

**REPUBLIC OF AZERBAIJAN**

*On the rights of the manuscript*

**ABSTRACT**

of the dissertation for the degree of Doctor of Science

**MODELS AND METHODS OF E-GOVERNMENT  
INFORMATION SECURITY MANAGEMENT**

Speciality: 3338.01 – System analysis, management and processing  
of information

Field of science: Technical sciences

Applicant: **Yadigar Nasib oglu Imamverdiyev**

**Baku – 2021**

The work was performed at the Institute of Information Technology of Azerbaijan National Academy of Sciences (ANAS).

Scientific consultant: Full member of ANAS, Doctor of technical sciences, Prof.  
**Rasim Mahammad oglu Alguliyev**

Official opponents: Doctor of technical sciences, Prof.  
**Nadir Bafadin oglu Agayev**  
Doctor of technical sciences, Assoc. Prof.  
**Lala Mehdi gizi Zeynalova**  
Doctor of technical sciences, Prof.  
**Ramin Rza oglu Rzayev**  
Doctor of technical sciences, Prof.  
**Javanshir Firudin oglu Mammadov**

Dissertation council ED 1.35 of Supreme Attestation Commission under the President of the Republic of Azerbaijan operating at the Institute of Information Technology of ANAS

Chairman of the Dissertation council: Full member of ANAS,  
Doctor of technical sciences, Prof.  
**Rasim Mahammad oglu Alguliyev**

Scientific secretary of the Dissertation council: Doctor of Philosophy in Technical Sciences,  
Assoc. prof.  
**Farhad Firudin oglu Yusifov**

Chairman of the scientific seminar: Doctor of technical sciences  
**Mutallim Mirzaahmed oglu Mutallimov**

## GENERAL DESCRIPTION OF WORK

**Relevance of work.** Currently, information and communication technologies (ICT) penetrate deeper and deeper into all spheres of society. As a result, humanity is entering a new phase of development - the era of the formation of the information society. The widespread use of ICTs in state and local governments in order to optimize government processes contributes to the creation of an electronic state (e-government), which is an important milestone in the formation of the information society. In the e-government, citizens are increasingly involved in the development and implementation of public policy, an effective system of interaction and cooperation between the state, the private sector and civil society is being created, and the effectiveness of public administration and the quality of public services are being improved.

However, in the field of e-government there are some serious problems that are pending. Information security (IS) has a direct and decisive influence on the effectiveness of the e-government and the trust of citizens in the state. Therefore, one of the most important and complex problems is the reliable provision of information security of the e-government, functioning in the new conditions.

The widespread use of ICT along with the acceleration of human development creates new threats to national, regional and global security.

Interstate contradictions and conflicts pass into cyberspace, and countries form cyber armies participating in information warfare operations in this space<sup>1</sup>.

The information space is by its nature transnational, global and uncontrolled at the national level. The international monopolization of the media (media) and the manipulation of public consciousness are also intensifying.

As a result of errors or accidents in the global information space, disasters of a new type arise - infogenic disasters.

---

<sup>1</sup> Imamverdiyev, Y. N. Cyber troops: functions, weapons and human resources // – Baku: Information society problems, – 2015. №2, – s. 15-25.

The collection of personal data for criminal purposes is widespread, and organized cybercrime is developing.

Thanks to the Internet of Things, the Industrial Internet, the Internet of Services, and artificial intelligence, the Industry 4.0 revolution is taking place, and cyber-physical-social systems are emerging that bring new opportunities and threats.

In connection with the transformation of threats to international security, new concepts of war appear, such as “asymmetric warfare”, “network warfare” and “war without a state”. New strategies are required to deal with asymmetric actors.

Cyber attacks on critical elements of a national information infrastructure are becoming more complex, targeted and widespread and occur frequently. At the same time, politically motivated attacks on government bodies and politicians are also growing. Successfully preventing such attacks is beyond the reach of various organizations and people and requires close cooperation between all stakeholders, including the private sector and civil society.

Thus, in an environment of comprehensive globalization and the threats it poses, in the face of uncertainty and increasing risks of cybersecurity to public processes, information security is one of the key functions of e-government self-defense. Therefore, managing the processes of ensuring IS of the e-government is an urgent interdisciplinary problem, and its solution directly depends on the level of development of corresponding scientific and methodological basis.

The creation of the information society and the e-government in the country, the reliable provision of information security is one of the priority areas of state policy in the Azerbaijan Republic. To implement the state policy in the field of information security in the country, the relevant state bodies systematically carry out the necessary measures to improve the regulatory framework, form the organizational structure of the information security system, develop information security policies, train personnel in the field of information security and conduct research.

Scientific and practical research in the field of information security management of the e-government appeared relatively

recently. At the same time, the e-government information security environment is changing very dynamically, security threats are constantly evolving, and the mechanisms of cyber attacks and defense are being updated. Rapid response to emerging new IS challenges requires improving approaches to IS management, and the development of new models and management methods.

Based on the foregoing, this dissertation is devoted to the problems of developing the scientific and methodological foundations of e-government information security management.

**Purpose and objectives of the work.** The aim of the dissertation thesis is the development of methods and models for the development and improvement of scientific, theoretical and methodological foundations of e-government information management.

To achieve this goal, the following **problems** are solved:

- development of a conceptual model for managing e-government information security;
- development of methods for assessing strategic threats and critical risks of e-government information security;
- development of methods for improving e-government biometric identification system;
- development of methods for detecting and effectively managing information security incidents;
- development of coordination models between state, civil and international actors involved in e-government information security;
- development of decision-making models at different levels of e-government information security management;
- development of methods and models for assessing e-government information security level..

**Research methods.** When solving the problems posed in the work, we used control theory, decision theory, fuzzy control theory, game theory, probability theory and mathematical statistics, combinatorial optimization, graph theory, social networks analysis, machine learning methods.

**Key Points to defend:**

- conceptual model of managing e-government information security;
- a method of consensus ranking of threats to national interests in the information sphere of e-government;
- risk assessment method in interconnected information infrastructures of e-government;
- models for assessing the survivability of a national Internet infrastructure;
- methods for improving recognition performance and security of biometric systems and the synthesis of biometric cryptosystems;
- a method of detecting DDoS attacks based on deep learning;
- a method for optimal planning of information security incident handling;
- coordination models in the field of e-government information security;
- models of strategic, tactical and operational management of e-government information security;
- methods and models for assessing e-government information security level.

**Scientific novelty** of the research and the results obtained in the thesis is as follows:

- development of a consensus ranking method of threats to national interests in the information sphere based on assessments of experts representing the political and intellectual elite;
- development of methods and models for assessing risks and survivability of the national Internet infrastructure in the interconnected information infrastructure of e-government;
- development of methods for improving e-government biometric authentication systems and approaches to the synthesis of biometric cryptosystems;
- development of methods and algorithms for detecting information security incidents, and multi-criteria prioritization and optimal planning of their processing;

- development of a model for the coordination of investments in a two-level hierarchical information security system of e-government;
- development of a model for the formation of international coalitions in the field of information security;
- development of mathematical and conceptual models for managing e-government information security at the strategic, tactical and operational levels;
- development of models for evaluating the e-government information security for direct (e-services) and feedback (citizens' trust).

**The practical value of the work.** The practical significance of the work is due to the fact that the obtained scientific and theoretical results can be used in the following areas:

- development of proposals for national policies, strategies and programs in the information security field;
- in intelligent support systems for strategic decision making on information security;
- in cyber attack detection systems;
- in situational centers that manage information security in real time;
- in the national biometric identification system;
- in interagency coordination centres for information security.

### **Implementation and application of the thesis results.**

The main results were obtained by the author during carrying out research in the framework of “The State Program on the creation of a biometric identification system in the Republic of Azerbaijan for 2007-2012”, as part of the fundamental research of the Azerbaijan National Academy of Sciences on the theme “Development of scientific and theoretical foundations for the creation, management and maintenance of e-government information security”, in the framework of the grant projects “Testing Security of Biometric Systems” of the US Civilian Research and Development Foundation, “Creating a Biometric Cryptosystem” National Science Foundation of the Republic of Korea, “Development of robust approaches for identification of person's voice”, and "Development of methods and

algorithms for information security in Big Data environment and some of their applications", funded by the Science Development Fund under the President of Azerbaijan Republic.

The main theoretical and practical results of the dissertation were used in the design and operation of security systems of the scientific computer network AzScienceNet of Azerbaijan National Academy of Sciences, about which there are relevant supporting documents.

**Work approbation.** The main scientific, theoretical and practical results of the work were reported and discussed at the next conferences:

- The 1st, 2nd, 3rd International Conference “Problems of Cybernetics and Informatics”, Baku, 2006, 2008, 2010;
- The 6th International Conference on Information Security and Cryptology (ISCTurkey), Ankara, 2013;
- The 2nd Republican Scientific and Practical Conference on Multi-disciplinary Problems of Information Security, Baku, 2015;
- IEEE International Conference on Application of Information and Communication Technologies (AICT), Baku, 2009, 2013, 2016;
- The 2nd International Conference on Information Security and Computer Technologies, Kropyvnytskyi (Ukraine), 2017;
- The 3rd Republican Scientific and Practical Seminar on Information Security, Baku, 2017.

**Publications.** On the topic of the dissertation, 33 scientific papers were published, including 22 articles in advanced scientific and practical journals and 11 articles at international and national conferences.

**Structure and scope of the work.** The dissertation consists of an introduction, seven chapters, conclusion, and a list of used literature from 313 titles. The main content of the work is presented on 246 pages, including 40 figures and 45 tables.

## **CONTENT OF THE WORK**

**The introduction** substantiates the relevance of the dissertation topic, defines purpose of the study and problems to be solved,



demonstrates the scientific novelty and practical significance of the results.

**The first chapter** is devoted to the analysis and research of the scientific and theoretical problems of e-government IS management. E-government information security management belongs to the class of hard-to-formulate problems: the management object is a complex socio-technical system that consists of autonomous components, each of which has purposeful functioning, and many processes take place in them (political, legal, social, technological, etc.), which influence each other and between them there are very complex causal relationships. The nature of the processes changes dynamically over time, and there is not enough quantitative information about the dynamics of processes, there are various types of uncertainties, etc.

Creating a conceptual model as an initial step is very useful in solving such difficult formalized complex problems. To this end, a conceptual model was proposed that defines the goals and key functions of e-government information security management [6, 9]. The dissertation identifies the following main management functions: assessment of threats and risks, authentication of e-service users, information security monitoring and incident handling, coordination of information security activities, management decision-making and assessment of the information security level.

