IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 10, 2021, accepted November 17, 2021, date of publication November 19, 2021,
date of current version December 2, 2021.

*Digital Object Identifier 10.1109/ACCESS.2021.3129488*

# Fuzzy Expert System of Information Security Risk Assessment on the Example of Analysis Learning Management Systems

**S. A. ABDYMANAPOV, M. MURATBEKOV, S. ALTYNBEK, AND A. BARLYBAYEV**
Kazakh University of Economics, Finance and International Trade, 010008 Astana, Nur-Sultan, Kazakhstan

Corresponding author: A. Barlybayev (frank-ab@mail.ru)

This work was supported in part by the Committee of Science of the Ministry of Education and Science of the Republic of Kazakhstan under Grant AP08856687 "Intelligent System of Support and Control of Distance Learning Technologies."

**ABSTRACT** The rapid development and application of new digital technologies has, on the one hand, opened up new opportunities for more efficient management of technological and business processes. On the other hand, this leads to a significant increase in security threats, increasing the vulnerability of businesses and organisations to cybercriminals. In recent years, the rapid growth of incidents of various kinds has shown that traditional approaches to information security (IS) are insufficient. Consequently, software product information security risk assessment has become an important task for most organisations. Several models have been proposed to help different enterprises deal with the challenges of building information security. This paper proposes a new hierarchical structured model for information security risk assessment using fuzzy logic. A new method for information security risk assessment of software is also described using the example of automated control systems or enterprise resource planning (ERP) systems (using learning management systems as an example). The proposed new risk assessment model has been software implemented using fuzzy logic in the form of 15 fuzzy machines. In a series of experiments, we have scrutinised the information security risk assessment of various software products. The proposed method should solve the problem of flexible risk assessment.

**INDEX TERMS** Fuzzy logic, business process modeling, information security risk, risk assessment.

## I. INTRODUCTION

It is known that no organisation can be immune to data breaches and that when breaches occur, they can have serious consequences. A data breach can be looked at differently in different areas. Any action to breach the security of protected data that results in the transfer of data to unauthorised entities can be seen as an IS breach. A security breach can be the result of a cyber-attack, theft or loss of devices, theft or leakage of employee data such as security credentials, and human error. In industrial and business systems, major cyber-attacks include SQL injection, cross-site scripting (XSS) and privilege escalation. SQL injection is one of the most common attacks that can destroy a database by placing crafted malicious code in SQL statements through web page input. Developing an effective cyber security solution enables us to reduce data breaches threatened by cyber security risks, such as cyber-attacks on storage, processing and database management. Organising cyber security in the life of a society remains one of the major unresolved challenges in the information and communications technology domain.

Hypothesis – the problem is that companies find it difficult to manage information security in complex systems such as ERP. Why can't software developers fully secure a complex system, even with IS standards and IS risk assessment models in their arsenal? What can software developers offer to improve information security of complex systems? This reveals the problem in achieving security when programming complex systems. Careless use by employees or miscalculations in building information security will have an impact on the financial losses of the company. Software developers may use models for building information security that are not suitable for complex systems. Given due consideration for

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Imran Tariq.

previous legacy models, a more flexible information security evaluation model is needed. The purpose of this research is to implement a flexible model for assessing information security risks for ERP systems. The issue of information security is very important precisely in ERP systems, since usually such systems allow you to manage all the main production business processes of an organization. The ERP system with poor information security will eventually lead the company to colossal financial losses. In conditions of lack of statistical data and high uncertainty of the external environment methods based on fuzzy expert systems that use the experience and knowledge of employees, inaccurate preliminary data, assumptions, can be the basis of sustainable economic development of the company. The general purpose of fuzzy management systems is to simulate the thought process of a person who makes conclusions in order to make some decision based on the information available about the control object. Situations of this kind are found in abundance in everyday life, as well as in the professional activities of people. Even if we do not take into account quite trivial operations (which nevertheless require such an approach), we can give a number of examples where automation and the use of elements of artificial intelligence are relevant and justified: from control of a car or technological process to the development of a company development strategy, based on a set of financial and economic indicators. The key to the successful use of such fuzzy-multiple methods in the management of complex systems is the ability of systems to use all the main sources of information about the control object, which include: mathematical models; actual data of observations of the behavior of the object; knowledge of people – experts in the studied area. Indeed, all these sources can be used in a fuzzy control system, mutually complementing each other. Mathematical model, if its construction is fundamentally possible and appropriate, is the most important source of information, allowing the replenishment of the knowledge base by the results of analytical research or simulation modeling. Processing of empirical data allows you to build an approximate model of the control object, as well as refine, tune the parameters of fuzzy control system. At the same time on the basis of knowledge and experience of experts a set of fuzzy rules, reflecting regularities of behavior of the studied object is formed. In cases when it is impossible to develop a mathematical model due to the high complexity of processes inherent in the control object, the advantages of methods based on fuzzy management are even stronger, as management is based not only on some model, but it is realized intellectual management, having in its basis the knowledge in all variety of their manifestations. Important advantages of fuzzy expert systems are non-linearity, the ability to use imprecise data, convenience for obtaining and processing of expert opinions.

There are no specific models or standards for information security assessment for complex systems. In any case, this points to the importance of studying all known information security assessment models. There are a number of good papers on "How to evaluate information security of a software product"?

