Visualization of a Spatio-Temportal Threat Model

A. V. Manzhosov(✉) and I. P. Bolodurina

Orenburg State University, 13 Victory Avenue, Orenburg 460018, Russian Federation
a.v.manzhosov@gmail.com

Abstract. Data visualization in the field of information security (IS) is becoming an urgent task. The more informative the visual display for the analyst, the faster and better he will be able to get the result. The visualization method is described in the article, which allows to reduce the time needed for determination the actual IS threats when processing the IS threat model. In the classic way of displaying, threat models are a list or a table of several tens of printed pages. To process such a volume of data, information security analysts need to spend a lot of time. It remains likely that the analyst will lose sight of important data. The article proposes a method for visualizing the spatio-temporal model of IS threats in three-dimensional and two-dimensional form. When visualizing a threat model, a surface with axes is used: time, risk, information asset. The proposed visualization of the IS threat model allows the analyst to identify current threats in less time. Scope - management of information security. The result of this work is a way to visualize the IS threat model, taking into account the spatio-temporal factor.

Keywords: Information security · Spatio-temporal model · Visualization

1 Introduction

The analysis of modern methods for determining current threats has shown that modern models of IS threats are built in the form of lists or tables. The article proposes a method for visualizing the spatio-temporal model of IS threats. Using the space and time factor when visualizing the IS threat model will allow to allocate resources aimed at protecting information in order to protect those information assets (IA) that are most vulnerable at a particular point in time and space. This will save some IAs from the excess resources for protection, while others protect properly. Space should be understood as all IA enterprises distributed physically or logically. The method of visualization of the spatio-temporal model of information security threats proposed in the article will reduce the time spent working with the security model of information security analytics. The following tasks are supposed to be solved: conducting an analytical review of studies on the methods of visualizing IS information, setting tasks for constructing a visualization of the spatio-temporal model of IS threats, developing An approach to visualizing the spatio-temporal model of IS threats, identifying the disadvantages of the proposed method for visualizing the spatio-temporal model of IS threats.

A. A. Radionov and V. R. Gasiyarov (Eds.): RusAutoConf 2020, LNEE 729, pp. 533–542, 2021.
https://doi.org/10.1007/978-3-030-71119-1_52

2 Research Overview on Information Security Data Visualization Techniques

In the article [1], the authors propose to analyze security metrics and visualization models in order to obtain an opinion on the best option among them, to help analysts in monitoring security and choosing IS countermeasures against a specific attack scenario. P. Hall, C. Heath and L. Coles-Kemp in a publication [2] investigate the problem of the lack of information of modern methods of data visualization in the field of information security. Researchers suggest turning to other areas of knowledge to find the best way to visualize data to increase information content and reduce the cognitive load on a personArticle [3] describes the current state of scientific knowledge related to data visualization. Researchers point out that visualization must meet people's needs. It is necessary to study the interaction of a person with a computer and visual methods that correspond to human cognitive laws. Modern studies of visual analysis of spatio-temporal data are still very preliminary, and theory, methods and technical systems in this area have not yet been formed.

G. Markowsky in the publication of the 2013 conference [4] supports the idea that the processing of large amounts of data by IS analysts is difficult and lengthy without auxiliary tools. The author cites as an example a selection of tools to present information flows in the form of graphs, charts, graphs, so that information security analysts use them in everyday tasks. Raffael Marty, author of Applied Security Visualization [5], considers data visualization as a solution to the problem of fast analytics of large amounts of data. Big data technologies have facilitated the collection and storage, but their processing and decision making is still a problem. When data is visualized by a professional designer, it is beautiful, but not informative. A security analyst makes a more informative visualization, but difficult to understand. Raffael Marty is committed to maximizing inks for data of particular importance and minimizing color for data of less importance. Other researchers propose to solve the problem of long analytics of large volumes of information security using machine learning [6]. Machine learning reduces the response time to an IS incident by eliminating false alarms from warning systems. An article by Trent S. and others [7] proposes to study the behavioral models of malicious software within the corporate network by reducing the amount of information that is being processed by IS and visualizing it. An understanding of the behavioral patterns of malicious software will allow to find differences from other legitimate enterprise traffic quickly. This method is proposed to be implemented using PCAP and EventPad. The development team proposes the use of an interactive security analysis panel, which varies depending on the system requirements for security and the vector attack space [8]. Such an interactive system can serve as a visualization tool for information security analysts in ordinary enterprise systems and cyberphysical systems. The developers of the user behavior map [9] use the time and space factor when analyzing user behavior from the point of view of information security. The actions of users on the network are examined and anomalous behavior is determined due to the geography of user requests. An interesting approach is the 2D and 3D visualization of information security events of the main Internet component - the root DNS [10]. Due to the enormous amount of information transmitted, it is necessary to make calculations in real time to form a visual image. The image of large volumes of data is implemented using rays and clouds of events. The developers of