Further, in accordance with this conceptual model, the urgent problems of research on the main functions of e-government IS management were identified and their current state was analyzed [8].

Finally, the priority areas of research on the management of information security of the e-government are identified, which are discussed in detail in the thesis.

**In the second chapter**, methods and models for assessing the risks of e-government information security are developed.

The strategic risks of e-government information security are aimed at national interests in the field of information. There are many such threats, and in order to effectively respond to these threats in the context of limited resources allocated for providing information security, it is necessary to conduct multi-criteria consensus ranking of these threats [21, 28].

Suppose that a list of  $n$  e-government information security threats  $A_i$  ( $i = 1, 2, \dots, n$ ) has been compiled (based on official documents, scientific studies, expert opinions and media reports, etc). Let  $p$  experts  $DM_k$  ( $k = 1, 2, \dots, p$ ) are selected, and each expert should evaluate each threat from the list with respect to  $m$  criteria  $C_j$  ( $j = 1, 2, \dots, m$ ). Experts give higher ratings to threats that, in their opinion, are more likely to be realized and may have a greater impact. Let threat ratings be evaluated on a 6-point scale: 0 – No threat; 1 – Low; 2 – Acceptable; 3 – Medium; 4 – Significant; 5 – High.

The assessment is performed by each expert, and let the matrix of estimates be  $\mathbf{X}^k = (X_{ij}^k)_{n \times m}$   $k = 1, 2, \dots, p$ . Each decision matrix is first normalized to reduce the impact of large estimates. Normalization is performed for each criterion  $j$  according to the following rule (for simplicity, the superscript  $k$  of the elements  $x_{ij}^k$  is omitted)

$$x_{ij} = \frac{X_{ij}}{\sum_{i=1}^n X_{ij}} \quad (1)$$

Based on these expert assessments, it is required to determine the weight of the criteria for each expert ( $w^C = (w_1^C, w_2^C, \dots, w_m^C)$ ), evaluate the alternatives ( $A'_1 > A'_2 > \dots > A'_n$ ), assign weights to experts ( $w = (w_1, w_2, \dots, w_p)$ ) and make the final consensus decision on the ranks of the threats ( $r^* = (r_1, r_2, \dots, r_n)$ ). The problem of weighted consensus ranking in general can be expressed in the following form.

Let  $\mathbf{r}_i = (r_{i1}, r_{i2}, \dots, r_{in})$  be the threat rank vector specified by the  $i$ -th expert ( $i = 1, \dots, p$ ), where  $r_{ij}$  is the rank of the  $j$ -th threat given by the  $i$ -th expert ( $j = 1, \dots, n$ ). The problem is to assign an individual weight  $w_i$  to each expert, and to find a weighted consensus threat rank  $\mathbf{r}^*$ . The goal is to minimize the distance between  $\mathbf{r}^*$  and all  $\mathbf{r}_i$ . If  $\mathbf{w} = (w_1, w_2, \dots, w_p)$  is the vector of weights assigned to experts, then the weighted consensus ranking problem can be expressed as the following optimization problem:

$$\operatorname{argmin}_{\mathbf{w}, \mathbf{r}^*} (1 - \lambda) \sum_{i=1}^p w_i \|\mathbf{r}^* - \mathbf{r}_i\|^2 + \lambda \|\mathbf{w}\|^2, \quad (2)$$

$$\text{Ограничения: } \sum_{i=1}^p w_i = 1, w_i \geq 0, \forall i, \quad (3)$$

where  $0 \leq \lambda \leq 1$  is a regularization parameter that controls the tradeoff between minimizing the weighted distance and the smoothness of the balance. To measure the inconsistency between the consensus ranking  $\mathbf{r}^*$  and the individual expert ranking  $\mathbf{r}_i$ , the Euclidean distance is used for simplicity. Therefore,  $w_i \|\mathbf{r}^* - \mathbf{r}_i\|^2$  measures the distance between the rank vector of the  $i$ th expert  $\mathbf{r}_i$  and the consensus rank  $\mathbf{r}^*$ , and the first term in (2) is used to minimize this distance for each expert, and the second term is a regularization parameter providing smoothness of weights.

Problem (2)-(3) is a quadratic function optimization problem with linear constraints, and existing algorithms could be used to solve it.

The e-government information infrastructure (II) consists of critical information infrastructures (CII) with strong interdependencies. As the e-government develops, these interdependencies become even stronger, which improves the quality of e-services. But these interdependencies also represent one of the most serious threats to e-government information security. The disruption of any of these infrastructures can have disastrous consequences for the entire e-government ecosystem. In existing methods, IS risks are assessed for individual infrastructures and, as a rule, do not take into account the interdependence of infrastructures.

Taking into account the above arguments, to assess risks in interdependent CII, a two-level hierarchical model of e-government interdependencies, a method for assessing IS risks in interdependent CII, and an approach to modeling extreme risks were developed [31].

In the two-level hierarchical model of interdependencies of the e-government at the low level of the hierarchy are CII operators (CIIO), and at the upper level, there is a national operator of e-government (NOEG). The connection between the CIIO and the NOEG is carried out through the appropriate Coordinator; it acts as the interface between them.

It is assumed that each CIIO conducts a general assessment of risks in the CII and, thus, determines its first-order

interdependencies. Since these interdependencies are known, it is expected that each CIIO will evaluate its input risks, i.e. potential risks associated with IS events in other infrastructures.

The NOEG is interested in protecting all e-government infrastructures. He receives information from each CIIO about dependency trees from the corresponding coordinator. The NOEG combines these data and creates a complete picture of the dependencies between the different CIIO; it gives a more macroscopic view at the national level. At the NOEG level, the input risks of the CIIO are analyzed to identify and confirm the dependencies between them, as well as to assess the impact of incidents or threats on the dependent CII.

Let a certain CII require an assessment of the risk of an event of type  $j$ . Suppose that data over a certain period of time about the frequency of  $j$ -type risk events and the amount of losses in infrastructures from these events are known by NOEG. These data allow the use of the Loss Distribution Approach (LDA) approach for risk assessment. An LDA application consists of modeling the frequency and volume of losses, and then combining them to calculate the total loss. Suppose that the NOEG has defined a list of dependent infrastructures for a given combination of “KII/Risk event”. Denote them as 1, 2, ...,  $m$ . We introduce the following notation:

- $X_{ij}$  – random value of the volume of losses for the pair  $(i; j)$ ;  $f_{ij}(x)$  is its distribution density function;  $F_{ij}(x) = P(X_{ij} \leq x)$  is its probability distribution function.
- $N_{ij}$  is a random value of the loss frequency for a pair  $(i; j)$ ;  $p_{ij}(k) = P(N_{ij} = k)$  is its distribution density function;  $P_{ij}(n) = P(N_{ij} \leq n)$  is its probability distribution function.

Then the total loss  $L_{ij}$  for the pair  $(i; j)$  is defined as:

$$L_{ij} = \sum_{k=1}^{N_{ij}} X_{ij}(k) = X_{ij}(1) + X_{ij}(2) + \dots + X_{ij}(N_{ij}), \quad (4)$$

where  $X_{ij}(k)$  is the volume of the  $k$ th loss that occurred for the pair  $(i; j)$ .

To simplify the model, the following assumptions are made:

1. The loss frequency  $N_{ij}$  and the loss volume  $X_{ij}$  are independent random variables;
2. The volume of losses  $X_{ij}$  are independent and equally distributed random variables.

The first hypothesis completely excludes the possibility of a correlation between the frequency and volume of losses. The second hypothesis states that two different losses for the same  $(i; j)$  are independent and distributed equally.

Finally, the total loss  $T_j$  for the  $j$ -th type of risk event is calculated as the sum over all dependent infrastructures:

$$T_j = \sum_{i=1}^m L_{ij}. \quad (5)$$

In most cases, it is difficult to obtain an analytical description of the aggregate distribution of losses, and simulation is often used for estimation (Monte Carlo method).

Modeling the loss frequency in the form of a Poisson distribution is considered standard. In the field of information security, it is often assumed that cyber attacks satisfy the properties of the Poisson process, that is, the number of intrusions is well modeled by the Poisson distribution, and the distribution of the interval between intrusions is exponential.

The volume of losses to account for extreme events is described by “heavy-tailed” distributions [13]. Typical probability models used to describe the magnitude of losses are the lognormal, gamma, and Weibull distributions, and the generalized Pareto distribution. Recently, researchers have turned their attention to the lognormal distribution, which allows for more in-depth analytical analysis.

In this study, a database collected by the AzScienceCERT computer incident processing team was used in the experiments to evaluate the parameters of the generalized Pareto distribution [13].

The main line of communication and management in KII is the Internet, and in this regard, the survivability of the national Internet infrastructure (NII) can be considered a very important component of e-government information security. Given this aspect, models are proposed for assessing the survivability of NII against large-scale cyberattacks and accidental accidents [30].

To assess the survivability of NII, appropriate criteria should be selected. The ANSI T1A1.2 Committee defines network survivability as transient performance from the time of an adverse event to the restoration of a stationary state of acceptable performance. In the field of NII, as the performance metrics, you can choose the number of users served per hour, the duration of outages, etc. The proposed survivability models are based on these indicators.

Suppose that the number of providers (national ISPs) serving international transit traffic in NII is  $n$ .  $a_i$  is the relative number of users of the  $i$ -th ISP.  $x_i(t) \in \{0,1\}$  is the state of the  $i$ -th ISP at time  $t$  (1 – normal, 0 – failed). Using these notations, the survivability of NII can be expressed as follows:

$$A(t) = \sum_{i=1}^n a_i x_i(t) \quad (6)$$

Suppose the following ideal case. Suppose that there are transit or peer-to-peer lines between national ISPs, and a special focal point during any large-scale cyberattack or accident dynamically redirects users of temporary ISPs to other ISPs through transit or peer-to-peer lines existing between them. In this case, the survivability of NII can be calculated by the following formula:

$$A(t) = \sum_{i=1}^n a_i x_i(t) + \sum_{i=1}^n \sum_{j \in J_i} (1 - x_i(t)) b_{ij} d_{ij}, \quad (7)$$

where:  $J_i$  is the set of ISPs over which the load of ISP  $i$  is distributed,  $(b_{i,1}, b_{i,2}, \dots, b_{i,k})$  is the load distribution vector for ISP  $i$ ,  $k = |J_i|$  and  $\sum_{j \in J_i} b_{ij} \leq a_i$ . If peering lines exist between ISP  $i$  and  $j$ , then  $d_{ij} = 1$ , otherwise  $d_{ij} = 0$ .