In this paper, Bo Feng, Qiang Li, Yuede Ji and others propose a new user analysis model to find potential victims by analyzing large amounts of personal information and user behaviour in social media, the model estimates the security risk [1]. Pil Sung Woo, Sang Sun Hwang, Soon Hyun Hwang and Balho H. Kim conducted a study on a theoretical standard for creating secure systems by analyzing the structure of power information management system in addition to quantifying the risk of cyber-attacks, which remain poorly understood [2]. In this paper, Timothy Kieras, Muhammad Junaid Farooq and Quanyan Zhu described Risk Analysis of Internet of Things (IoT) Supply Chain Threats (RIoTS), a security risk assessment framework borrowed from systems reliability theory to include the supply chain [3]. In this paper, Manish Shrestha, Christian Johansen, Josef Noll and Davide Roverso described Smart Grid Security Classification (SGSC), which is related to risk analysis methods (ANSSI standard methodology) with the difference that the SGSC classification method aims to assign a security class to a system based on (combinations of) scores assigned to different aspects of system vulnerabilities and the corresponding implemented protection mechanisms [4]. In this paper, Jasna Markovic-Petrovic, Mirjana Stojanovic and Slavica Bostjancic Rakas proposed a new method for security risk assessment in supervisory control and data acquisition (SCADA) networks using fuzzy logic [5]. Wenrui Wang, Fan Shi, Min Zhang, Chengxi Xu and Jinghua Zheng proposed a heterogeneous information network based ranking method for vulnerability risk assessment in a particular network [6]. Jiali Wang, Martin Neil and Norman Fenton obtained a combined Extended Factor Analysis of Information Risk-Bayesian Networks (EFBN) approach using Monte Carlo simulation and showed that it can provide an integrated solution for cybersecurity risk assessment and decision making [7]. In this study, Yahia Alemami, Mohamad Afendee Mohamed, Saleh Atiewi aims to present the most popular and interesting algorithms currently in use [8]. In this paper, Yazdan Movahedi, Michel Cukier, Ambrose Andongabo and Ilir Gashi described the approach, which investigated consists of clustering vulnerabilities by using textual information in vulnerability records and then modelling the mean-vulnerability function by relaxing the monotonic intensity function assumption that prevails in studies that use software reliability models (SRMs) and heterogeneous Poisson process in modelling [9]. In this paper, Kaikai Pan, Andre Teixeira, Claudio David Lopez and Peter Palensky analyzed the cybersecurity of Energy Management System (EMS) against data attacks. The results show how vulnerable the EMS is to data attacks and how collaborative modeling can help in vulnerability assessment [10]. In this study, Omer Keskin, Kevin Matthe Caramancion, Irem Tatar, Owais Raza and Unal Tatar presented and compared existing Cyber Third-Party Risk Management (C-TPRM) methods created by different companies to identify the most commonly used indicators and evaluation criteria [11]. Lelin Lv, Huimin li, Lunyan Wang, Qing Xia and Li Ji innovatively introduce interval intuitionistic fuzzy weighted averaging operator (IVIFWA), Tchebycheff metric distance and interval intuitionistic fuzzy weighted geometric operator (IVIFWG) into a relation system, reference point method and full multiplication method, MULTIMOORA sub-method to optimize FMEA information aggregation process [12]. In this paper, Samia Oukemeni, Helena Rifa-Pous, and Joan Manuel Marques Puig proposed a general framework to guide the development of privacy indicators and to measure and evaluate the privacy level of Social Networking on the Internet, in particular microblogging systems [13]. In this paper, Simon Parkinson, Mauro Vallati, Andrew Crampton and Shirin Sohrabi presented GraphBAD, a graph-based analysis tool capable of analyzing security configurations to identify anomalies that may lead to potential security risks [14]. In this paper, Abdullah Algarni, Vijey Thayananthan and Yashwant Malaiya described a comprehensive formal model that estimates two components of security risks: cost of hacking and probability of data leakage within 12 months [15]. In this research, Muhamad Al Fikri, Fandi Aditya Putra, Yohan Suryanto and Kalamullah Ramli focuses on information security risk assessment by implementing a combined technique in a commercial organization using semi-quantitative methods [16]. The aim of the paper by the authors Muhammad Imran Tariq, Shakeel Ahmed, Nisar Ahmed Memon and others was to improve the method of information security management analysis by proposing a formalized approach, i.e. fuzzy analytic hierarchy process (AHP). This approach was used to prioritise and select the most appropriate set of information security controls to meet the information security requirements of an organisation [17]. In this paper, Jinxin Zuo, Yueming Lu, Hui Gao, Ruohan Cao, Ziyv Guo and Jim Feng summarised the architecture and vulnerabilities in IoT and proposes a comprehensive information security assessment model based on multilevel decomposition feedback [18].

Cybersecurity standards are published materials that outline methods that focus on protecting the cyber environment of a user or organisation. The main purpose is to reduce risks, including preventing or mitigating cyber-attacks. These published materials consist of collections of tools, policies, security concepts, security measures, guidelines, risk management approaches, actions, training, best practices, safeguards and technologies.

Basic standards on information security:

1) ISO/IEC 27000 – Information security management systems – Overview and vocabulary.
2) ISO/IEC 27001 – Information technology – Security Techniques – Information security management systems – Requirements. The 2013 release of the standard specifies an information security management system in the same formalized, structured and succinct manner as other ISO standards specify other kinds of management systems.
3) ISO/IEC 27002 – Code of practice for information security controls – essentially a detailed catalog of information security controls that might be managed through the ISMS.
4) ISO/IEC 27003 – Information security management system implementation guidance
5) ISO 15408 – This standard develops what is called the "Common Criteria". It allows many different software and hardware products to be integrated and tested in a secure way.
6) IEC 62443 – cybersecurity standard defines processes, techniques and requirements for Industrial Automation and Control Systems (IACS).
7) ETSI EN 303 645 – standard provides a set of baseline requirements for security in consumer Internet of things (IoT) devices.

## II. RISK ASSESSMENT CRITERIA

We need to define criteria and metrics for assessing software information security by analysing the above-mentioned standards. On the basis of interdisciplinary analysis (the above-mentioned studies and standards) a list consisting of 50 IS risks, which can be used in the practical activities of the enterprise, since the neutralization (elimination, minimization) of IS risks is the essence and content of the process of ensuring IS of the enterprise. On the basis of the offered list also it is possible to build models of threats on which the task of creation of information security systems (ISS) is made. Besides the list of concrete risks can be used during estimation of influence of accepted IS measures on efficiency of activity of enterprise. The IS risks are presented in Table 1.

Table 1 is presented as a fuzzy information security risk assessment model in Figure 1. These characteristics are fully consistent with the definition of an information security risk assessment for a software product. The problem appeals to the solution of three questions: software security scale, regulation of user behaviour, list of requirements for software developers. Therefore, we propose the following methodology for information security assessment using fuzzy logic.

A flexible information security assessment model requires the execution of fuzzy logic because of its flexibility and variability in evaluating any initially hard-coded parameter. A fuzzy approach helps to make decisions with different options, fuzziness and vulnerabilities [17]. It is practical for dealing with uncertainty, complexity and decision making on complex issues of controversial nature. In the paper Muhammad Imran Tariq, Shakeel Ahmed, Nisar Ahmed Memon and others argue that prioritizing information security management tools using fuzzy AHP leads to efficient and cost-effective evaluation of information security management tools for an organization to select the most appropriate ones. The proposed formalised approach and prioritisation processes are based on International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 27001: 2013 standards [17]. The evaluation results have clearly demonstrated the advantages of the proposed

