systems. *IEEE Transactions on Automatic Control*, 58(11):2715–2729, Nov 2013.

Математические методы анализа риска информационной безопасности

Соболь А. М., Кочин В. П., Гракова Н. В.

В статье рассматриваются международные стандарты для оценки рисков информационной безопасности, а также математические методы. Описана семантическая модель оценки рисков информационной безопасности организации. Для каждого элемента приведен расчет значения.

Received 01.04.2023