**AI<sup>3</sup> model for assessing survivability.** Let the topology of the national Internet segment with  $C$  providers be given. Let us introduce the following notation:  $N$  is the number of all users of the Internet segment in question;  $K_j$  is number of failures in ISP  $j$  during a predefined long observation period,  $j = 1, \dots, C, k = 1, \dots, K_j$ .  $N_{jk}$  – number of users affected by the  $k$ -th failure in ISP  $j$ ;  $\varphi_{jk}$  – interruption duration (in hours) caused by the  $k$ -th failure that occurred in ISP  $j$ .

**Average Internet Interruption Index (AI<sup>3</sup>)** is an important indicator of the ability of NII to cope with failure recovery, and measures the average impact of Internet service failures on users:

$$AI^3 = \sum_{j=1}^C \sum_{k=1}^{K_j} \varphi_{jk} \frac{N_{jk}}{N} \quad (8)$$

**In the third chapter**, a number of methods were developed to improve the biometric identification system of the e-government.

The biometric identification system forms the basis of the e-government authentication and authorization system and plays an extremely important role in ensuring the security of e-services. However, when creating biometric identification systems nationwide, a number of scientific and practical problems arise. The main problems are the lack of the necessary level of recognition quality and security of existing biometric systems from the point of view of practical use, the low level of interoperability between different systems working with the same biometric modalities, and the difficulty of integrating biometric systems with other IS systems, including cryptographic systems. To solve these problems, an approach is proposed consisting of a biometric model of aggregation of information on the quality of biometric samples in biometric systems [4], a method for detecting altered fingerprints based on fractal characteristics [7] and method for synthesizing biometric cryptosystems [10].

It is known that, biometric systems are characterized by statistical errors of the first and second type. These errors are characterized by coefficients FRR (False Rejection Rate) – percentage of failures when the system denies access to an authorized user; FAR (False Acceptance Rate) – percentage of erroneous accesses when access to the system is erroneously granted to an unauthorized user. Therefore, in any biometric access system, users are interested in the degree to which one can trust that the biometric system has made the right decision. The assessment of confidence in solving a biometric system in the literature is often called the reliability of a decision. Assessing the reliability of a

decision turns a unimodal biometric verification system into a binary classification system (reliable/unreliable, accept/refuse). The problem of assessing the reliability of the decision of a biometric system has recently attracted attention.

Obviously, the reliability of a decision made in a biometric system depends on the quality of the biometric sample. In the proposed approach, assessments of the quality of fingerprint images obtained during registration and submitted for verification are aggregated based on the theory of evidence of Dempster-Schafer and reliability of the biometric system is determined.

In the Dempster-Schafer theory, the subject area is represented by  $\Theta$  a set of complete and mutually exclusive hypotheses, and each hypothesis is associated not with a probability value, but with a probability interval of uncertainty (likelihood). The set of all subsets of the set  $\Theta$ , including the empty set, is denoted by  $2^\Theta$ .

To determine the initial values of evidence reliability, the mass function  $m()$  is used, which is defined on the set  $2^\Theta$  and takes values from the interval  $[0,1]$  and satisfies the conditions:

$$m(\emptyset) = 1; \sum_{A \in 2^\Theta} m(A) = 1. \quad (9)$$

Value  $m(A)$  represents the degree of reliability of evidence, confidence in the validity of hypotheses confirmed by evidence  $A$ . Each subset  $A$  satisfying the condition  $m(A) > 0$  is called a focal element of  $m$ . Based on the basic probabilities, a belief function and plausibility function are determined.

The belief function  $bel(): 2^\Theta \rightarrow [0,1]$  satisfies conditions  $bel(\emptyset) = 0$  and  $bel(\Theta) = 1$ . For any focal element  $A$ , the belief function can be calculated by summing the values  $m()$  over all subsets of  $A$ :

$$bel(A) = \sum_{B|B \subseteq A} m(B) \quad (10)$$

Plausibility function  $pl(A)$  and belief function  $bel()$  are related as follows:  $pl(A) = 1 - bel(\bar{A})$ .

To aggregate image quality estimates in a biometric template, we consider the problem of classification into 2 classes. We denote the



set of classes by  $\Lambda = \{\lambda^{reliable}, \lambda^{non-reliable}\}$ . Suppose that the available information consists of a training sample  $T = \{(x^1, \lambda^1), \dots, (x^N, \lambda^N)\}$ , where  $x^i, i = 1, \dots, N$  are images,  $\lambda^i, i \in \{\text{reliable}, \text{non-reliable}\}$  - labels of the corresponding classes. Suppose that the similarity between images is measured by a certain distance function  $d(\cdot, \cdot)$ .

Let  $x$  be the input image to be classified based on the information contained in  $T$ . Each pair  $(x^i, \lambda^i)$  constitutes a different evidence regarding the class membership of  $x$ . If we consider each image from the training set, then using the Dempster rule we can combine the masses, as a result we get the total confidence regarding the class of the image  $x$ . Since the training images located far from  $x$  provide little information, it is enough to consider  $k$  nearest neighbors of  $x$ , in this case  $m$  will be defined as follows:

$$m = m(\cdot | x^{i_1}) \oplus \dots \oplus m(\cdot | x^{i_k}), \quad (11)$$

where  $I_k = \{i_1, \dots, i_k\}$  - contains indices of  $k$  nearest neighbors of  $x$  in the training set  $T$ .

If the Euclidean distance is used as  $d$ , then the function  $\phi_q$  can be chosen in the form  $\phi_q(d) = \exp(-\gamma_q d^2)$  and for any  $q \in \{\text{reliable}, \text{non-reliable}\}$  formula  $m$  can be represented as

$$m(\{\lambda_q\}) = \frac{1}{K} \left( 1 - \prod_{i \in I_{k,q}} (1 - \alpha \cdot \exp(-\gamma d_i^2)) \right) \prod_{r \neq q} \prod_{i \in I_{k,q}} (1 - \alpha \cdot \exp(-\gamma d_i^2))_r \quad (12)$$

where  $I_{k,q}$  is the subset  $I_k$  corresponding to those neighbors of  $x$  that belong to the class  $\lambda_q$ ,  $K$  is the normalizing factor.

The decision is to assign the image of  $x$  to the class  $K$ , with the largest maximum  $m(\{\lambda_q\})$ , where  $0 < m(\{\lambda_q\}) < 1$ .

Automatic fingerprint identification systems occupy about half of the global market for biometric systems. These systems are based on the assumption that fingerprints are unique and do not change throughout an adult's life. The use of altered fingerprints undermines

these assumptions and poses a threat to the reliability and security of biometric systems.

As a result of artificial changes in fingerprints, new structural elements are formed: scars, areas of destruction of papillary patterns, zones of discontinuous changes in the orientation field of fingerprints, etc. The research hypothesis is based on this observation and proceeds from the ability of fractal analysis to describe in detail the local and global spatial structure of complex systems.

The proposed method for detecting altered fingerprints based on fractal characteristics can be represented as the following sequence of steps:

1. The input image of the fingerprint is pre-processed and normalized.
2. The fractal characteristic is calculated, and on its basis a vector of features is formed.
3. The feature vector is classified using the SVM classifier.

It is proposed to use a feature vector based on the fractal dimension calculated by the modified Katz method, the local scaling exponent, and the multifractal spectrum as fractal characteristics for detecting altered fingerprints.

The general scheme of the biometric cryptosystem proposed for fingerprints includes subsystems of pre-processing of fingerprints; detection of a core (reference) point on a fingerprint; fingerprint image tessalation; extraction of texture features of a fingerprint, including FingerCode and LBP (Local Binary Pattern); discretization of biometric features; aggregation of reliable bits and fuzzy commitment scheme (FCS). FCS uses error correction codes and cryptographic hash functions to hide the cryptographic key in biometric templates.

For texture descriptors of a binary image of fingerprints, a discretization scheme based on reliability was chosen. Due to the low accuracy of texture descriptors, the loss of discriminatory information in discretization schemes, etc., the use of a discrete fingerprint descriptor does not allow creating a biometric cryptosystem with the desired performance. To overcome this problem, a method of aggregation of discretized texture fingerprint

descriptors is proposed. The choice of effective error correction codes is also very important. Aggregation of the most reliable bits from the discretized texture fingerprint descriptors and the use of effective LDPC (Low-Density Parity-Check) codes allow you to create a biometric cryptosystem with the key length and recognition rates required in practice.

To test the performance of the proposed approach, the FVC 2000 DB2a fingerprint database was used, which contains 8 images of each of 100 different fingers. The first five images of each finger are used to create a secure biometric template, and the remaining three images are used for verification.

In table 1, the proposed biometric cryptosystem is compared with other biometric cryptosystems found in the literature.

Table 1. Comparison of the proposed cryptosystem with other systems

Method	Biometric feature	Key length (bits)	GAR (%)	FAR (%)
Hao et al.	Iris	140	99.53	0.0
Zhou et al.	Face	107	99.6	12.0
Maiorana	Hand signature	29	93.05	6.95
Nandakumar et al.	Fingerprint	40	99.98	17.5
Arakala et al.	Fingerprint	34	85.0	15.0
Li et al.	Fingerprint	50	95.15	0.0
Tuyls et al.	Fingerprint	76	94.6	5.2
<b>Proposed</b>	<b>Fingerprint</b>	<b>76</b>	<b>95.3</b>	<b>0.0</b>
		<b>100</b>	<b>92.67</b>	<b>0.0</b>
		<b>120</b>	<b>92.0</b>	<b>0.0</b>
		140	89.33	0.0

The proposed cryptosystem in terms of key length, indicators of FRR and FAR, is superior to other cryptosystems, with the exception of the IrisCode cryptosystem.

**The fourth chapter** discusses methods for managing IT incidents in the e-government environment.

Detection of information security incidents in the e-government environment at an early stage and their elimination as soon as possible with minimal resources is a very important aspect of information security management. Distributed Denial of Service

(DDoS) is one of the most common IS incidents, and despite extensive research, its early detection is still a problem. To detect DDoS attacks, an approach is developed based on one of the architectures of deep neural networks, the so-called Restricted Boltzman Machine (RBM) [24].