the data preprocessing algorithm use the visualization of information security events on a geographical map to track them in real time [11]. The visual-interactive environment differs from analogues in that it uses a geographical map. An article by Robert Gove and Lauren Deason [12] is devoted to the development of a method for visualizing the text information of an event log in a system where malicious software is present. An attack visualization is built based on duplicate DNS queries, excluding legitimate repetitive traffic. The developers presented a tool for visualizing firewall rules [13], which allows analyzing the current conditions and displaying them in the form of images. This will reduce the time it takes to manually check all the rules and their compliance with the requirements. Article [14] describes the concept of a spatio-temporal data mining model using machine learning to find targets that are subjected to a sequential attack, and to determine whether an individual participant can potentially conduct attacks on a global scale. An article by T. Ahola, K. Virrantaus, and others offers a consideration of the spatio-temporal population model, which is constructed by location and population density [15]. According to the authors, the spatio-temporal model should be used for visual analytics in the risk assessment process for making urgent decisions in emergency situations.

IS analysts using data visualization accelerate the task of identifying actual threats. This is achieved by filtering out the non-informative part of the data that prevents the analyst from making choices faster and more accurately. The publications reviewed indicate that the direction of data visualization in the field of information security is widespread and is constantly being improved. This is evidenced by the fact that the annual SYMPOSIUM ON VISUALIZATION FOR CYBER SECURITY (VIZSEC) is devoted to this area [16]. It is worth noting that researchers are more interested in data visualization for monitoring and analysis of the current state of security systems. The problem of visualization of the IS threat model was not covered by researchers. The IS threat model is a description of the existing IS threats, their relevance, their feasibility and consequences. Threats can be caused by various sources, with different probability of implementation, which depends on the presence of favorable conditions for exploiting vulnerabilities associated with these threats. Since these conditions are constantly changing, IS analysts need to, at some intervals, usually every six months or a year, review current threats to IS. The result is a long-term IS policy of the entire organization, investment in tools to protect against the most relevant IS threats. The IS risk management manual describes a process model that reflects a constant cycle of reviewing current IS threats and building a long-term protection strategy [8, 17]. Constantly reviewing IS risks is a long and time-consuming process, which includes building a model of IS threats. Its complexity is associated with a large amount of processed information. The IS threat model in the classic version is reflected in the form of a list or a table of several tens of pages of printed text, and the analyst must make a lot of effort not to miss important details when working. In this regard, the urgent task is to optimize the processing of the IS threat model, increase the speed and quality of processing a large amount of data due to the visualization of information.

3 Statement of the Problem of Developing a Visualization of the Spatio-Temporal Model of Information Security Threats

The risk value R is taken as an indicator of the relevance of an IS threat. Risk is a combination of consequences arising from an undesirable event and the probability of an event occurring [18]. The probability P in this case is the probability of the formation of conditions under which there is a potential or real danger of IS violation as a result of data leakage through technical channels or unauthorized access to them. Damage D is the value of losses, expressed in real monetary terms, from the implementation of a threat to information security. The risk assessment of information security threats is presented in the form (1):

$$R = P \times D \tag{1}$$

IS risks depend on the probability of the threat, considered over a period of time; in some space; [19], which is all the IA of a company distributed physically or logically. In order to give a risk assessment (1), it is necessary to [18]:

- Establish the value of IA
- Identify potential threats and vulnerabilities
- Identify existing parry measures
- Set the probability of the implementation of threats
- Determine the consequences (damage from) the implementation of threats
- Calculate the risk of information security
- Build a spatio-temporal model of IS threats
- Conduct analytical work on the IS threat model using its visual representation
- Determine the level of unacceptable risk for IA
- Identify measures to counter unacceptable risk

Figure 1 shows a model of IS risk analysis using the visualization of a spatio-temporal threat model. This model in a concise form expresses the overall goal of the study, which consists in identifying and analyzing IS risks using the visualization of the spatio-temporal model of IS threats.

