Journal of Theoretical and Applied Information Technology
30th September 2018. Vol.96. No 18

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

THE METHODS AND TECHNOLOGIES OF RELIABILITY AND SECURITY OF INFORMATION SYSTEMS AND INFORMATION AND COMMUNICATION INFRASTRUCTURES

[1]SEILKHAN BORANBAYEV, [2]NIKOLAJ GORANIN, [1]ASSEL NURUSHEVA

[1] Department of Information Systems, L.N.Gumilyov Eurasian National University, Astana, Kazakhstan

[2]Faculty of Fundamental Sciences, Vilnius Gediminas Technical University, Vilnius, Lithuania

E-mail: [1] sboranba@yandex.kz, [2]nikolaj.goranin@vgtu.lt, [1]nurusheva.assel@mail.ru

ABSTRACT

The article is devoted to the investigation of the problem of the reliability and security of information systems and information and communication infrastructure functioning. Some models and methods for calculating reliability and assessing of the information risks, and the tools for managing information security risks are considered. A review of the best experiences of countries with a high global cybersecurity index is made. The directions recommended to achieve the global cybersecurity index of Kazakhstan, established by the Cybersecurity Concept of the country ("Cybershield of Kazakhstan") are defined.

Keywords: *Information system, Reliability, Security, Risk, Method, Cybersecurity, Global Cybersecurity Index.*

1. INTRODUCTION

It is well known that modern society is becoming increasingly dependent on information technology, its continuous and trouble-free operation, respectively, on its reliability and security.

Priority components of the information security system of any organization or institution include the information risk management system.

Standards and approaches to the management of information risks (international specifications and standards) is established: ISO 17799-2002 (BS 7799), ISO/IEC 27002, GAO and FISCAM, SCIP, COBIT, NIST 800-30, SAC, COSO, SAS 55/78 and others. [1]

At the same time, threats and risks of information security keep growing. Thus, according to statistics given by KZ-CERT Computer emergency response team, there were processed 21 thousand of incidents in 2016 and 13 thousand of information security incidents in the first half of 2017 in Kazakhstan. Most of the incidents are related to botnets. [2]

The bulk of threats blocked on a unified access gateway to the Internet is also associated with botnets (more than 80%). [3, 4]

Botnet is the most dangerous modern type of all incidents and the biggest known threat of the global IT infrastructure, requiring special attention and taking timely and appropriate measures to prevent it and to exclude the spread in the future. [5]

Now most of the information protection tools are focused on the eliminating of the consequences and minimizing of the damage from the events of the security incidents. Intrusion (attacks or leaks of confidential information) detection and prevention systems are often used. This system allows identifying unauthorized access to the protected system or its unauthorized management in real time and quickly implementing actions to prevent it. Such systems are very useful for organizations, but it does not allow knowing in advance about the alleged attacks.

The elimination of damage from attacks can be achieved using attack prediction tools. Such tools are usually based on the methods of data mining and machine learning. Basically, information for analysis and forecasting is provided by:

- logging of users' sessions;

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- audit data and other resources allow analyzing the users' actions, requested resources, input data, intensity and frequency of actions;

-the information about the sequences of users' actions which leads to the damage.

The methods of machine learning include classification (for example, decision trees, neural networks, proximity measures in high-dimensional space, etc.), clustering, regression, etc. If we imagine that each user's session is a point in a high-dimensional space, then based on the similarity one can detect whether this or that session represents a danger or not. These methods do not take into account that the attacker can use various user's sessions, tools, resources, etc., therefore, methods of analyzing the chains of events are usually used. [6]

To forecast various types of information security incidents, different approaches and models are explored and used. For example, N.Goranin proposed a model for predicting the distribution of malicious software based on the use of a genetic algorithm. [7, 8] The focus of his work consists of three types of malicious programs: the most aggressive - Internet worms [9, 10], the most rapidly spreading botnets [11, 12] and mobile malware [13]. Genetic algorithm approach was selected taking into consideration its efficiency while solving tasks with large solution space and ability to model the evolution process which is the case for malware, often considered as a form of artificial life, evolution forecasting. [14-16]. The considered model covers the malware feature representation description in the genetic algorithm suitable format, evolution evaluation fitness functions for propagation and forecasting of survivability strategy evolution of several malware types in friendly and hostile environments, algorithm operating conditions and a genetic algorithm based method for decision tree generation, used for malware risk evaluation. A specialized tool based on the principles of a genetic algorithm for predicting of the evolution of malwares and other subjects of information security was also developed. The main difference of this tool was its convenience and ease of use and configuration for a certain modeled problem area, the ability to provide specific information on security issues. [17]

Forecasting incidents gives the opportunity for specialists to take appropriate measures to prevent, minimize or eliminate damage.