RBM is a stochastic network of neurons consisting of two layers: visible and hidden layers. The visible layer describes the data, and the hidden layer examines the features from the visible layer and creates a probability distribution of the data. The network is called restricted because the neurons of one layer are connected only by neurons from other layers. The connection between the layers is symmetrical, and information can be transmitted in both directions.

Three deep learning methods were implemented in the experiments: RBM Bernoulli-Bernoulli, RBM Gauss-Bernoulli, Deep Belief Network and three traditional machine learning methods: SVM (radial basis), SVM ( $\epsilon$ -SVR) and Decision Tree classifiers.

To detect DoS attacks, an RBM network was used, consisting of 7 layers, 100 hidden neurons with randomly selected weights and 38 visible neurons, the activation function was sigmoidal. The experiments were carried out on 5 classes from the NSL-KDD database (38 attributes were used): probe, U2R (User to Root), R2L (Remote to Local), DoS and normal.

Features in the columns were normalized in the interval [0, 1]. 5 epochs were used to train the network. 20% (25 194 samples) of the NSL-KDD-Train data were used for training, and 20% (4508 samples) of the NSL-KDD-Test data were used for testing.

Table 2 presents a comparative analysis of RBM results with traditional classification algorithms for various metrics.

Table 2. Evaluation of the effectiveness of the methods

	F-measure	g-mean	Precision	Recall	TN	TP
SVM (radial basis)	0.7400	0.7173	0.6096	0.9416	0.5464	0.9416
SVM ( $\epsilon$ -SVR)	0.7550	0.7251	0.6139	0.9804	0.5363	0.9804
Decision tree	0.7190	0.6620	0.5710	0.9705	0.4516	0.9705

RBM	0.7530	0.7348	0.6233	0.9509	0.5678	0.9509
-----	--------	--------	--------	--------	--------	--------

To evaluate the results of the experiments, we used metrics Accuracy, F-measure, g-mean, precision, recall, TN (True Negative), TP (True Positive). As can be seen from table 2, the results of the RBM algorithm are superior to the results of other algorithms.

In large information systems, dozens, and sometimes hundreds of IS incidents are detected every day. Information security incident handling is carried out by special teams called CERT (Computer Emergency Response Team). Limited human resources and strict requirements for the timing of response to incidents require prioritization of incidents determining processing sequence of them, which, based on a number of criteria.

In the work, an extended fuzzy AHP is used to prioritize IS incident handling [12].

Let the set of incidents  $X = \{x_1, x_2, \dots, x_m\}$  and the set of criteria  $G = \{g_1, g_2, \dots, g_n\}$  be given. According to the well-known extension analysis, an extension analysis is performed for each criterion  $g_i$ . For each incident  $m$ , the following extension analysis values can be obtained:

$$M_{g_i}^1, M_{g_i}^2, \dots, M_{g_i}^m, i = 1, \dots, n, \quad (13)$$

where all  $M_{g_i}^j (j = 1, \dots, m)$  are triangular fuzzy numbers. The steps of the extension analysis can be expressed as follows:

**Step 1.** A fuzzy synthetic measure regarding the  $i$ -th incident is defined as follows:

$$S_i = \sum_{j=1}^m M_{g_i}^j \otimes [\sum_{i=1}^n \sum_{j=1}^m M_{g_i}^j]^{-1}. \quad (14)$$

**Step 2.** For two triangular fuzzy numbers  $M_1 = (l_1, m_1, u_1)$  and  $M_2 = (l_2, m_2, u_2)$  the degree of possibility of  $M_1 \geq M_2$  is determined as follows:

$$V(M_2 \geq M_1) = \begin{cases} 1, & \text{if } m_2 \geq m_1 \\ 0, & \text{if } l_1 \geq u_2 \\ \frac{l_1 - u_2}{(m_2 - u_2) - (m_1 - l_1)}, & \text{otherwise} \end{cases} \quad (15)$$

**Step 3.** In order to compare  $M_1$  and  $M_2$ , it is necessary to determine both degrees of possibility  $V(M_1 \geq M_2)$  and  $V(M_2 \geq M_1)$ . The degree of possibility that a convex fuzzy number  $M$  is greater than all given  $k$  convex fuzzy numbers  $M_i (i = 1, \dots, k)$  is equal to:

$$\begin{aligned} & V(M \geq M_1, M_2, \dots, M_k) = \\ & = V[(M \geq M_1) \text{ and } (M \geq M_2) \dots \text{and } (M \geq M_k)] = \\ & = \min V(M \geq M_i), i = 1, 2, \dots, k. \end{aligned} \quad (16)$$

Let's assume that,

$$d(A_i) = \min V(S_i \geq S_k), k = 1, 2, \dots, n; k \neq i. \quad (17)$$

Then the weight vector is set as follows:

$$W' = (d'(A_1), d'(A_2), \dots, d'(A_n))^T, \quad (18)$$

where  $A_i (i = 1, \dots, n)$  –  $n$  elements.

**Step 4.** The normalized weight vectors are calculated:

$$W = (d(A_1), d(A_2), \dots, d(A_n))^T, \quad (19)$$

where  $W$  is vector of crisp (real) numbers. Incident priorities are determined based on normalized weight vectors.

The optimal distribution of real-time information security incident processing work between CERT groups is also an urgent problem, and the approach to multi-criteria optimization of incident processing is described below [29]. It is assumed that the CERT service provider receives several requests for processing IS incidents. These requests may come from different security domains. The coordinator of the CERT provider should optimally distribute these requests among its specialized IS incident response teams (CERT groups), in accordance with certain criteria, taking into account some restrictions.

Let the set of incidents  $J_1, J_2, \dots, J_n$  be handled by CERT-groups  $R_1, R_2, \dots, R_m$ . A CERT group can even consist of one person. Processing of incident  $J_i$  consists of  $n_i$  procedures ( $i=1, \dots, n$ ). It is assumed that the incidents are independent of each other and there is no precedence relationship between the procedures of various incidents. And the procedures of one incident form a chain in accordance with precedence relation:  $O_{1j} \rightarrow O_{2j} \rightarrow \dots \rightarrow O_{n_i j}, i = 1, \dots, n$ . Each incident  $J_i$  is associated with directive response time  $d_i$  and weight  $w_i$  (severity level or penalty factor for processing delays).

It is assumed that the planning horizon is divided into equal periods of time, called periods (for example, hours), and the processing times are discrete multiples of a given period. Initiated procedures cannot be stopped, that is, preemption is not allowed. At time  $t = 0$ , all CERT groups are available, and can start processing of any incident. Each procedure can be processed by only one CERT-group.

We introduce the following notation:

$n$  – number of incidents;

$m$  – number of incident response groups (CERT-groups);

$n_i$  – total number of response procedures in the  $i$ -th incident;

$N$  – total number of response procedures,  $N = \sum_{i=1}^n n_i$ ;

$O_{ij}$  –  $j$ -th procedure for responding to the  $i$ -th incident;

$p_{ijk}$  – processing time of the  $O_{ij}$  procedure by the  $k$ -th CERT-group;

$t_{ijk}$  – the start time of the  $O_{ij}$  processing by the  $k$ -th CERT-group;

$t_{ij}^F$  – time of completion of the  $O_{ij}$  procedure;

$i, h$  – incident index,  $i, h = 1, 2, \dots, n$ ;

$k$  – the index of the response groups, where  $k = 1, 2, \dots, m$ ;

$j, g$  – index of response procedures, where  $j, g = 1, 2, \dots, n_i$ ;

$d_i$  – directive response time for the  $i$ -th incident;

$T_i$  – delay time for responding to the  $i$ -th incident;

$w_i$  – weight of the  $i$ -th incident;

$W_k$  – total time spent by the  $k$ -th CERT-group on incident handling;

$x_{ijk} = \begin{cases} 1, & \text{if the } k\text{th CERT group is assigned for procedure } O_{ij}, \\ 0, & \text{otherwise} \end{cases}$

Based on the above notation, the total time  $W_k$  spent by the  $k$ -th CERT-group on incident handling can be expressed as follows:

$$W_k = \sum_{i=1}^n \sum_{j=1}^{n_i} p_{ijk} x_{ijk}, \quad (20)$$

The response delay time  $T_i$  for the  $i$ -th incident is determined as follows:

$$T_i = \max(t_{i,n_i}^F - d_i, 0), \quad (21)$$

Typically, when planning incident handling, you need to consider several criteria. Of course, first of all, it is necessary to minimize the total time spent on handling incidents. However, it is important to split the workload between CERT groups so that the

CERT groups are not overloaded. At the same time, critical incidents should be handled within the deadlines. Based on these comments, for planning of incident handling, a problem of minimization of the following criteria was formulated:

- (1) the total time spent on handling incidents;
- (2) the maximum processing delay time, taking into account the criticality of incidents;
- (3) the maximum time that CERT teams spend on incident handling.

Using the above notation, these criteria can be expressed as follows:

$$\min F_1 = \max_{1 \leq i \leq n} \left\{ \max_{1 \leq j \leq n_i} \{t_{ij}^F\} \right\}, \quad (22)$$

$$\min F_2 = \max_{1 \leq i \leq n} \{w_i T_i\}, \quad (23)$$

$$\min F_3 = \max_{1 \leq k \leq m} \{W_k\}. \quad (24)$$

The model has the following restrictions:

$$t_{ij}^F - t_{i,j-1}^F \geq p_{ijk} x_{ijk}, j = 2, \dots, n_i, \forall i, k \quad (25)$$

$$\begin{aligned} &[(t_{hg}^F - t_{ij}^F - t_{h g k}) x_{h g k} x_{ijk} \geq 0] \\ &\quad \vee [(t_{ij}^F - t_{hg}^F - t_{ijk}) x_{h g k} x_{ijk} \\ &\quad \geq 0], \forall (i, j), (h, g), k \end{aligned} \quad (26)$$

$$\sum_{k=1}^m x_{ijk} = 1, \forall i, j. \quad (27)$$

Condition (26) provides restrictions on the sequence of procedures. (27) states that each CERT group can process only one procedure at any time. (28) indicates that only one response group can be selected to process each procedure.