**TABLE 1.** Risks Structure.

| # | Risks |
|---|---|
| | 1. Organizational risks |
| | 1.1. Documentation risks |
| *1* | 1.1.1. Lack of signaling means in case of emergency situations |
| *2* | 1.1.2. Lack of regulations for actions of information security employees in the event of an emergency situation |
| *3* | 1.1.3. Uncontrolled use and write-off of information carriers |
| *4* | 1.1.4. Lack of video surveillance systems for key nodes of information systems, access control to work premises |
| *5* | 1.1.5. Uncontrolled use of the Internet |
| | 1.2. Human risks |
| *6* | 1.2.1. Personnel errors, low qualifications |
| *7* | 1.2.2. Intentional harm by disloyal employees |
| *8* | 1.2.3. Malicious actions of the network administrator |
| *9* | 1.2.4. Combining the duties of an Information System administrator and an Information Security administrator |
| *10* | 1.2.5. Malicious acts when servicing |
| | 2. Reputation (branding) risks |
| *11* | 2.1. Dissemination in the external environment of information of an economic nature that threatens the company's reputation |
| *12* | 2.2. Mentioning a company in the context of extremism, money laundering, cyber threats and cyber terrorism. |
| *13* | 2.3. Use of uncertified and unlicensed products |
| *14* | 2.4. Possibility of external penetration into the company's Intranet system |
| | 3. Privacy risks |
| | 3.1. Privacy regulations |
| *15* | 3.1.1. Lack of clear regulations for working with personal data |
| *16* | 3.1.2. Acceptance of untested cryptographic information protection devices into operation |
| *17* | 3.1.3. Lack of monitoring and analysis procedures for all performed operations |
| *18* | 3.1.4. Lack of organizational procedures that allow for internal investigations of violations of confidentiality risks |
| | 3.2. Authorization |
| *19* | 3.2.1. Long-term preservation of the authorization window in case of inactivity or in the event of an employee leaving the premises |
| *20* | 3.2.2. Unauthorized access to passwords and keys |
| *21* | 3.2.3. Failure to respect the confidentiality of passwords |
| *22* | 3.2.4. Violations of the order of storage and transmission of passwords |
| *23* | 3.2.5. Inaccurate identification of Information System users |
| *24* | 3.2.6. The absence of protective measures in the systems, ensuring the impossibility of denying the authorship of the operations and transactions carried out |
| *25* | 3.2.7. Lack of mechanisms for registering unauthorized access to information for identification, authorization of customers and employees |
| | 3.3. Unauthorized access |
| *26* | 3.3.1. Unauthorized access to data in Information System and PC |
| *27* | 3.3.2. Leakage of service information through various channels |
| *28* | 3.3.3. The ability to remotely retrieve information from external positions |
| *29* | 3.3.4. Possibility of uncontrolled information retrieval from internal positions |
| *30* | 3.3.5. Unauthorized use of the electronic payment system, remote service |
| *31* | 3.3.6. Virtual theft and forgery using personal data |
| | 3.4. Theft |
| *32* | 3.4.1. Interception of data in various ways |
| *33* | 3.4.2. Actual theft and theft of technical equipment (phones, laptops, flash drives, communicators, etc.) |

**TABLE 1.** *(Continued.)* Risks Structure.

| # | Risks |
|---|---|
| | 4. Integrity risks |
| | 4.1. Hardware integrity |
| *34* | 4.1.1. The usual failure of technical equipment (average) |
| *35* | 4.1.2. Failure of technical means due to force majeure circumstances |
| *36* | 4.1.3. Changing the configuration of information processing facilities and systems |
| | 4.2. Software integrity |
| *37* | 4.2.1. Software control failures |
| *38* | 4.2.2. Penetration of malicious codes into information systems |
| *39* | 4.2.3. The emergence of windows of vulnerability in the protection of information systems associated with the use of "patches" in protected software |
| *40* | 4.2.4. Software attacks on the capabilities of processors and RAM |
| *41* | 4.2.5. Combining the responsibilities of a software developer and user |
| | 4.3. Integrity of information |
| *42* | 4.3.1. Loss or unavailability of important data |
| *43* | 4.3.2. Use of incomplete or distorted information |
| *44* | 4.3.3. Violations of the order of copying (backing up) information |
| | 5. Availability risks |
| *45* | 5.1. Unauthorized latent long-term exploitation of information and computing resources |
| *46* | 5.2. DDoS attacks on the ABS and employees' computers |
| *47* | 5.3. Unauthorized remote access to Information System and PC |
| *48* | 5.4. Unprotected remote access (authorized) to Information System and PC |
| *49* | 5.5. Insecurity of email |
| 50 | 5.6. SPAM threats |

method using fuzzy logic over the purely objective approach in terms of more accurate risk assessment and higher return on security investments [5]. Muhammad Imran Tariq proposed a framework for information security assessment in cloud systems, which was implemented using a fuzzy inference system based on fuzzy set theory and fuzzy logic rules. Matlab was used to test the framework. The fuzzy results confirm that the proposed framework can be used to protect information in a cloud computing environment [19]. In these researches, Hakan Acikgoz, Fatih Kececioglu, Ahmet Gani, Mustafa Tekin and Mustafa Sekkeli suggests Controllers of Type 2 Fuzzy Logic Takagi Sugeno Kang (IT2-TSK-FLC) and Type 2 Fuzzy Logic Interval System (T2FLS). The results confirm that the proposed controllers provide fast speed, reliable operation against uncertainties and have better performance [20], [21].

We propose 4 levels of tangibility in assessing the information security of a software application. At the first level, both external and internal components of information security are used as an indicator of the risk assessment objective. At the first level, we establish the Risk objective. For ease of grouping in the second level, we introduce the first level of risk classification. At the third level, risks are described, or a subset of the risk classification is set. The fourth level describes the risks, assuming that the third level did not describe the risks. This structure can be used as separately (element by element) for an assessment of risks of certain groups and subgroups, and as means for complex (holistic) assessment of information security of the software product used in the company.

Next, using the classification of information security risk assessment criteria, we construct 15 machine phases using the Mamdani algorithm. In these papers, Alibek Barlybayev, Batyr Orazbayev and others showed that the Matlab software product is very suitable for this simulation [22]–[24]. Using a fuzzy expert system to assess information security is not a new idea. But the main works with the use of fuzzy logic is related to the existing standards for assessing information security, with the carnally known established formulas for calculating information security risks. This can lead to misuse of fuzzy logic as a tool, when multiple parameters are reduced to one or two variables. This paper proposes a new four-level hierarchical system of parameters for assessing information security risks. And the use of fuzzy logic makes the calculations flexible, since the number of parameters, rigidly defined at the initial stage, is constantly increasing.

## III. A FUZZY INFORMATION SECURITY RISK ASSESSMENT MODEL

In the first fuzzy machine 1.1. Documentation risks we will use the input variables: 1.1.1. Lack of signaling means in case of emergency situations; 1.1.2. Lack of regulations for actions of information security employees in the event of an emergency situation; 1.1.3. Uncontrolled use and write-off of information carriers; 1.1.4. Lack of video surveillance systems for key nodes of information systems, access control to work premises; 1.1.5. Uncontrolled use of the Internet. The output variable will be 1.1. Documentation risks.

In the second fuzzy machine 1.2. Human risks we will use the input variables: 1.2.1. Personnel errors, low qualifications; 1.2.2. Intentional harm by disloyal employees; 1.2.3. Malicious actions of the network administrator; 1.2.4. Combining the duties of an Information System administrator and an Information Security administrator; 1.2.5. Malicious acts when servicing. The output variable will be 1.2. Human risks.

In the third fuzzy machine 1. Organisational service risks we will use input variables: 1.1. Documentation risks; 1.2. Human risks. 1. Organizational risks.

In the fourth fuzzy machine 2. Reputation (branding) risks we will use input variables:2.1. Dissemination in the external environment of information of an economic nature that threatens the company's reputation; 2.2. Mentioning a company in the context of extremism, money laundering, cyber threats and cyber terrorism; 2.3. Use of uncertified and unlicensed products; 2.4. Possibility of external penetration into the company's Intranet system. The output variable will be 2. Reputation (branding) risks.