By using the experience of foreign countries in the field of security we can notice that, on the one hand, they want to achieve the safe and reliable information and communication systems, and on the other hand, they recognize the necessity of openness of the Internet. For example, the following definition was proposed in the information security strategy of the Netherlands: «Cybersecurity is the protection from failures and misuse of information and telecommunications systems that can adversely affect the accessibility and reliability of information and telecommunications systems, compromise the confidentiality and integrity of information, stored in the systems.» [18]

It is clear from the definition that the fault tolerance, directly related to ensuring the reliability of information systems, is one of the main components of cybersecurity.

Taking into account the above mentioned information, the Concept of Cybersecurity ("Cybershield of Kazakhstan"), approved by the Decree of the Government of the Republic of Kazakhstan, includes the one of the basic principles: "state bodies and service providers adopt a risk-oriented approach to security, giving priority to efforts to ensure the highest level of reliability of created information systems in normal and freelance regimes and their resistance to willful failures." [19]

2. THE METHODS FOR RELIABILITY OF INFORMATION SYSTEM FUNCTIONING

The methods for information systems reliability and authenticity can be divided into 2 classes:

1) the methods, that ensure the accuracy (fault-free performance) of functional technical and program links of information systems;

2) the methods for controlling the authenticity of information and its correction, providing the detection and correction of the errors in the information.

There are different types of reliability: organizational; structural; technological; operational; economic; temporary; social; algorithmic and others.

Reliability analysis of information systems are usually considered at stages of design; manufacturing; exploitation. The factors that influence information system reliability at various stages are given in Table 1.

When the computer models (analytical and simulation) are designing and implementing, various methods and models are used to calculate reliability.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: The Factors That Influence Reliability Of Information System At The Various Stages [20]

Mathematical models of software reliability allow making estimates of software reliability dependency against some parameters. The classification of software reliability models is given in Table 2.

Table 2: The Classification Of Software Reliability Models [21]

As we can see, the software reliability models can be divided into analytical models and empirical models. Analytical models allow calculating the quantitative indicators of reliability. They are based on data about the behavior of the program at time of testing. Analytical models can be divided into dynamic models and static models.

The appearance of software failures is considered depending on time in dynamic models but the appearance of failures is considered depending on the number of test runs or the characteristics of the input data in statistical models.

Next, let us briefly review the models shown in Table 2.

For the Schumann's model, initial data are collected during the testing of the program in the period of fixed or random time intervals (the stages on which the sequence of test execution is implemented and the errors are fixed).

According to the LaPadula model, the sequence of test execution is performed in m stages. Each stage introduces changes (corrections) to the program. The increasing reliability function is based on the number of errors found during each test run. This model is predictive and on the basis of test results predicts the probability of further program failure-free operation. [21]

The basis for the Schick-Wolverton model is the assumption that the error rate is proportional not only to the number of errors in the programs, but also to the testing time (the probability of detecting errors increases with time). [20].

The Jelinski-Moranda model is based on the following assumptions:

- time until the next failure is distributed exponentially;

- the failures intensity is proportional to the number of remaining errors in the program. [22]

The Muse model is continuous-time dynamic model. When test is executing according to the Muse model, time of the test run is fixed before the next failure. It is possible to detect more than one error while program executing before the next failure occurs, because not every error can cause the failure.

The model of transition probabilities is based on the Markov process, which takes place in a discrete system with continuous time. The process that takes place in the system is called the Markov process (or a process without consequences) if for each moment of time the probability of any system state in the future depends only on the system state at the present time and does not depend on how the system came to this state. [9].

The Mills model allows estimating the number of errors originally found in the program.

The Lipov model complements the Mills model, making it possible to evaluate the probability of detecting a number of errors by the moment of evaluation.

The simple intuitive model involves testing by two independent groups of programmers. The results of the tests comparison provide a prediction of the errors number.

The Corcoran model takes into account the result of N tests, in which Ni errors of i-th type are detected. Thus, the probability of fail-safe execution of the program without using the test time parameters is estimated.

The Nelson model takes into account the probability of selecting a specific test set for the next execution of the program.

The empirical models are based on analysis of structural features of programs. They consider the dependencies of reliability indicators on the number of intermodule links, the number of cycles in the modules, the ratio of the number of rectilinear sections of the program to the number of branch points, etc. Such models seldom give final results of reliability indicators, but their use in the software design phase is useful for the predicting the required resources of testing, specification of planned terms.

The complexity model can be described by the following characteristics: the number of its program modules, the number and complexity of the inter-module interfaces.