To solve the multicriteria optimization problem formulated above, the simplest approach was chosen from existing methods – the general objective function is defined as the sum of the above objective functions, assigning each of them the same weight:

$$F = \frac{1}{3} F_1 + \frac{1}{3} F_2 + \frac{1}{3} F_3. \quad (28)$$



**In the fifth chapter**, coordination models are developed in the field of e-government information security management and a system of indicators is proposed for multi-criteria assessment of the coordination system [32], a model for coordinating information security investments in a two-level hierarchical system [25] and an international coalition model for providing information security services [33].

The method of evaluating the coordination system is based on an information approach. Information is a key resource for coordination, and the effectiveness of the entire coordination system depends on its quality, accuracy and timeliness.

Suppose that  $n$  agents are involved in the coordination system for managing the e-government information security, and the agent relationships are described by a graph. The vertices of the graph are agents involved in the coordination system (actors in terms of analysis of social networks), and the edges indicate their relationships. Suppose that the link graph of agents of the coordination network is represented by the incidence matrix  $A = \|a_{ij}\|$ , elements of which are defined as follows:

$$a_{ij} = \begin{cases} 1 - \text{агенты } i \text{ и } j \text{ связаны ребром,} \\ 0 - \text{в противном случае.} \end{cases} \quad (29)$$

The topological structure reflects the degree of interaction or subordination and does not contain any information about the coordination functions and information flows. However, it is possible to reengineer the coordination system and increase its effectiveness by analyzing the topological structure.

In the work, to characterize the efficiency of the coordination system, the degree of inertia of the system is used. Typically, the inertia of a system ( $\Delta\tau$ ) is defined as the delay between the output signal ( $t_{out}$ ) and the input signal ( $t_{in}$ ) of the system ( $\Delta\tau = t_{out} - t_{in}$ ).

Suppose that a certain graph  $G$  is given that describes the coordination system and two numbers are assigned for each of its edges  $(i, j)$ :  $(In_{ij}, Fb_{ij})$ .  $In_{ij}$  is the transfer time of information from  $i$  to  $j$ , and  $Fb_{ij}$  is the reaction time to this information from  $j$  to  $i$ . An

inertia  $K(\mu)$  of any path  $\mu$  is defined as the difference between the total information transfer time along this path  $In(\mu) = \sum_{(i,j) \in \mu} In_{ij}$  and the total feedback transfer time  $Fb(\mu) = \sum_{(i,j) \in \mu} Fb_{ij}$ :

$$K(\mu) = In(\mu) - Fb(\mu). \quad (30)$$

For a given coordination structure, the concept of “inertial diameter” can also be introduced. The diameter of the graph  $d(G)$  is defined as the maximum length of the shortest path connecting its two vertices:

$$d(G) = \max_{a,b \in V(G)} d(a, b), \quad (31)$$

where  $a$  and  $b$  are two arbitrary vertices of the graph,  $V(G)$  is the set of all vertices,  $d(a, b)$  is the distance between the vertices  $a$  and  $b$ . To solve this problem, you can find the shortest paths between all pairs of vertices on the graph using the Floyd-Warshall algorithm (or Bellman-Ford) and select their maximum.

For a response time, policy requirements may be established. If the response does not occur within the directive response time, a penalty mechanism may be provided. Consider the problem of evaluating the efficiency of coordination, taking into account the mechanism of fines. Let two weights be given for each edge  $(i, j)$  of the graph:  $(Out_{ij}, T_{ij})$ . Here  $Out_{ij}$  is the current response time, as indicated above,  $T_{ij}$  is the directive response time. Each path from a given initial actor to the final actor defines a certain information process. In this case, the path length is equal to the sum of the response times along its edges. If the duration of the process in question differs from the previously specified period  $T_{ij}$ , then a penalty  $\chi_{ij}$  is set, proportional to the deviation:

$$\chi_{ij} = \begin{cases} \alpha(T_{ij} - Out_{ij}), & Out_{ij} \leq T_{ij} \\ \beta(T_{ij} - Out_{ij}), & T_{ij} \leq Out_{ij} \end{cases} \quad (32)$$

where the coefficients  $\alpha$  and  $\beta$  can be both positive and negative.

The problem of evaluating the operativeness of the coordination system taking into account fines for delays can be posed as a problem of finding a path that minimizes fines and use the Bellman-Ford algorithm to solve it.

At the upper level of the two-level IS system, there is the Coordinator ( $C_0$ ), and at the lower level there are separate IS domains ( $C_1, \dots, C_n$ ). The coordinator allocates a common budget  $B$  to ensure the security of all domains. Each domain  $i$  informs the Coordinator about its IS level ( $s_i$ ), and asks the Coordinator to allocate a budget (investment)  $x_i \geq 0$  for ensuring and improving IS. The IS level of each domain satisfies the condition  $0 \leq s_i < 1, i = 1, \dots, n$ . It is believed that the greater the value of  $s_i$ , the higher the level of information security. Absolute information security is not expected, therefore  $s_i = 1$  is excluded.  $s_i = 0$  indicates that the information security in the  $i$ -th security domain is not provided. The IS level of the entire system is defined as  $\bar{s} = \frac{1}{n} \sum_{i=1}^n s_i$ .

After receiving information from all domains, the Coordinator, taking into account IS levels of domains, restrictions on the general budget and the interdependence of domains, makes a decision  $\hat{x}_1, \hat{x}_2, \dots, \hat{x}_n$  on the distribution of investments between domains. Each domain acts selfishly and is interested in obtaining the highest possible level of investment. The coordinator's task is to minimize losses from IS incidents throughout the system within this budget, in other words, to maximize social welfare. Below, this task is modeled as a game of interdependent security.

We consider a system consisting of  $n$  players (IS domains). Assume that the interdependence of the players is represented by the directed graph  $G = (N, L)$ , where  $N = \{1, \dots, n\}$  and  $L \in R_+^{n \times n}$  denote the set of players and the set of directed dependencies between them, respectively. Player  $j$  can affect player  $i$ 's security level only if  $l_{ji} > 0$ . We denote the set of neighbors of player  $i$  as  $N^i = \{j: l_{ji} > 0\}$ . At any point in time, player  $i$  can undergo a cyberattack directly from the external environment with probability  $p_i$  or from any neighbor  $j \in N^i$  with probability  $l_{ji}$ . The network topology  $G$  and the probability of a cyberattack from outside  $p_i$  does not change with time.

The goal of each player  $i$  is to maximize their utility function  $u_i$ , given below:

$$U_i(\mathbf{x}) = -L_i x_i + C_i x_i - t_i, \quad (33)$$

where  $\mathbf{x} = \{x_1, x_1, \dots, x_n\}^T$  denotes the investment vector,  $L_i$  is the potential loss of player  $i$  in the event of an information security incident,  $C_i$  is the (special) investment cost of player  $i$ , costs  $C_i > 0$  are spent per unit of investment. The threshold  $t_i$  characterizes the penalty/reward to which the player may be subjected, and in the general case  $\mathbf{x}$  may depend on the investment vector. For simplicity,  $t_i = 0$  is accepted in the following comments. It is assumed that each player acts rationally and chooses his investment level so as to maximize his utility function.

An interdependent security game  $(\{1, \dots, n\}, \{x_{i \geq 0}\}, \{u_i(\cdot)\})$  is defined as a strategic game between the  $n$  players listed above. In this game, the optimal vector of information security investments is found as a solution to the following problem, which maximizes social welfare and is solved by the Coordinator:

$$\max_x \sum_{i=1}^n U_i(x) \quad (34)$$

$$\begin{aligned} x_i &\geq 0, i = 1, \dots, n, \\ \sum_{i=1}^n C_i x_i &\leq B, \end{aligned} \quad (35)$$

According to the above hypothesis about players, there is only one  $\mathbf{x}^*$  socially optimal investment profile for problem (34)-(35). Note that the coefficients  $L_i$ ,  $C_i$  and the risk functions  $f_i$  are confidential data of players; the Coordinator does not know about these data and therefore cannot solve the problem (34)-(35). At the same time, players also do not have enough information to find a solution  $\mathbf{x}^*$ .

Therefore, it is necessary to find the coordination mechanism implemented by the Coordinator in order to solve the problem (34)-(35). To do this, it is assumed that the players provide their confidential data about  $L_i$ ,  $C_i$ , and  $f_i$  to the Coordinator, provided that he does not transfer it to other players. This assumption is based on the fact that there may be legislative requirements for state bodies to submit statistical reports on the level of IS to an authorized state

body. In this case, the Coordinator will be able to solve the problem with full information and find the Nash equilibrium for this game.

Ensuring the IS of an e-government requires intensive international cooperation, and any single country cannot fully achieve its goals in this area, and to solve this problem it must cooperate with other countries. It is assumed that the conflict of interests of some countries in the field of information security is not antagonistic, and there is the possibility of concluding agreements between them, with mutual obligations in this field, and that countries can share the benefits of the coalition.

Let  $n$  countries participate in the coalition. The payoff function of the  $i$ th country ( $U_i$ ) can be expressed as the difference between the benefits ( $B_i$ ) and costs ( $C_i$ ).

Suppose that  $t_i \in (0; 1)$  is the share of the  $i$ th country in total costs. In the general case, the cost function can be defined as the function  $C_i = C(t_i)$  of  $t_i$ . If the total costs of the coalition are  $G$ , the costs of the  $i$ -th country in the coalition will be  $g_i = t_i G$ . Obviously,  $G = \sum_{i \in N} g_i$ .

We also assume that the number of users of the  $i$ -th country using information security services provided by the coalition is  $n_i$ , and  $S(n_i)$  is the cost of the  $i$ th country for using these services.

Suppose that the entire gain of the coalition is described by function  $B$ . To characterize the distribution of the total gain between coalition countries, we introduce the parameter  $\alpha_i \in (0; 1)$ , where  $\sum_{i \in N} \alpha_i = 1$ .  $i$ -th country receives  $\alpha_i$  part of this gain, i.e.  $B_i(G, \alpha_i) = \alpha_i B(G)$ .

Given the above, the payoff function of the  $i$ -th coalition country can be determined as follows:

$$U_i(G, g_i, \alpha_i, n_i) = \alpha_i B(G) - C(g_i) - S(n_i). \quad (36)$$

Decision parameters are  $t_i$  and  $\alpha_i$ . The strategy of each country participating in the coalition is to minimize their costs and maximize their benefits.

Coalition stability is an important issue in coalition games. The following concepts of stability are used in the work:

- internal stability (a coalition member has no incentive to leave the coalition);

- external stability (a country that is not a member of the coalition has no incentive to join the coalition).