In the fifth fuzzy machine 3.1. Privacy regulations we will use the input variables: 3.1.1. Lack of clear regulations for working with personal data; 3.1.2. Acceptance of untested cryptographic information protection devices into operation; 3.1.3. Lack of monitoring and analysis procedures for all performed operations; 3.1.4. Lack of organizational procedures that allow for internal investigations of violations of confidentiality risks. Output variable - 3.1. Privacy regulations.

In the sixth fuzzy machine 3.2. Authorization we will use the input variables: 3.2.1. Long-term preservation of the authorization window in case of inactivity or in the event of an employee leaving the premises; 3.2.2. Unauthorized access to passwords and keys; 3.2.3. Failure to respect the confidentiality of passwords; 3.2.4. Violations of the order of storage and transmission of passwords; 3.2.5. Inaccurate identification of Information System users; 3.2.6. The absence of protective measures in the systems, ensuring the impossibility of denying the authorship of the operations and transactions carried out; 3.2.7. Lack of mechanisms for registering unauthorized access to information for identification, authorization of customers and employees. Output variable - 3.2. Authorization.

In the seventh fuzzy machine 3.3. Unauthorized access we will use the input variables: 3.3.1. Unauthorized access to data in Information System and PC; 3.3.2. Leakage of service information through various channels; 3.3.3. The ability to remotely retrieve information from external positions; 3.3.4. Possibility of uncontrolled information retrieval from internal positions; 3.3.5. Unauthorized use of the electronic payment system, remote service; 3.3.6. Virtual theft and forgery using personal data. Output variable - 3.3. Unauthorized access.

In the eighth fuzzy machine 3.4. Theft, machine we will use the input variables: 3.4.1. Interception of data in various ways; 3.4.2. Actual theft and theft of technical equipment (phones, laptops, flash drives, communicators, etc.). Output variable - 3.4. Theft.

In the ninth fuzzy machine 3. Privacy risks we will use the input variables: 3.1. Privacy regulations; 3.2. Authorization; 3.3. Unauthorized access; 3.4. Theft. Output variable - 3. Privacy risks.

In the tenth fuzzy machine 4.1. Hardware integrity we will use the input variables: 4.1.1. The usual failure of technical equipment (average); 4.1.2. Failure of technical means due to force majeure circumstances; 4.1.3. Changing the configuration of information processing facilities and systems. Output variable - 4.1. Hardware integrity.

In the eleventh fuzzy machine 4.2. Software integrity we will use the input variables: 4.2.1. Software control failures; 4.2.2. Penetration of malicious codes into information systems; 4.2.3. The emergence of windows of vulnerability in the protection of information systems associated with the use of "patches" in protected software; 4.2.4. Software attacks on the capabilities of processors and RAM; 4.2.5. Combining the responsibilities of a software developer and user. Output variable - 4.2. Software integrity.

In the twelfth fuzzy machine 4.3. Integrity of information we will use the input variables: 4.3.1. Loss or unavailability

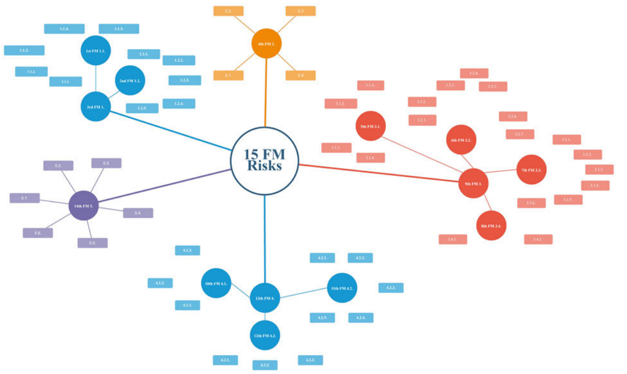


**FIGURE 1.** Fuzzy Information Security Risk Assessment Model.

of important data; 4.3.2. Use of incomplete or distorted information; 4.3.3. Violations of the order of copying (backing up) information. Output variable - 4.3. Integrity of information.

In the thirteenth fuzzy machine 4. Integrity risks we will use the input variables: 4.1. Hardware integrity; 4.2. Software integrity; 4.3. Integrity of information. Output variable - 4. Integrity risks.

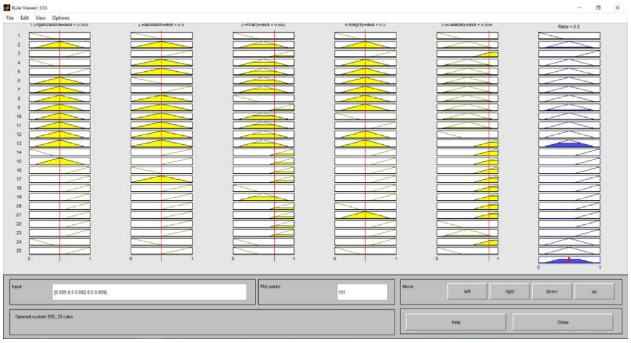
In the Fourteenth Fuzzy Machine 5. Availability risks we will use the input variables: 5.1. Unauthorized latent long-term exploitation of information and computing resources; 5.2. DDoS attacks on the ABS and employees' computers; 5.3. Unauthorized remote access to Information System and PC; 5.4. Unprotected remote access (authorized) to Information System and PC; 5.5. Insecurity of email. 5.6. SPAM threats. Output variable - 5. Availability risks.

In the Fifteenth Fuzzy Machine Risks we will use the input variables: 1. Organizational risks; 2. Reputation (branding) risks; 3. Privacy risks; 4. Integrity risks; 5. Availability risks. Output variable - 5 Risks.

All 15 fuzzy machines are closely related, which are described in Figure 2. The features represent the values of the subclasses. The subclassifications provide the value of the classifications. The classifications provide information security evaluation.

Describe the upper and lower values of all variables. Linguistic variable "Low" – 'trimf', [−0.4 0 0.4]. Linguistic variable "Moderate" – 'trimf', [0.1 0.5 0.9]. Linguistic variable "High" – 'trimf', [0.6 1 1.4]. The lower and upper values define a trapezoidal membership function for each input and output variable. The centroid defuzzification method was used for each fuzzy machine. Figure 2 shows the test results for each of the fifteen fuzzy machines. The defuzzification result is shown in blue in the right corner. As an example, the Platonus Learning Management System v5.2 (build#788) was used at the Kazakh University of Economics, Finance and International Trade http://pl.kuef.kz/.

We modeled on Matlab a fuzzy expert system using the Mamdani algorithm to assess the information security risks of software. Regarding the linguistic variables, we used the risk criteria from Table 1. Now we were faced with the task of programming this model into a single fuzzy expert system.