When processing a spatio-temporal model of information security threats, an information security analyst uses its visualization and control interface, which allows the use of visual and visual-analytical tools to assess information security risk. As a result of working with visualization, the IS analyst assesses the risk, and therefore a decision or action to change the current IS policy is taken, which will be reflected in the statistics of IS incidents.

Risk assessment is often carried out in two (or more) iterations. A high-level assessment is first conducted to identify potentially high risks that warrant further assessment. The next iteration may include further in-depth consideration of potentially high risks. In cases where the information received is insufficient to assess the risk, a more detailed analysis is carried out: on individual parts of the scope or using a different method. The choice of approach to risk assessment depending on the objectives and goals of risk assessment is carried out by the management of the organization concerned.

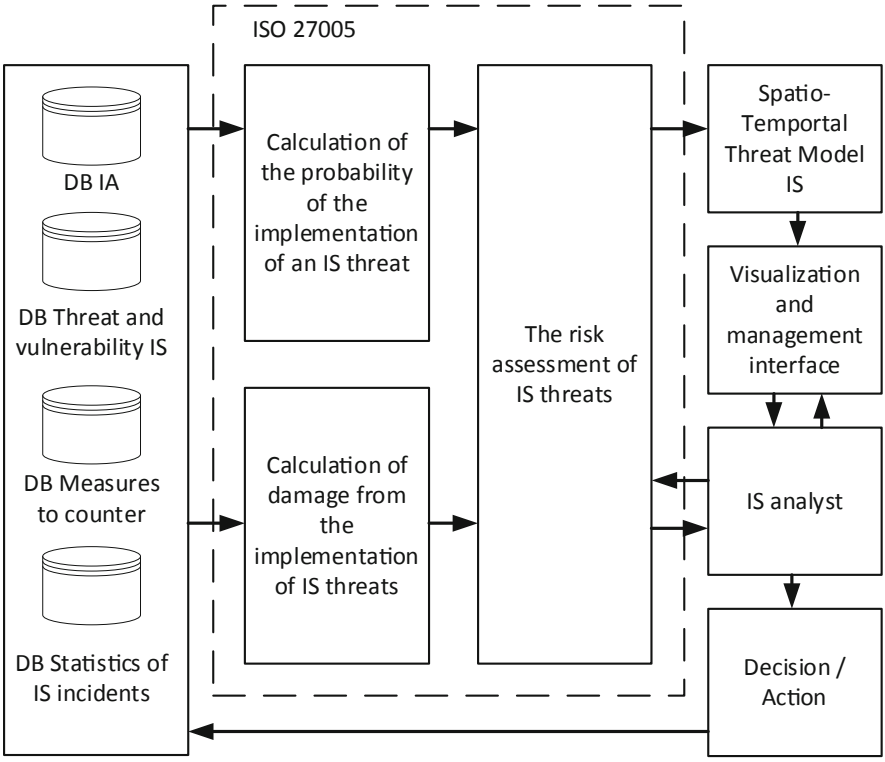

Fig. 1. IS risk analysis model using the visualization of a spatio-temporal threat model.

In the presented risk analysis model of information security, the analyst makes the final decision based on the visualization of the spatio-temporal threat model. Therefore, the more detailed and informative visualization will be used, the faster and better will be the result of the work of an information security analyst. Visualization is one of the most promising areas for increasing the efficiency of methods for analyzing and presenting multidimensional data in the field of information security.

4 An Approach to Visualization of the Spatio-Temporal Model of Information Security Threats

When analyzing IS risks, a necessary and sufficient subset of data is determined, which must be taken into account to obtain a reliable model of IS threats. When trying to visualize the IS threat model, a typical case that can become a problem is that the data set is too large. In such cases, visualization becomes difficult to perceive. To visualize the spatio-temporal threat model, it is necessary to highlight the data on the basis of which it is possible to construct visualization convenient for analysis [8]:

- Time $t \in [t_1;\ t_m]$
- IA space $s \in [s_1;\ s_n]$
- Amount of risk R

Processes or events prevail in space and develop over time, this spatio-temporal dynamic helps to understand their multidimensional interaction, identify seasonal patterns and observe causal relationships in the analysis of information security risks. Also, the use of the space and time factor on one visualization with the risk value allows us to build more compact visualizations. An example of three-dimensional visualization of the spatio-temporal model of IS threats is presented in "Fig. 2".