Let  $P$  be the coalition in question;  $P \setminus \{i\}$  denotes the remaining coalition when country  $i$  leaves the coalition, and  $P \cup \{j\}$  denotes the coalition when country  $j$  outside the coalition joins it. A stable coalition  $P$  is defined as follows:

$$\text{Внутренняя устойчивость: } U_i(P) \geq U_i(P \setminus \{i\}) \quad \forall i \in P, \quad (37)$$

$$\text{Внешняя устойчивость: } U_j(P) \geq U_j(P \cup \{j\}) \quad \forall j \notin P. \quad (38)$$

It is assumed that the payoff functions  $U_i$  are twice continuously differentiable, quasi-convex, and strictly monotonic. These assumptions make it possible to find the equilibrium vectors  $g^*(P)$  and  $\alpha^*(P)$  as the Nash equilibrium between all players in the coalition  $P$  and players not in  $P$ . Each member of the coalition can get their payoffs according to the “cost-benefit” rule.

**The sixth chapter** discusses decision-making models for managing e-government information security.

For strategic management of e-government information security, a model based on fuzzy cognitive maps (Fuzzy Cognitive Map, FCM) was proposed [18]. To build an FCM model for e-government information security it is necessary to:

- 1) determine the factors that affect the state of information security;
- 2) build a matrix of mutual influence of factors;
- 3) build a cognitive model of information security management;
- 4) on the developed model, work out possible strategies for managing e-government information security.

FCM is one way of representing knowledge. To build the FCM, the knowledge and experience of experts in the subject field should be used. To determine the factors influencing e-government information security management, we analyzed the national cybersecurity strategies of a number of countries, as well as model strategies of international organizations. These strategies were developed with the wide involvement of leading information security experts and can be considered as fairly good sources of experts' knowledge accumulation. During the analysis of cybersecurity

strategies, a number of factors were identified that influence e-government information security management, a list of which is presented in Table 3.

When constructing FCM, the most difficult task is to assign weights for the influence of factors. The following simple expert method is used to calculate the weights of the influence of factors. Let each expert evaluate the weight of mutual influences as a number from the interval  $[-1, 1]$ . Further, these mutual influence weight matrices are aggregated as the average value of the sum of the weights or by application of a threshold function (for example, a sigmoid function). Since the experience and knowledge of experts about the subject of assessment can be different, each expert can be assigned a non-negative numerical weight of confidence. Given the confidence weights of experts, the aggregate values of the mutual influence weights can be calculated by the following formula (only weights of the same sign are taken into account):

$$W_{ij} = \frac{\sum_{k=1}^m b_k w_{ij}^k}{m}, \quad (39)$$

where  $w_{ij}^k$  is estimation of the weight of the mutual influence between  $C_i$  and  $C_j$  by the  $k$ th expert;  $b_k$  is the confidence weight of the  $k$ -th expert;  $m$  is the number of experts. If rating of an expert differs from ratings of most experts, then he/she is fined – he/she is assigned a very low or zero confidence weight.

FCM has the same basic weaknesses as other fuzzy systems: they are not able to learn on their own. With the availability of relevant data, the weight of the mutual influences of factors can be improved using the training mechanisms of neural networks. Most of these approaches are based on the Hebb learning method, but there are also approaches that use heuristic methods.

**Modeling of FCM dynamics.** Output processes of FCM include the state vector  $A_{1 \times n}$ , which consists of  $n$  factor values, and the weight matrix  $W_{n \times n}$ . The value of each factor is influenced by the values of the factors associated with it and their previous value. The activation value for each factor is calculated iteratively by the following rule:

$$A_i^{(t+1)} = f \left( \sum_{j=1}^n w_{ij} A_j^{(t)} \right), i \neq j, \quad (40)$$

where  $t$  is the current time;  $A_i$  is the activation level of factor  $C_i$ ;  $A_j$  – level of activation of factor  $C_j$ ;  $w_{ij}$  is the weight of the mutual influence between  $C_i$  and  $C_j$ ; and  $f$  is a threshold function.

In this work, a sigmoid function is used as a threshold function (binary and trivalent functions can be also used):

$$f(x) = \frac{1}{1+e^{-\lambda x}}, \lambda > 0. \quad (41)$$

### Testing on the model of various IS management strategies.

Note that each of the  $C_j$  concepts can take values in the interval  $[0, 1]$ , which is also called the “activation level”.

For example, consider the modeling of the following IS management scenarios.

**Scenario A:** Self-development of the situation  $A(0) = (1., 1., 1., 1., 1., 1., 0.)$ .

**Scenario B:** Using only technical measures  $A(0) = (0, 0, 1, 0, 0, 0, 0)$ .

In computational experiments, we used a sigmoid function with parameter  $\lambda = 1$ . As a rule, calculations by formula (41) converged in less than five time steps of modeling. All models ended in a stable state, but theoretically they could also go into the limit cycle or into a chaotic attractor. The intermediate values of the factors in the calculations for scenario B are shown in table 3.

Table 3. Final results of the calculations according to the scenario B

Factors	Initial values - Scenario B	Final values - Scenario B	Difference between the stable states of Scenarios A and B
Legal measures	0.00	0.5275	0.0008
Organizational measures	0.00	0.5147	0.0008
Technical measures	1.00	1.00	0.4184
Capacity building	0.00	0.5875	0.0309
Stakeholder collaboration	0.00	0.5378	0.0104
IS threat development	0.00	0.5000	0
IS level	0.00	0.6048	0.0424



From table 3 we can conclude that using only technical measures does not lead to a significant improvement in the level of information security (the maximum difference between the scenarios is 0.0424).

A hypergame model was developed to optimize e-government information security management tactics [11]. Game theory is one of the most powerful mathematical tools for modeling information security decisions. However, classical game theory assumes that all players are fully aware of each player's strategies and preferences. This is a very strict assumption, and in many real-life situations, there is often significant informational asymmetry between players. Players do not always know all the information about the true intentions, strategies or preferences of each player. As a result, they perceive the situation from their point of view and may be mistaken in their perception. This work uses one family of games with incomplete information called hypergames. The theory of hypergames extends classical game theory with the ability to take into account differences in the incorrect perception of players. There are very few studies on the use of hypergames to study information security decisions. Here the hypergame approach is presented as a tool for tactical analysis in the context of information security. The proposed two-level hypergame models the perceptions of the attacker (A) and the defender (D) about the information security situation as a series of games as follows.

Suppose that,  $T_A = \{a_1, a_2, \dots, a_n\}$  is the set of tactics (attack scenarios) of A and  $T_D = \{d_1, d_2, \dots, d_m\}$  is the set of tactics (defense mechanisms) of D; but the number of tactics may not be the same. The result of the game is a pair of tactics chosen by A and D. Thus, the set of possible outcomes is  $O = T_A \times T_D = \{(a_1, d_1), (a_1, d_2), \dots, (a_n, d_m)\}$ . Each player compiles an ordered preference vector of results:  $P_A = \langle o_{A1}, o_{A2}, \dots, o_{An \cdot m} \rangle$  and  $P_D = \langle o_{D1}, o_{D2}, \dots, o_{Dn \cdot m} \rangle$ . In the preference vector, the elements are arranged from the preferred to the least preferred:  $\forall o_i, o_{i+1} \in P$ , the element  $o_i$  is preferred to  $o_{i+1}$ .

A two-player game can be described as  $G_{A,D} = ([A, D], [T_A, T_D], [P_A, P_D])$ . With these notations, the hypergame of A

and  $D$  is defined as  $H(A, B) = \{p(A, G_{A,D}), p(D, G_{A,D})\}$ , where  $p$  function indicates the game the individual player perceives. For example,  $p(D, G_{A,D})$  indicates the game that  $D$  perceives based on the information it has.

Numerical experiments were performed using HYPANT<sup>2</sup> open source software for hyperoin, where  $A$  has 2 attack scenarios and  $D$  has 3 defense mechanisms.

In the work, a conceptual model of situational management of information security of the e-government is developed, and an approach to the implementation of the model based on the theory of precedents is proposed [15]. In the conceptual model of situational management, the information infrastructure of the e-government consists of information security domains. In each domain, based on the security policy of the domain, information security monitoring is implemented. Information security monitoring refers to the process of constant observing of information security events in order to timely identify and respond to events that have led, or may lead to the realization of information security threats.

The state of the e-government information security at time  $t_i \in T$  is described by the set of information security events  $X = \{x_{i1}, \dots, x_{im}\}$  registered and not resolved before this time, where  $x_{ij}$  is the number of information security events in the security domain  $j$  at time  $t_i$ . Of course, this set may be empty at some points in time. Note that an event can be a sequence of other events (a complex event).

In the work, the IS event is formally described as follows:

$$e = (Etype, DT, ID, rb, sev, v_1, \dots, v_n), \quad (42)$$

where  $e$  is an IS event,  $Etype$  describes the type of event,  $DT$  indicates the time and date of the event,  $ID$  is an identifier of the source where the event is detected,  $rb$  is the degree of trust of the source,  $sev$  is the degree of risk of the event,  $v_1, \dots, v_n$  is other attributes required to describe the event depending on the application (for example, IP address, protocol, port number, etc.). In addition, the description of IS events usually includes text information, for

---

<sup>2</sup> <http://users.monash.edu/~lbrumley/hyper.html>

example, symptoms, manifestations of an event, error messages, etc. To describe this data, it is proposed to use the method of latent semantic analysis (LSA)<sup>3</sup>.

Information about IS events in domains is registered in the local registry and transferred to the national IS event tracking system of the National IS Center (NISC). The NISC collects data on events from all IS domains, carries out their processing, analysis (aggregation, correlation) and visualization. Using these data, the NISC builds a holistic picture of the IS situation, analyzes the situation and evaluates the potential effects of IS events not only at the level of a separate domain, but also at the scale of several interconnected and interdependent IS domains. The NISC selects the appropriate method for processing events from the National IS Event Database, and transfers the recommended solutions to the relevant IS domains. The national database of IS events is the central knowledge base about events and how to handle them; templates for coordinated measures for processing IS events are also stored here. IS domains adapt the recommended NISC solution to the current situation and processes the event. For this purpose, the necessary technical resources are allocated, an event processing group is appointed, which consists of technical and other specialists (experts), and a decision maker (DM). During event processing, the event handling group can make the necessary changes to the adapted solution. After processing the event, the tested method of processing the event is entered in the National IS Event Database, indicating the group of experts and decision makers who processed the event.