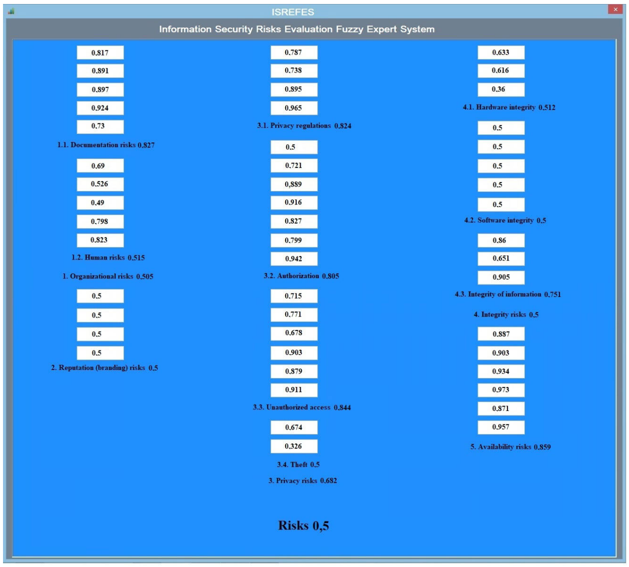


Input: [0.505 0.5 0.682 0.5 0.859]

Plot points: 101

Opened system 555, 25 rules

**FIGURE 2.** Test results of calculation of the fuzzy machine Risks.



Information Security Risks Evaluation Fuzzy Expert System

0,817
0,891
0,897
0,924
0,73
1.1. Documentation risks 0,827
0,69
0,526
0,49
0,798
0,823
1.2. Human risks 0,515
1. Organizational risks 0,505
0,5
0,5
0,5
0,5
2. Reputation (branding) risks 0,5

0,787
0,738
0,895
0,965
3.1. Privacy regulations 0,824
0,5
0,721
0,889
0,916
0,827
0,799
0,942
3.2. Authorization 0,805
0,715
0,771
0,678
0,903
0,879
0,911
3.3. Unauthorized access 0,844
0,674
0,326
3.4. Theft 0,5
3. Privacy risks 0,682

0,633
0,616
0,36
4.1. Hardware integrity 0,512
0,5
0,5
0,5
0,5
0,5
4.2. Software integrity 0,5
0,86
0,651
0,905
4.3. Integrity of information 0,751
4. Integrity risks 0,5
0,887
0,903
0,934
0,973
0,871
0,957
5. Availability risks 0,859

Risks 0,5

**FIGURE 3.** Information Security Risks Evaluation Fuzzy Expert System (ISREFES).

The fuzzy expert system is developed in the C # programming language and is described in Figure 3.

## IV. EVALUATION EXPERIMENT

Classic Standard Risk Formula NIST 800-30:

$R{=}P(t){*}S$

*R— Risk. P(t) — Probability of an information security threat. S— asset value.*

Since we want to correlate among the different methods, we need to normalize the calculated formulas:

$R_{norm}{=}(P(t){-}P(t)_{min})/(P(t)_{max}{-}P(t)_{min}){*}(S{-}S_{min})/(S_{max}{-}S_{min})$ Standard Risk Formula ISO/IEC TR 13335-3:1998:

$R{=}P(t){*}P(v){*}S$

*P(t) – Probability of an information security threat. P(v) – vulnerability potential. S— asset value.*

$R_{norm}{=}(P(t){-}P(t)_{min})/(P(t)_{max}{-}P(t)_{min}){*}(P(v){-}P(v)_{min})/(P(v)_{max}{-}P(v)_{min}){*}(\mathrm{S}{-}\mathrm{S}_{\mathrm{min}})/(\mathrm{S}_{\mathrm{max}}{-}\mathrm{S}_{\mathrm{min}})$

Standard Risk Formula BS 7799:

$R{=}S{*}L(t){*}L(v)$

*S— asset value.*

**TABLE 2. Results Of Evaluating LMS.**

| LMS | NIST 800-30 | ISO/IEC TR 13335-3:1998 | BS 7799 | ISREFES | Expert |
|---|---|---|---|---|---|
| ENU | 0,193 | 0,396 | 0,385 | 0,293 | 0,189 |
| KazGUU | 0,701 | 0,798 | 0,764 | 0,741 | 0,698 |
| EKTU | 0,602 | 0,693 | 0,68 | 0,642 | 0,598 |
| KazNU | 0,823 | 0,9 | 0,898 | 0,857 | 0,81 |
| KSU | 0,411 | 0,501 | 0,481 | 0,45 | 0,401 |
| AITU | 0,517 | 0,599 | 0,577 | 0,547 | 0,499 |

$L(t)$— *threat level.*

$L(v)$— *level/degree of vulnerability.*

$R_{norm}$=(S-$S_{min}$)/($S_{max}$-$S_{min}$)∗($L(t)$-$L(t)_{min}$)/($L(t)_{max}$ -$L(t)_{min}$)∗($L(v)$-$L(v)_{min}$)/($L(v)_{max}$-$L(v)_{min}$)

Then we conduct an experiment to assess the information security risk of the software used by some universities. In addition, these 6 LMS are evaluated by a software quality assessment expert. The results of the evaluation are described in Table 2. The list of software used as a role of LMS:

1) Platonus v5.2 (build# 1003) B L.N. Gumilyov Eurasian National University https://edu.enu.kz/.
2) Canvas in KazGUU https://kazguu.instructure.com/login/canvas.
3) Academic portal of EKSTU in the East Kazakhstan State Technical University named after D. Serikbayev. D. Serikbayev http://www.do.ektu.kz/doektu/Default.aspx?lang=en.
4) UNIVER system at Al-Farabi Kazakh National University https://univer.kaznu.kz/user/login.
5) KSU portal at Kostanai State University named after A. Baitursynov http://ksu.edu.kz/ru/portal/.
6) Portal in Astana IT University https://moodle.astanait.edu.kz/.

According to NIST 800-30, ISO/IEC TR 13335-3:1998, BS 7799, and ISREFES, the assessment was conducted by non-specialists in software information security. These auditors studied the characteristics and sub-characteristics of these information security risk assessment methodologies. The auditors made assessments strictly according to the rules of the described methodology. After reviewing the entire procedure, they placed the scores for the 6 software samples in the 2nd, 3rd, 4th, and 5th columns of Table 2.

The last column of results in Table 2 was put by an expert in the field of cryptography, software architecture, he also has relevant certificates. When the expert evaluated the quality of 6 programs, he relied on his experience, not on a particular method. That is, the expert did not use the described techniques. In addition, this expert has worked with these software for a long time, so he knows how to choose the best one. Consequently, the expert's evaluation is more objective, because the expert makes his/her evaluation based on his/her personal experience with the 6 programs and his/her experience in developing secure software. Next, we conduct a correlation study. This study will give us an understanding of the effectiveness of our methodology. The results of the analysis are presented in Table 3.