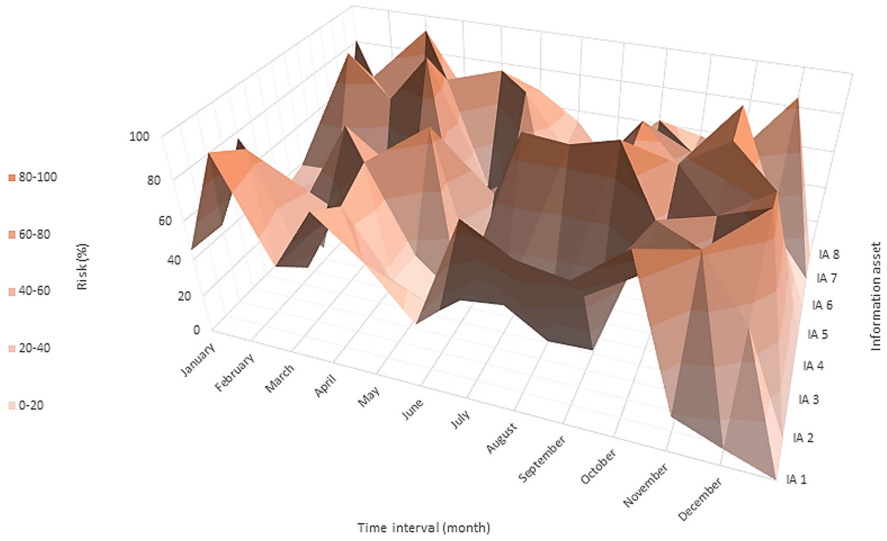

Fig. 2. An example of three-dimensional visualization of the spatio-temporal model of IS threats.

The three-dimensional spatio-temporal model of information security threats is a curved risk surface located in the coordinate system (time interval; information asset (IA); risk). A risk surface is a set of points satisfying condition (1). The risk surface is usually a curved surface. Curvature is an indicator that the risk in a given space and time changes. A smooth surface indicates that the risk does not change over time for all the considered IA. A surface with an unchanged risk value will be considered a risk plane. Using risk planes, on the basis of a three-dimensional space-time model of IS threats, a two-dimensional is constructed. An example of two-dimensional visualization of the spatio-temporal model of IS threats is presented in "Fig. 3".

The two-dimensional spatio-temporal model of information security threats is presented in the form of contour lines - a series of curves of closed lines corresponding to a certain risk value. The horizontal is constructed by the cross-section of the risk surface by the risk plane parallel to the axes of space and time and perpendicular to the risk axis. The lower the risk value of the secant plane, the dimmer the horizontals are displayed, the

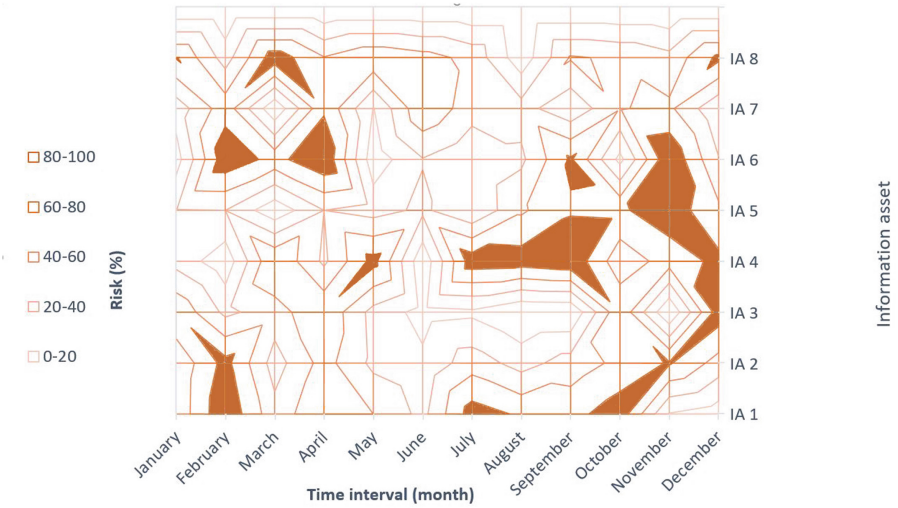

Fig. 3. An example of two-dimensional visualization of the spatio-temporal model of IS threats.

higher the risk value of the secant plane - the more vivid the risk horizontal is shown. The horizontal connects the points of the risk surface of a single value. Visually, horizontal color brightness is a risk level for an information security analyst. An unacceptable risk value for an IA is determined by an information security analyst before visualization. On two-dimensional visualization, an unacceptable risk value is presented in the form of a plane whose color corresponds to the horizontal color of the same risk level.