A precedent can be formally defined as follows. Precedent  $p$  consists of a tuple  $\langle s, r, h, z \rangle$ , where  $s \in S$  is a situation,  $r \in R$  is decision associated with it and carried out by a group of experts  $h \in H$  led by a decision maker (DM)  $z \in Z$ . Several decisions can correspond to each situation  $s$ , so we can assume that there are precedents of the form  $\langle s, r \rangle$ , and  $\langle s, r' \rangle$ , where  $r \neq r'$ .

---

<sup>3</sup> Evangelopoulos, N. E. Latent semantic analysis // Wiley Interdisciplinary Reviews: Cognitive Science, – 2013, 4 (6), – p. 683-692.

In the general case, a decision can be understood as: actions previously performed in similar situations and their results; a guide to action in given situation; expert advice on how to perform actions.

The description of the result of applying the solution – processing the IS event may contain the planned and actual time of processing the event; actions taken to eliminate the event and its consequences; event processing result; a list of actions required to prevent an event. A description of the result may also include links to other events (precedents). LSA method can also be used to describe this data.

Each precedent  $p_i$  can be considered as a conditional implication  $s_i \Rightarrow r_i, i = \overline{1, n}$ . Thus, if a certain situation  $s_i \approx s_j, j = \overline{1, n}, i \neq j$  is given, and there is a precedent  $p_i = \langle s_i, r_i, h_i, z_i \rangle$ , it can be argued that  $r_j$  is an approximate decision for the situation  $s_i$ . The closer the situation  $s_i$  to the situation  $s_j$ , the more likely that  $r_j$  is a decision for  $s_i$ .

The “ $k$  nearest neighbors” method is the most common and often used approach for finding the “closest” precedent to the given precedent in the precedent database. First,  $k$  similar precedents are found from the precedent database (usually  $k = 3$  or  $k = 5$ ), and then among them, based on the chosen similarity metric, the precedent closest to the current precedent is determined.

The degree of proximity of two precedents is determined based on the degree of proximity of relevant features of precedents. Assume that to each feature is assigned a weight coefficient (for example, based on the PSO algorithm), which reflects the relative importance of the feature. To determine the degree of proximity to the precedent in all features, you can use the following formula:

$$sim(i, k) = \frac{\sum_{j=1}^n w_j \cdot sim(e_{ij}, e_{kj})}{\sum_{j=1}^n w_j}, \quad (43)$$

where  $w_j$  is the weight of the  $j$ th attribute;  $sim$  – similarity metric;  $e_{ij}$  and  $e_{kj}$  are feature values of  $e_j$  for the current event  $i$  and precedent  $k$ , respectively.

The choice of similarity metric *sim* is very important, as the search for similar precedents depends significantly on this choice. As can be seen from the above description, part of the precedent features takes numerical and nominal values, and the other part is described by text data encoded by semantic vectors. Given this, it is proposed to use two types of similarity metrics. It is proposed to determine the similarity of features with numerical and nominal values on the basis of a heterogeneous distance function (Heterogeneous Euclidean-Overlap Metric, HEOM)<sup>4</sup>. The similarity between two semantic vectors is calculated by the cosine of the angle between these vectors.

**The seventh chapter** explores the methods and models for evaluating the e-government information security.

E-services are the main line of contact between the e-government and citizens and the private sector, and the level of IS of e-services allows us to judge the level of management efficiency of e-government IS as a whole. The following method is proposed for assessing the level of information security of e-services [20].

Suppose that the requirements for e-services information security are grouped in  $m$  directions (security services). For each  $i$ -th IS service, special IS indicators are determined, they are formulated in the form of questions, answers to which are given by the estimates  $M_{ij}, i = 1, \dots, m, j = 1, \dots, n$ . Answers are expressed on the following scale:

- 0 – requirements are not met;
- 0.25 – requirements are met to a small extent;
- 0.5 – requirements are met to a large extent;
- 0.75 – requirements are met almost completely;
- 1 – requirements are fully implemented.

The group indicator  $S_i, i = 1, \dots, m$  is determined by the following formula:

---

<sup>4</sup> Wilson, D., Martinez, T. Improved heterogeneous distance functions // Journal of Artificial Intelligence Research, – 1997, 6 (1), – p. 1-34.

$$S_i = \sum_{j=1}^{n_j} \alpha_{ij} M_{ij}, \quad (44)$$

where  $M_{ij}$  is the value of the  $j$ -th special indicator for the  $i$ -th security service;  $\alpha_{ij}$  is the weight of the  $j$ -th special indicator for the  $i$ -th security service. If the weights of the indicators are the same, then it is assumed  $\alpha_{ij} = \frac{1}{n_i}$ ,  $j = 1, \dots, n$ , where  $n_i$  is number of indicators for the  $i$ th security service.

The e-service information security level ( $SL$ ) can be found by the rule of the weakest link:

$$SL = \min_i S_i. \quad (45)$$

In the existing composite indices, weights of individual indicators included in them are either equal or subjectively assigned. To overcome this drawback, a method is proposed for determining the weights of indicators in composite national cybersecurity indices based on entropy and static and dynamic cybersecurity indices are introduced [27].

Let a matrix  $D = (x_{ij})_{m \times n}$  be given of estimations of the cybersecurity levels of  $m$  countries by  $n$  indicators, where  $x_{ij}$  is an estimation of the  $i$ -th country by the  $j$ -th indicator. The entropy-based algorithm can be expressed as follows:

**Step 1. Normalization of the estimation matrix.** As a result, the matrix  $R = (r_{ij})_{m \times n}$  is obtained, where  $r_{ij} \in [0,1]$  is the estimation of the  $j$ -th country according to the  $i$ -th indicator. In the considered problem, the value of the indicator is considered the better, the greater, therefore, the following formula is used for normalization:

$$r_{ij} = \frac{x_{ij} - \min_i \{x_{ij}\}}{\max_i \{x_{ij}\} - \min_i \{x_{ij}\}}. \quad (46)$$

**Step 2.** Calculation of entropy. The entropy of the  $i$ -th indicator is determined by the following formula:

$$H_j = -k \sum_{i=1}^n f_{ij} \ln f_{ij}, j = 1, 2, \dots, m, \quad (47)$$

where  $f_{ij} = r_{ij} / \sum_{i=1}^n r_{ij}$ ,  $k = 1 / \ln n$ . When  $f_{ij} = 0$ , it is assumed, that  $f_{ij} \ln f_{ij} = 0$ .

**Step 3.** Determination of weights based on entropy. The entropy weight of the  $j$ th indicator is defined as follows:

$$w_j = \frac{1 - H_j}{m - \sum_{j=1}^m H_j}, \quad (48)$$

where  $0 \leq w_j \leq 1, \sum_{j=1}^m w_j = 1$ .

Table 4 presents the entropies and weights of indicators calculated on the basis of data from the global cybersecurity indices of the CIS countries for 2017<sup>5</sup> according to formulas (47)-(49). As you can see, with the entropy approach, the indicators “Technical” and “Capacity building” have more weight.

Table 4. Entropy and weights of indicators

Indicator	Entropy	Entropy-based weights
Legislative	0.929	0.108
Technical	0.821	0.273
Organizational	0.903	0.147
Capacity building	0.805	0.296
Cooperation	0.884	0.176

Let  $x_{ij}^t$  be the value of the  $j$ -th indicator for the  $i$ -th country at time  $t$  ( $j = 1, \dots, m; i = 1, \dots, n; t = t_0, t_1$ ). Static Cybersecurity Index (SCI) can be defined as follows:

$$SCI_i^t = \prod_{j=1}^m \left( \frac{x_{ij}^t}{x_{rj}^t} \right)^{\frac{1}{m}}, \quad (49)$$

where  $x_{rj}^t$  is the base value of the  $j$ -th indicator at time  $t$ , for example, the average value of the indicator around the world.

For each country, you can build a Dynamic Cybersecurity Index (DCI) from time  $t_0$  to  $t_1$  using the following formula:

<sup>5</sup> GCI 2017 Regional Report: CIS Region Report, 2017, 36 p.

[http://www.itu.int/en/ITU-D/Cybersecurity/Documents/CIS\\_GCIv2\\_report.pdf](http://www.itu.int/en/ITU-D/Cybersecurity/Documents/CIS_GCIv2_report.pdf)

$$DCI_i^t = \prod_{j=1}^m \left( \frac{x_{ij}^{t_1}}{x_{ij}^{t_0}} \right)^{\frac{1}{m}}. \quad (50)$$

It is also advisable to develop indicators for assessing the level of e-government IS, taking into account user comments as a measure of feedback. In the model proposed to implement this idea, trust in the e-government information security is evaluated based on various sources of information (components) from which citizens receive information [19]:

- Personal experience ( $I$ );
- Reviews of social networks (friends and acquaintances) ( $W$ );
- Reviews expressed in the media ( $M$ );
- Certificates or obligations provided by government ( $S$ ).

Trust values for the components are calculated as the weighted average of all ratings:

$$T_K(a, c) = \frac{\sum_{r_i \in R_K(a, c)} w_K(r_i) \cdot v_i}{\sum_{r_i \in R_K(a, c)} w_K(r_i)}, \quad (51)$$

where  $T_K(a, c)$  are trust values of agent  $a$  in the e-government information security calculated relative to factor  $c$  by the component  $K$ .  $R_K(a, c)$  is the set of ratings collected to calculate the trust by component  $K$ .  $w_K(r_i) \geq 0$  – weighted rating functions to calculate the degree of relevance of the rating  $r_i$ .  $v_i$  – rating values of  $r_i$ . The trust value is normalized to the range  $[-1, 1]$  by dividing by the sum of weights. The weighting rating function  $w_K(r_i)$  is determined separately for each component. The total trust value is calculated as

$$T(a, c) = \frac{\sum_{K \in \{I, W, M, S\}} W_K \cdot T_K(a, c)}{\sum_{K \in \{I, W, M, S\}} W_K} \quad (52)$$

where  $W_K$  are weights selected in accordance with the importance of the components for the task in question.