**TABLE 3. Matrix of Paired Correlation Coefficients.**

| Standards | NIST 800-30 | ISO/IEC TR 13335-3:1998 | BS 7799 | ISREFES | Expert |
|---|---|---|---|---|---|
| NIST 800-30 | 1 | 0,9874 | 0,9833 | 0,9965 | 0,9996 |
| ISO/IEC TR 13335-3:1998 | 0,9874 | 1 | 0,9983 | 0,9970 | 0,9894 |
| BS 7799 | 0,9833 | 0,9983 | 1 | 0,9946 | 0,9850 |
| ISREFES | 0,9965 | 0,9970 | 0,9946 | 1 | 0,9974 |
| Expert | 0,9996 | 0,9894 | 0,9850 | 0,9974 | 1 |

ISREFES showed the strongest positive correlation with NIST 800-30, ISO/IEC TR 13335-3:1998, BS, Expert. The other evaluation techniques, however, have only one high correlation greater than 0.99 if ISREFES is excluded from the sample.

Explore Table 2 using a statistical hypothesis test. The point of testing is to draw a strong inference about a certain property of the general population from the available sample of data. A strong inference is some statement with a probability close to unity.

Assume that the value of the general average is equal to the value of ISREFES. The following conditions are given:

$\mu$ *- is the general average, which is equal to ISREFES.*

*n - number of techniques, not including ISREFES, equal to 4, NIST 800-30, ISO/IEC TR 13335-3:1998, BS 7799, Expert.*

$X_{avg}$ *- arithmetic mean.*

*s - root mean square deviation.*

$t_{fact}$ *- t-criterion.*

$\alpha$ *- the significance level, equal to 0,05, 5% probability of error.*

*d.f. - the number of degrees of freedom, equal to 3.*

$t_{crit}$ *- critical value of the t-criterion, two-way inverse Student's t-distribution.*

*p-value - a measure of the probability that an observed difference could have occurred just by random chance, two-sided Student's t-distribution.*

The question is whether the sample data is consistent with the hypothesis that the overall mean is equal to ISREFES. In conventional terms it looks like $H_0 : \mu =$ *ISREFES.*

$H_a : \mu \neq$ *ISREFES.*

The general approach to any statistical hypothesis testing is that we cannot prove the tested hypothesis. We can only refute it. Here the object of the study is not to confirm the standards, but to look for evidence of deviation from them. That is, the so-called alternative hypothesis. In our case, the alternative hypothesis is that the general mean does not equal ISREFES. $H_a : \mu \neq$ *ISREFES*. The calculations are shown in Table 4. t-criterion was in the range -0.07758≤$t_{fact}$ ≥0.064225.

The question is whether this is a lot or a little, good or bad? In other words, is it possible to say that the sample mean ($X_{avg}$) and the general mean (ISREFES) are close enough to

**TABLE 4.** Statistical Test for Comparing the Means to Evaluations LMS.

| LMS | μ | $X_{avg}$ | s | $t_{fact}$ | tcrit | p-value |
|---|---|---|---|---|---|---|
| ENU | 0,293 | 0,29075 | 0,089300392 | -0,05039 | 3,182446 | 0,962977675 |
| KazGUU | 0,741 | 0,74025 | 0,038013682 | -0,03946 | 3,182446 | 0,971003166 |
| EKTU | 0,642 | 0,64325 | 0,03892557 | 0,064225 | 3,182446 | 0,952830992 |
| KazNU | 0,857 | 0,85775 | 0,037130042 | 0,040399 | 3,182446 | 0,970313578 |
| KSU | 0,45 | 0,4485 | 0,038669885 | -0,07758 | 3,182446 | 0,94304686 |
| Aitu | 0,547 | 0,548 | 0,036891191 | 0,054213 | 3,182446 | 0,960173393 |

**TABLE 5.** Statistical Test With a Sample Number of Up to 30.

| LMS | μ | $X_{avg}$ | s | $t_{fact}$ | tcrit | p-value |
|---|---|---|---|---|---|---|
| ENU | 0,293 | 0,29075 | 0,089300392 | -0,138 | 2,04523 | 0,891191515 |
| KazGUU | 0,741 | 0,74025 | 0,038013682 | -0,10806 | 2,04523 | 0,914688961 |
| EKTU | 0,642 | 0,64325 | 0,03892557 | 0,175888 | 2,04523 | 0,861604572 |
| KazNU | 0,857 | 0,85775 | 0,037130042 | 0,110636 | 2,04523 | 0,912667138 |
| KSU | 0,45 | 0,4485 | 0,038669885 | -0,21246 | 2,04523 | 0,833233821 |
| Aitu | 0,547 | 0,548 | 0,036891191 | 0,14847 | 2,04523 | 0,882999653 |

consider the difference between them to be random? Or was the t-test too high, and the difference between the means does not fall within the range of possible random deviation? To answer these questions it was helpful to compare the observed criterion with the critical level, which cuts off the unlikely event. The observed value of the t-criterion is less than the critical value, which can be clearly seen in the table. The observed t-criterion falls into the hypothesis acceptance zone. Or in other words to the place where such deviation from the general average for a given sample size and significance level is frequent. Therefore, if the observed criterion is less than the critical one, the null hypothesis is not rejected, which does not mean it is proved. However, the t-criterion is quite far from the critical region.

But could there be a difference between the averages after all? Perhaps we just didn't detect it? We tested the same hypothesis another way, with a p-value. The p-value is the probability of obtaining an observed or even larger criterion, provided that the null hypothesis is true. The p-value is greater than the given level of significance. The null hypothesis cannot be rejected because the p-value is greater than 0,05. At this significance level and sample size, we do not reject the null hypothesis, although we do not prove it. For the test, we will artificially increase the number of samples to 30. $n= 30$, $d.f. = 29$. The calculation data is shown in Table 5.

Increasing the sample reduced the variance of the mean and hence increased the sensitivity of the criterion. By increasing the number of degrees of freedom to 29, the scatter of the criterion narrowed considerably, i.e. it became more powerful. And the sample mean, while unchanged, did not fall within the critical range. The p-value remained quite large. The null hypothesis that the sample and the general mean are equal is not rejected. We conclude statistically that the ISREFES methodology is correct. The main thing is to use the concept of "risk" as the main indicator. Also, the sense of Risk is divided into Organizational risks, Reputation (branding) risks, Privacy risks, Integrity risks, Availability risks at the level of being. Fuzziness gives the very flexibility in impact characteristics, removed the coefficients robustness of influence on the final estimate.