5 Testing Results of the Visualization of the Spatio-Temporal Model of Information Security Threats

The proposed method for visualizing the spatio-temporal threat model has been tested in developing the threat model of a virtual network security system for an industrial enterprise. When developing an IS threat model, analysts are offered two options for visualizing the threat model. The proposed method for visualizing a two-dimensional space-time model of information security threats and the classical tabular presentation method were compared. Both IS threat models were built using the same methodology [20]. The comparison criterion is the amount of time required by an information security analyst to work with information security threat models that have a different visual representation. Figure 4 shows a histogram of the time spent on processing threat models in a tabular representation and two-dimensional visualization by analysts A, B, C.

The use of the method proposed in the article reduced the time to determine the actual IS threats by an average of 17.9%. All analysts noted that the two-dimensional method of visualization is more convenient to read during analysis than the three-dimensional one. This is due to the fact that to read three-dimensional visualization, it is necessary to use a viewer of three-dimensional objects in order to be able to rotate the risk surface for detailed analysis [21].

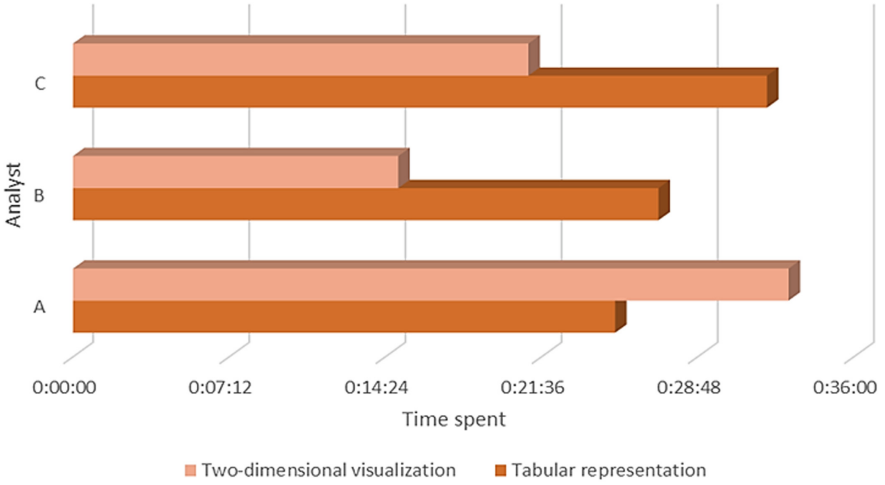

Fig. 4. A histogram of time spent on processing IS threat models in a tabular representation and two-dimensional visualization by analysts A, B, C.

Despite all the advantages, the proposed method for visualizing the spatio-temporal model of information security threats has an assumption in the construction: the risk surface displays the risk from a single threat or one type of information security threats.

The assumption is proposed to minimize by using information security classes or clusters. This will allow us to build more detailed and informative visualizations of spatio-temporal models of IS threats. For greater informational content of one visualization, it is proposed to combine several surfaces of spatio-temporal threat models on one visualization.

6 Conclusion

The presented study offers visualization of the IS threat model as a tool to accelerate risk assessment and select security measures at the stage of processing the IS threat model. The proposed method for visualizing the spatio-temporal model of information security threats has a number of advantages over traditional methods for presenting threat models in tabular form or in the form of lists. Three-dimensional and two-dimensional risk surfaces, located in the axes of time and space, clearly demonstrate IS analytics how to most efficiently distribute resources aimed at protecting information. This will save some areas of space at a certain point in time from an excess of resources for protection, while others will be protected properly. Visualization of the IS threat model accelerates the identification of actual threats by the IS analyst. The disadvantages of visualizing the spatio-temporal threat model are that it is convenient to analyze one information security threat on one visualization. This drawback is covered by the use of threat classification when rendering.

Acknowledgments. The study was carried out with the financial support of the Russian Federal Property Fund in the framework of the scientific project № 20-07-01065 and a grant from the President of the Russian Federation for state support of leading scientific schools of the Russian Federation (NSh-2502.2020.9).