**The results** of the dissertation show the main scientific-theoretical and scientific-practical results obtained during the solution of the issues raised in the dissertation:



1. Based on the results of the analysis and research of the current state of e-government information security management problems, the main scientific-theoretical and scientific-practical problems in this field are determined [1, 2, 3, 5, 8]. This result is of practical importance as a systematized information base for planning and organizing future scientific and practical research in the field of information security and creating resources for relevant levels of education.
2. A conceptual model of managing of e-government information security management [9] and a conceptual architecture of e-government information security management system [6] are proposed. The practical significance of the result is that it creates a conceptual framework for improving the architecture and structure of the e-government information security system.
3. A consensus method has been developed for ranking strategic risks to national interests in the field of information [28, 21], a method for assessing risks in interconnected critical information infrastructures [31, 13], and models for assessing the survivability of a national Internet infrastructure [30]. The practical significance of the result is due to the proposed approaches to strategic planning to ensure information security and to identify key areas for ensuring the security of critical information infrastructures.
4. For the e-government biometric identification system, methods were proposed for aggregating information in biometric systems [4], detecting altered fingerprints based on fractal characteristics [7], and a method for synthesizing biometric cryptosystems based on discretized texture fingerprint descriptors [10] was developed.
5. Methods of DDoS attack incident detection [24], multicriteria prioritization of information security incidents [12] and a method for optimal planning of incident handling [29] have been developed. The practical significance of the result is based on the improvement of the national CERT system and the provision of a

methodological framework for the organization of relevant services.

6. A model for evaluating the e-government coordination system [32, 16], a model for investment coordination in a two-level hierarchical information security management system [25], and a model for the formation of international coalitions [33, 17] are proposed. The practical significance of the result is that it offers economically sound approaches that are involved in ensuring information security and will allow for the effective coordination of the activities of different stakeholders.
7. A fuzzy cognitive model for the strategic management of the e-government information security [18], a hyper-game model for choosing cyber defense tactics [11], and a situation-based management model of the e-government information security [15] are proposed. The practical significance of the result is due to the fact that the proposed models can be implemented in the form of specific procedures for interdepartmental information security councils and situation centers.
8. Methods have been developed for assessing the level of e-services information security [20], a method of static and dynamic cybersecurity indices with entropy weights [27], and a model for assessing the trust of citizens in e-government information security [19]. The practical significance of the proposed approaches is based on the possibility of forming a system of statistical reporting on information security and its application in statistical analysis in various areas.

**The main provisions of the thesis are published in the following scientific papers:**

1. Imamverdiyev, Y. N. Some issues of creating a reliable and secure e-government // **Proc. of the 1st International Conference “Problems of Cybernetics and Informatics”**, – Baku: – 26-28 October, – 2006, – c. 2, – p. 80-82.
2. Abdullayeva, F., Imamverdiyev, Y., Musayev, V., Wayman, J. Analysis of security vulnerabilities in biometric systems // **Proc.**

- of the 2nd International Conference “Problems of Cybernetics and Informatics”, – Baku: – 10-12 September, – 2008, – p. 60-63.
3. Alguliev R., Imamverdiyev Y. E-government information security management research challenges // **IEEE International Conference on Application of Information and Communication Technologies (AICT)**, – Baku: – 14-16 October, – 2009, – p.1-5. (**Scopus**)
  4. Imamverdiyev, Ya. N. A model of fusion of information on image quality based on the Dempster-Shafer theory for biometric systems interoperability // – Redding (USA): **Journal of Automation and Information Sciences**, – 2010. 42(2), – p. 66-74. (**Web of Science; Impact Factor: 0.024**)
  5. Alguliev, R.M., Imamverdiyev, Y.N. E-government information security management: research challenges // – Baku: **Problems of Information Society**, – 2010. №1, – p. 3-13.
  6. Imamverdiyev Y. Architecture of e-government information security management system // **Proc. of the 3rd International Conference “Problems of Cybernetics and Informatics”**, – Baku: – 6-9 September, – 2010, – p.79-82.
  7. Imamverdiyev, Y. N. Method for detecting altered fingerprints based on fractal characteristics // – Moscow: **Information Technology**, – 2012. № 9, – p. 11-16.
  8. Imamverdiyev, Y.N. State-of-the-art analysis of the researches on e-government information security management // – Baku: **Problems of Information Society**, – 2012. № 2, – p. 19-26.
  9. Imamverdiyev, Y.N. Conceptual model of e-government information security management // – Baku: **Problems of Information Society**, – 2013. № 1, – p. 20-31.
  10. Imamverdiyev, Y., Teoh, A., Kim, J. Biometric cryptosystem based on discretized fingerprint texture descriptors // **Expert Systems with Applications**, – 2013. 40, – p.1888–1901. (**Web of Science; Impact Factor: 4.298**)

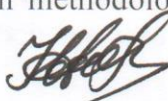
11. Imamverdiyev, Y. A hypergame model for information security // **6th International Conference on Information Security and Cryptology (ISCTurkey)**, – Ankara: – 20-21 September, – 2013, – p. 65-70.
12. Imamverdiyev, Y. An information security incident prioritization method // **IEEE 7th International Conference on Application of Information and Communication Technologies (AICT)**, – Baku: – 23-25 October, – 2013, – p.183-187. (**Web of Science**)
13. Imamverdiyev, Y. An application of extreme value theory to e-Government information security risk assessment // **IEEE 7th International Conference on Application of Information and Communication Technologies (AICT)**, – Baku: – 23-25 October, – 2013, – p.349-352. (**Web of Science**)
14. Imamverdiyev, Y.N. Next generation national cyber security strategies // – Baku: **Problems of Information Society**, – 2013. № 2, – p. 42-51.
15. Imamverdiyev, Y. N. A model for situational management of e-government information security // – Moscow: **Information Technology**, – 2014. №8, – p. 24-33.
16. Imamverdiyev, Y.N. Coordination problems in information security of e-government // – Baku: **Problems of Information Society**, – 2014. № 2, – p. 24-30.
17. Musayev, V.Y., Imamverdiyev, Y.N. International challenges, initiatives and commitments in the field of information security // **Proc. of the 2nd National Scientific-Practical Conference on “Multi-disiplinar Problems of Information Security”**, – Baky: – 17-18 May, – 2015, – p. 102-105.
18. Imamverdiyev, Y. N. A fuzzy cognitive model for the strategic management of e-government information security // – Moscow: **Information Technology**, – 2015. №6, – p. 440-447.
19. Imamverdiyev, Y. E-government information security trust assessment model // – (India) **International Journal of Research Studies in Computer Science and Engineering**, – 2016. 3(2), – p. 1-6.

20. Imamverdiyev, Y. E-services security assessment model // **IEEE 10th International Conference on Application of Information and Communication Technologies (AICT)**, – Baku: – 12-14 October, – 2016, – p. 595-598. (**Web of Science**)
21. Imamverdiyev, Y.N. Consensus ranking method of information security threats of a nation state // **II Міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології"** ("Information Security and Computer Technologies"), – Kropyvnytskyi: – 20-22 April, – 2017, – p. 12-13.
22. Imamverdiyev, Y.N. Problems of forming international coalitions on information security // **Proc. of the 3rd republican scientific-practical seminar "Actual problems of information security"**, – Baku: – 08 December, – 2017, – p. 77-80.
23. Alguliyev, R., Imamverdiyev, Y., Sukhostat, L. Cyber-physical systems and their security issues // – Amsterdam: **Computers in Industry**, – 2018. 100, – p. 212–223. (**Web of Science; Impact Factor: 4.769**)
24. Imamverdiyev, Y., Abdullayeva, F. Deep learning method for denial of service attack detection based on restricted Boltzmann machine // – (New Rochelle, NY, USA) **Big Data**, – 2018. 6(2), – p. 1-17. (**Web of Science, Impact Factor: 2.106**)
25. Imamverdiyev, Y.N. An investment coordination model in two-level hierarchical information security management systems // – Moscow: **Economic Security and Quality**, – 2018. №3 (32), – p. 41-47.
26. Imamverdiyev, Y.N. A conceptual approach for the detection of APT (Advanced Persistent Threat) attacks // – Baku: **National security and military science**, – 2018. №1 (4), – p. 93-103.
27. Imamverdiyev, Y.N. Entropy weights and dynamic index for national cybersecurity // – Baku: **Problems of Information Society**, – 2018. №2, – p.16-27.

28. Imamverdiyev, Y.N. A consensus ranking method for information security threats of an e-government // – Baku: **Problems of Information Technology**, – 2018. №2, – p. 34-45.
29. Imamverdiyev, Y.N. A model for optimal planning of information security incident response operations // – Baku: **Problems of Information Technology**, – 2018. №2, – p. 80-91.
30. Imamverdiyev, Y. N. Survivability evaluation models for national Internet infrastructure // – Moscow: **Telecommunications**, – 2018. №12, – p.36-45.
31. Imamverdiyev, Y. N. Method for assessing information security risks in interconnected information infrastructures // – Oryol: **Information Systems and Technologies**, – 2019. № 1 (111), – p. 102-112.
32. Imamverdiyev, Y.N. A multi-criteria evaluation model for e-government information security coordination system // – Baku: **Problems of Information Technology**, – 2019. № 1, – s. 47-58.
33. Imamverdiyev, Y.N. An international coalition model for information security // – Baku: **Problems of Information Society**, – 2019. № 1, – p. 14-20.

### **The role of the applicant in papers published in collaboration:**

- [2] – vulnerabilities of the biometric system are analyzed by modules;
- [3] – current areas of research on the topic are analyzed;
- [5] – research methodology was developed and corresponding directions were analyzed;
- [10] – architecture of the biometric cryptosystem was developed, main components were implemented, and experiments were carried out;
- [17] – a research methodology was developed and international experience was analyzed;
- [23] – a tree model of attack vectors was proposed;
- [24] – research statement and research methodology belong to the applicant.



The defense will be held on **27th** The defense will be held on **27<sup>th</sup>**  
**May 2021** at **14<sup>00</sup>** at a meeting of the Dissertation council ED 1.35 of  
Supreme Attestation Commission under the President of the  
Republic of Azerbaijan operating at the Institute of Information  
Technology of ANAS.

Address: Az 1141, Baku city, Bakhtiyar Vahabzadeh street, 9A

Dissertation is accessible at the library of the Institute of Information  
Technology of ANAS.

Electronic versions of dissertation and its abstract are available on  
the official website of the Institute of Information Technology of the  
ANAS.

Abstract was sent to the required addresses on **23<sup>rd</sup>** **April 2021**

Signed for print: 22.04.2021

Paper format:  $60 \times 80 \frac{1}{16}$

Volume: 75,721 characters

Number of hard copies: 20