## V. CONCLUSION

This paper proposes a new method of information security risk assessment. The method is based on fuzzy logic using the Mamdani algorithm. The constructed fuzzy expert system has an extended classification of risk assessment criteria, which is based on the analysis of the above-mentioned standards. On the basis of interdisciplinary analysis (the above-mentioned studies and standards) the list consisting of 50 IS risks, which can be used in the practical activities of the enterprise, since the neutralization (elimination, minimization) of IS risks is the essence and content of the process of ensuring IS of the enterprise. On the basis of the offered list it is also possible to build models of threats, on the basis of which the tasks of creation of ISS are made. In addition, the list of specific risks can be used in the assessment of the impact of the IS measures taken on the effectiveness of the enterprise. This fuzzy method makes the calculations flexible, since the number of parameters, rigidly defined at the initial stage, is constantly increasing. The results and conclusion of the experiments confirm the correctness of the developed method. ISREFES showed a result $> 0.99$, the strongest positive correlation with NIST 800-30, ISO/IEC TR 13335-3:1998, BS, Expert. The other evaluation techniques, however, have only one high correlation greater than 0.99 if ISREFES is excluded from the sample. Ambiguity adds flexibility to the evaluation. This methodology can be used to assess the information security risks of any complex (socially significant ERP system) automated management system used in other areas, such as the banking sector, medical information systems, etc. The only disadvantage of these methods is the high labor intensity of experts in the evaluation.

## REFERENCES

[1] B. Feng, Q. Li, Y. Ji, D. Guo, and X. Meng, "Stopping the cyberattack in the early stage: Assessing the security risks of social network users," *Secur. Commun. Netw.*, vol. 2019, pp. 1–14, Jul. 2019.

[2] P. S. Woo, S. S. Hwang, S. H. Hwang, and B. H. Kim, "Risk assessment for the security of power information control systems," *Int. J. Smart Grid Clean Energy*, vol. 8, no. 4, pp. 488–494, 2019.

[3] T. Kieras, M. J. Farooq, and Q. Zhu, "RIoTS: Risk analysis of IoT supply chain threats," in *Proc. IEEE 6th World Forum Internet Things (WF-IoT)*, Jun. 2020, Art. no. 9221323.

[4] M. Shrestha, C. Johansen, J. Noll, and D. Roverso, "A methodology for security classification applied to smart grid infrastructures," *Int. J. Crit. Infrastruct. Protection*, vol. 28, Mar. 2020, Art. no. 100342.

[5] J. D. Markovic-Petrovic, M. D. Stojanovic, and S. Rakas, "A fuzzy AHP approach for security risk assessment in SCADA networks," *Adv. Elect. Comput. Eng.*, vol. 19, no. 3, pp. 69–74, 2019.

[6] W. Wang, F. Shi, M. Zhang, C. Xu, and J. Zheng, "A vulnerability risk assessment method based on heterogeneous information network," *IEEE Access*, vol. 8, pp. 148315–148330, 2020.

[7] J. Wang, M. Neil, and N. Fenton, "A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model," *Comput. Secur.*, vol. 89, Feb. 2020, Art. no. 101659.

[8] Y. Alemami, M. A. Mohamed, and S. Atiewi, "Research on various cryptography techniques," *Int. J. Recent Technol. Eng.*, vol. 8, no. S3, pp. 395–405, 2019.

[9] Y. Movahedi, M. Cukier, A. Andongabo, and I. Gashi, "Cluster-based vulnerability assessment of operating systems and web browsers," *Computing*, vol. 101, no. 2, pp. 139–160, Feb. 2019.

[10] K. Pan, A. Teixeira, C. D. Lopez, and P. Palensky, "Co-simulation for cyber security analysis: Data attacks against energy management system," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Oct. 2017, pp. 253–258.

[11] O. F. Keskin, K. M. Caramancion, I. Tatar, O. Raza, and U. Tatar, "Cyber third-party risk management: A comparison of non-intrusive risk scoring reports," *Electronics*, vol. 10, no. 10, p. 1168, May 2021.

[12] L. Lv, H. Li, L. Wang, Q. Xia, and L. Ji, "Failure mode and effect analysis (FMEA) with extended MULTIMOORA method based on interval-valued intuitionistic fuzzy set: Application in operational risk evaluation for infrastructure," *Information*, vol. 10, no. 10, p. 313, Oct. 2019.

[13] S. Oukemeni, H. Rifa-Pous, and J. M. Marques Puig, "IPAM: Information privacy assessment metric in microblogging online social networks," *IEEE Access*, vol. 7, pp. 114817–114836, 2019.

[14] S. Parkinson, M. Vallati, A. Crampton, and S. Sohrabi, "GraphBAD: A general technique for anomaly detection in security information and event management," *Concurrency Comput., Pract. Exper.*, vol. 30, no. 16, Aug. 2018, Art. no. e4433.

[15] A. M. Algarni, V. Thayananthan, and Y. K. Malaiya, "Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems," *Appl. Sci.*, vol. 11, no. 8, p. 3678, Apr. 2021.

[16] M. A. Fikri, F. A. Putra, Y. Suryanto, and K. Ramli, "Risk assessment using NIST SP 800-30 revision 1 and ISO 27005 combination technique in profit-based organization: Case study of ZZZ information system application in ABC agency," *Proc. Comput. Sci.*, vol. 161, pp. 1206–1215, Jan. 2019.

[17] M. I. Tariq, S. Ahmed, N. A. Memon, S. Tayyaba, M. W. Ashraf, M. Nazir, A. Hussain, V. E. Balas, and M. M. Balas, "Prioritization of information security controls through fuzzy AHP for cloud computing networks and wireless sensor networks," *Sensors*, vol. 20, no. 5, p. 1310, Feb. 2020.

[18] J. Zuo, Y. Lu, H. Gao, R. Cao, Z. Guo, and J. Feng, "Comprehensive information security evaluation model based on multi-level decomposition feedback for IoT," *Comput., Mater. Continua*, vol. 65, no. 1, pp. 683–704, 2020.

[19] M. I. Tariq, "Agent based information security framework for hybrid cloud computing," *KSII Trans. Internet Inf. Syst.*, vol. 13, no. 1, pp. 406–434, 2019.

[20] O. F. Kececioglu, A. Gani, and M. Sekkeli, "Design and hardware implementation based on hybrid structure for MPPT of PV system using an interval type-2 TSK fuzzy logic controller," *Energies*, vol. 13, no. 7, p. 1842, Apr. 2020.

[21] H. Acikgoz, O. F. Kececioglu, A. Gani, M. Tekin, and M. Sekkeli, "Robust control of shunt active power filter using interval type-2 fuzzy logic controller for power quality improvement," *Tech. Gazette*, vol. 24, no. 2, pp. 363–368 Sep. 2017.

[22] A. Barlybayev, Z. Kaderkeyeva, G. Bekmanova, A. Sharipbay, A. Omarbekova, and S. Altynbek, "Intelligent system for evaluating the level of formation of professional competencies of students," *IEEE Access*, vol. 8, pp. 58829–58835, 2020.

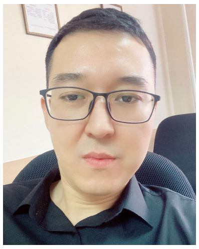
[23] A. S. Abdygalievich, A. Barlybayev, and K. B. Amanzholovich, "Quality evaluation fuzzy method of automated control systems on the LMS example," *IEEE Access*, vol. 7, pp. 138000–138010, 2019.