References

1. Kolomeec, M., Gonzalez-Granadillo, G., Doynikova, E., et al.: Choosing models for security metrics visualization. In: 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security. Springer, Warsaw (2017)
2. Hall, P., Heath, C., Coles-Kemp, L.: Critical visualization: a case for rethinking how we visualize risk and security. J. Cybersecurity **1**(1) (2015). https://doi.org/10.1093/cybsec/tyv004
3. Yang, L., Ma, Z., Zhu, L., et al.: Research on the visualization of spatio-temporal data. In: IOP Conference Series: Earth and Environmental Science (2018)
4. Markowsky, G.: Visualizing cybersecurity events. In: International Conference on Security and Management, vol. 1, pp. 445–451 (2013)
5. Marty, R.: Applied Security Visualization. Addison-Wesley Professional, Boston (2008)
6. Sopan, A., Berninger, M., Mulakaluri, M., et al.: Building a machine learning model for the SOC, by the Input from the SOC, and Analyzing it for the SOC. In: Symposium on Visualization for Cyber Security. Institute of Electrical and Electronics Engineers, Berlin (2018)
7. Trent, S., Kohlhammer, J., Sauer, G., et al.: Eventpad: rapid malware analysis and reverse engineering using visual analytics. In: Symposium on Visualization for Cyber Security. Institute of Electrical and Electronics Engineers, Berlin (2018)
8. Bakirtzis, B., Simon, J.B., Fleming, H.C., et al.: Security visualization for cyber-physical system design and analysis. In: Symposium on Visualization for Cyber Security. Institute of Electrical and Electronics Engineers, Berlin (2018)
9. Siming, C., Shuai, Ch., Andrienko, N., Andrienko, G., et al.: User behavior map: visual exploration for cyber security session data. In: Symposium on Visualization for Cyber Security. Institute of Electrical and Electronics Engineers, Berlin (2018)
10. Krokos, E., Rowden, R.A., Whitley, K., et al.: Visual analytics for root DNS data. In: Symposium on Visualization for Cyber Security. Institute of Electrical and Electronics Engineers, Berlin (2018)
11. Ulmer, A., Schufrin, M., Sessler, D., et al.: Visual-interactive identification of anamolous IP-block behavior using geo-IP data. In: Symposium on Visualization for Cyber Security. Institute of Electrical and Electronics Engineers, Berlin (2018)
12. Gove, R., Deason, L.: Visualizing automatically detected periodic network activity. In: Symposium on Visualization for Cyber Security. Institute of Electrical and Electronics Engineers, Berlin (2018)
13. Kim, H., Ko, S., Kim, D.S., et al.: Firewall ruleset visualization analysis tool based on segmentation. In: Symposium on Visualization for Cyber Security. Institute of Electrical and Electronics Engineers, Berlin (2017)
14. Gokaraju, B., Agrawal, R., Adrian Doss, D., et al.: Identification of spatio-temporal patterns in cyber security for detecting the signature identity of hacker. Saint Petersburg (2018)
15. Ahola, T., Virrantaus, K., Matthias Krisp, J., et al.: A spatio-temporal population model to support risk assessment for emergency response decision-making. Int. J. Geogr. Inf. Sci. **21**(8), 935–953 (2014). https://doi.org/10.1080/13658810701349078

16. IEEE Symposium on Visualization for cyber security (2020). https://vizsec.org. Accessed 03 Mar 2020
17. International organization for standardization. ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management (2005). https://www.iso.org/standard/39612.html. Accessed 10 Feb 2020
18. International Organization for Standardization. ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management (2011). https://www.iso.org/standard/56742.html. Accessed 02 Mar 2020
19. Aralbaev, T.Z., Aralbaeva, G.G., Abramova, T.V., et al.: Optimization of methods for monitoring the technical condition of distributed automated systems under the influence of spatio-temporal threats based on monitoring network information flows. OSU, Orenburg (2018)
20. BS 7799-3: Information security management systems – Guidelines for information security risk management. BSI Standards Limited (2017)
21. Roddick, J.F., Lees, B.G.: Paradigms for spatial and spatio-temporal data mining. In: Miller, H.G., Han, J. (eds.) Geographic Data Mining and Knowledge Discovery. Taylor & Francis, London (2001)