The model that determines the time for debugging programs is used for the programs with a hierarchical structure. The model makes it possible to determine the number of necessary corrections and the time required to bring the program to operational state in case of the test assembly of the system. [21]

3. THE METHODS FOR RISK ANALYSIS

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A risk assessment is performed mainly by qualitative and quantitative methods. The risk assigns the values in accordance with the selected scale, which allows determining the necessary means and protection measures in the qualitative assessment. The qualitative method is easy operating, but does not give a numerical estimate of the effectiveness of the use of the countermeasure complex. [1]

Now there are many approaches and methods for analyzing the information security risks and information system reliability. So, Miloslavskaya N.G. and Senatorov M.Y. (2014) identified more than 40 foreign web-sites using tools to manage information security risks. [23]

Most of organizations that specialize in solving information security problems offer various methods for assessing information risks. Known methods can be divided into single-stage and multi-stage ones according to the type of decision-making procedure used in them. In a one-step methodology ("Risk Matrix"), risk assessment is performed using a one-time decisive procedure. In a multi-stage methodology (NIST, CRAMM), risk assessment is performed with a preliminary assessment of key parameters. The mechanism of risk assessment based on fuzzy logic is an expert system, in which certain rules form the knowledge base. For example, "table" logic or logic, reflecting the relationships formed by "if, ..., then" rules. The method for assessing the critical threats, assets and vulnerabilities (OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation) has a number of modifications for the enterprises of different sizes and types in the field of activity. [24]

Kukanova N. [25] carried out the comparative analysis of three such software complexes for analysis and control of information risks: British CRAMM (Insight Consulting company), American RiskWatch (RiskWatch company) and Russian GRIF (Digital Security company).

The CRAMM method (www.cramm.com) is a powerful and universal tool that allows, in addition to risk analysis, solving a number of other audit tasks, including:

- an information system scanning with the issuance of accompanying documentation;
- an audit in accordance with the requirements of the British government, standard BS 7799: 1995 "Code of Practice for Information Security Management";
- the development of a security policy and business continuity plan.

The method is based on a comprehensive (quantitative and qualitative) risk assessment approach.

CRAMM involves the separation of the entire procedure into 3 stages:

1) the determination of sufficiency for the application system protection of base-level facilities that implement traditional security functions, the need for more detailed analysis;

2) the identification of risks and evaluation of their value;

3) the choice of the countermeasures.

The conceptual scheme of the scanning according to the CRAMM method is shown in the Figure 1.

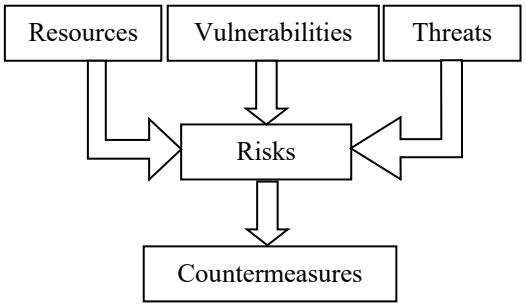

Fig. 1: The conceptual scheme of the scanning according to the CRAMM method

The RiskWatch software (www.riskwatch.com) is a powerful tool for risk analysis and management. It includes components for variety types of security audit and risk analysis:

- for physical methods of information system protection;
- for information risks;
- for assessment in compliance with the requirements of the HIPAA standard;
- for assessment the requirements of ISO 17799.

The annual loss prediction and assessment of the return on investment are used as criteria for assessing and managing risks in the RiskWatch method. The program is oriented to an accurate quantification of the ratio of losses from security threats and the costs.

In fact, the risk is estimated using the mathematical expectation of losses for the year. In addition, the "what if" scenarios are considered, which allow such situations to be assumed, provided that security measures are introduced. By comparing the expected losses, the effect of the proposed countermeasures is estimated.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The GRIF is a comprehensive system for analyzing and managing the organization's information system risks. The GRIF analyzes the level of security of all valuable resources, assesses the possible damage and allows effectively managing risks by choosing countermeasures.

The GRIF gives an opportunity to analyze the information system risks by analyzing the information flow model and the model of threats and vulnerabilities, depending on the user's initial data and data in outputting. [25]

COBRA is a risk analysis and assessment tool in compliance with BS7799 standard, which implements risk quantitative assessment methods and tools for consulting and safety reviews. COBRA uses the principles of building expert systems and an extensive knowledge base on threats and vulnerabilities and a multitude of questionnaires. The risk analysis is carried out at a basic level of security without risk level identifying.

Risk Advisor is an analytic's or manager's tool in the field of information security, that implements a technique which allows setting the model of information system from a perspective of information security, identifying risks, threats, incident loss. The tool allows documenting all possible aspects related to risk management at the upper levels (administrative and organizational levels). Assessment is given in qualitative scales without detailed analysis of the risk factors.