[24] B. B. Orazbayev, Z. Y. Shangitova, K. N. Orazbayeva, B. A. Serimbetov, and A. B. Shagayeva, "Studying the dependence of the performance efficiency of a claus reactor on technological factors with the quality evaluation of sulfur on the basis of fuzzy information," *Theor. Found. Chem. Eng.*, vol. 54, no. 6, pp. 1235–1241, Nov. 2020.

**S. A. ABDYMANAPOV** was born in Krasnogorskiy (now Kordayskiy), Zhambyl, Kazakhstan, in 1949. He received the degree in mathematics from the Mechanical-Mathematical Faculty, Kazakh State University named after S. M. Kirov (now the Kazakh National University named after Al-Farabi), Almaty, in 1972, and the master's degree from the Institute of Mathematics and Mechanics, Academy of Sciences, Kazakh Soviet Socialist Republic, Almaty, in 1979. He was an Assistant with the Chair of the Differential and Integrated Equations, Mathematical Faculty, Karaganda State University (KSU), Karaganda, from 1972 to 1976. He was a Teacher and a Senior Teacher of the Chair of Differential and Integrated Equations, Mathematical Faculty, KSU, from 1976 to 1986. He defended the dissertation on the specialty "the differential equations and the mathematical physics on the theme 'resolvability of some problems for the general differential equation of elliptic type of the fourth order in fractional spaces'" with the Institute of Mathematics and Mechanics, Academy of Sciences, Kazakh Soviet Socialist Republic, in 1982. His academic status was promoted as a Senior Lecturer of the Chair of the Differential and Integrated Equations by the Higher Certifying Commission, USSR, in 1986. He was a Senior Lecturer of the Chair of Differential and Integrated Equations, Mathematical Faculty, KSU, from 1986 to 1990, where he was the Chairman, from 1990 to 1992. He was the Dean of the Mathematical Faculty, Karaganda State University named after E. A. Buketov, from 1992 to 1993. He was the Pro-Rector on study of the Karaganda State University named after E. A. Buketov, from 1993 to 2000. He was a Correspondent Member of the International Informatization Academy, in 1995. He was an Academician (member) of the International Academy of Ecology, Man and Nature Protection Sciences, in 1996. His academic status was appropriated as a Professor in mathematics by the decision of the Higher Certifying Commission, Cabinet of Ministers, Republic of Kazakhstan, in 1997. He was a Correspondent Member of the International Higher Education Academy of Sciences, Saint Petersburg, in 1997. He successfully defended the dissertation for scientific degree of doctor of pedagogical sciences on a specialty "the general pedagogy on the theme 'the theory and practice of perfection of university education,"' Almaty, in 1999. He acquired the scientific degree of doctor of pedagogical sciences by the decision of the Presidium of the Higher Certifying Commission, Ministry of Science and Higher Education, Republic of Kazakhstan, in 2000. He was a first Pro-Rector of the Republican State Enterprise, L. N. Gumilyov Eurasian National University, Astana, from 2000 to 2004. He was a Full Member (academician) of the International Informatization Academy, in 2001. He created the Scientific-Research Institute on the problems of higher education, L. N. Gumilyov Eurasian National University, in 2001. He became a Full Member and an Academician of the International Higher Education Academy of Sciences, in 2001. He was selected as a member of the Royal Academy of Doctors, Spain, in 2004. He was a Rector of the L. N. Gumilyov Eurasian National University, from 2004 to 2008. He was the Chairman of the Republican Council, Rectors of Higher Schools, Kazakhstan; a member of the Republican Educational-Methodological Council, Higher and Postgraduate Education, Ministry of Education and Science, Republic of Kazakhstan; and a Board Member of the Ministry of Education and Science, Republic of Kazakhstan, from 2004 to 2008. He was a Chairman of the Section of Public and Humanitarian Sciences, Commission on the State awards in the field of science, technologies, and education of the Government of the Republic of Kazakhstan, from 2005 to 2006. He was a member of the Commission Concerning Free Pardon Issues by the President of the Republic of Kazakhstan, The National Commission on UNESCO Affairs, Republican Scientific and Technical Council, Ministry of Education and Science, Republic of Kazakhstan, from 2005 to 2008. He was the Chairman of the Board of Directors of the Kazakh–Chinese Institute of Confucius and the Vice-President of the Association of Assistance to the United Nations in the Republic of Kazakhstan, from 2006 to 2008. He was the President and a member of the Board of Directors of the joint-stock company Akmola Financial and Economic College (JSC AFEC), Astana, from 2008 to 2009. He was a member of the Board of Directors and the Chairman of the Board (Rector) of the joint-stock company Financial Academy, from 2009 to 2012. Since 2012, he has been a Rector with the Kazakh University of Economics, Finance and International Trade.

**M. MURATBEKOV** received the Candidate of Mathematical and Physical Sciences degree in differential equations and mathematical physics, in 2001, and the Ph.D. degree in mathematics at Berlin, Germany, in 2008. He is currently the Director of the Center of Information Technologies, Kazakh University of Economics, Finance and International Trade, Nur-Sultan, Kazakhstan. He is also productively engaged in research work with students and undergraduates. Since 2012, he has been the Head and a member of the working group in the performance of the contracts: Head of the scientific project ‘‘Development of PKI software system for the Certifying Authority on the basis of the newest modern cryptoalgorithms’’; the Senior Research Associate in the project ‘‘Development of mathematical model of recognition of Kazakh language hand writer text and its program realization’’; the Leading Research Associate in the project ‘‘Develop information and software unit to simulate potential disaster on water objects of Kazakhstan for space monitoring system’’; and the Senior Research Associate in the project. He has more than 40 scientific articles whose main results are published in scientific editions, and materials of the international scientific conferences.

**S. ALTYNBEK** received the B.S. and M.S. degrees in mathematical area from Al-Farabi Kazakh National University, Almaty, in 2004, and the Ph.D. degree in mathematics from Free Berlin University, Germany, in 2008. From 2004 to 2019, he was a Senior Lecturer and an Associate Professor with the Department of Computer Science and Information Security, L. N. Gumilyov Eurasian National University, Nur-Sultan, Kazakhstan. Since 2008, he was a Senior Researcher in four scientific projects. Since 2019, he has been the Head of the Maintenance and Repair Department, Kazakh University of Economics, Finance and International Trade, Nur-Sultan. He is the author of more than 40 articles. His research interests include e-learning, cryptology, neural networks, and mathematical modeling of physical process.



**A. BARLYBAYEV** was born in 1987. He received the bachelor's degree in information systems from the Faculty of Mathematics and Information Technology, L. N. Gumilyov Eurasian National University, with the thesis of development of workstation automated work station, in 2009, the master's degree in computer science from the Faculty of Information Technologies, L. N. Gumilyov Eurasian National University, with the dissertation of development of educational portal for universities, in 2011, and the Ph.D. degree in computer science from the Faculty of Information Technologies, L. N. Gumilyov Eurasian National University, with the dissertation of models and algorithms of intelligent e-learning, in 2014. He is currently the Head of the Software Development Department, Kazakh University of Economics, Finance and International Trade.