The Avangard system is software that is designed to solve security management tasks in large automated information systems. The main features of the system: a flexible organization model input and editing system, the ability to build a risk model, a system for risks assessing and comparing, evaluating the countermeasures, design countermeasure options and assessment residual risk.

The CONDOR includes the databases of information security management standards (ISO 17799: 2000, ISO 17799: 2005, ISO 27001, STO BR IBBS-1.0-2006), presented as a requirements list. In addition, the system supports the ability to create own requirements databases to give compliance assessment. The report reflects the provisions of the security policy. Expert advices are issued for the provisions that are not accomplished. The reports include the diagrams. The method for qualitative risk assessment is implemented on the risk level scale (high, medium and low).

A research on detection and measurement of information system risks through the adaptive management diagnostic expert systems was carried out by J.Janulevičius et al. [26] The aim of the research was to develop a model for the adaptive diagnostic expert system for risk analysis. The main task of the expert systems is the transfer of the necessary expert knowledge from an expert person to information system; therefore the knowledge kept in the system is the main factor of the most system's results. The process of knowledge forming in this area consists of the design of the system, the generation of rules, the definition of information necessary for the rules and the provision of each rule with values of probabilistic influence. The design of the system uses fuzzy logic, which allows describing events by associating them with probabilistic values. Taking into account the importance of current knowledge on information security risks and threats, the system knowledge base should be with constantly updated information. Most of this information is published in the periodic technical documentation and is presented in a structured form; therefore this part of the updating works can be automated by developing the appropriate module. The proposed module consists of a documentation fetcher, a information parser, a rule generator and rule import to knowledge base tool. The document fetcher periodically checks known sources to renew versions of existing documentation and fetches it as soon as newer version is detected. This documentation is processed by the information analyzer, which processes the text by taking the information necessary for the knowledge base of the expert system. As soon as the new facts become available in the module, it creates appropriate rules. The rules are checked for duplication in the system database. Thus, an automated update mechanism can fetch and analyze rules described and offered from a third-party source. [26]

So, we should note that the management of information risks is a costly, not simple and time-consuming process that requires the expert opinion. At the same time, the advantages that it gives significantly outweigh expended efforts and resources. Now there are a large number of approaches and software designed to simplify and automate the stages of risk management. [1]

Despite the importance of this direction, there is no domestic product for analyzing the risks and failures of information systems aimed at their reliability in Kazakhstan.

In [27-29], an approach that based on risk assessment and it neutralization to improve the reliability of information systems was considered. This approach allows giving risk assessment of the early stage of software development process and determining the most effective risk mitigation

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

strategies in cases where traditional methods cannot be applied. The approach is based on the adaptation of the RED [30, 31] and GREEN [32] methods to assess the risks of software systems, and reduces risk by using risk mitigation and it assessment strategies based on collected historical data on risk reduction.

The objective of information system reliability and fault tolerance has become especially relevant due to the fact that at present cloud technologies are becoming more widespread. The main advantages of cloud services are the scalability of resources, significantly low costs for infrastructure support. The large providers of the cloud service invested heavily in developing a massive access infrastructure for their customers around the world. Nevertheless, for the bulk of consumers, the issue of trusting their information to third-party cloud service providers is very acute. The heads of information technology departments of their companies that make decisions to move their own infrastructure to the cloud have doubts about reliability of cloud services. In this regard, the development of methods to increase the software fault tolerance and reliability, in particular in the cloud, is an important scientific and technical task. In [33-41], were developed methods and technologies that make possible to evaluate software fault tolerance using the method of diversification. This approach allows minimizing the cost of software development through standardized modeling languages to build business processes (BPMN - Business Process Model Notation, BPEL - Business Process Execution Language, etc.). The following results were obtained: the architecture of the solution, which makes possible to evaluate the software fault tolerance using the method of diversification was developed, also were developed models and protocols for the further development of middleware with the capabilities of: a) processing the operation with non-determinism in several WFE's work; b) allowing trouble-free WFE errors , c) synchronizing the interaction of several WFE with external services and devices; the algorithm of fault tolerance evaluation is implemented and specialized software for it application in cloud computing was developed; integration of the fault tolerance evaluation algorithm of the developed specialized software with the middleware, and the use of an integrated solution for the evaluating reliability indicators.

4. GLOBAL CYBERSECURITY INDEX

To implement the Decree of the President of the Republic of Kazakhstan "On measures to implement the President's Address "Third Modernization of Kazakhstan: Global Competitiveness" dated 15th February, 2017 No422 dated 31st January, 2017 the Decree of the Government of the Republic of Kazakhstan the Cybersecurity Concept ("Cybershield of Kazakhstan") until 2022 dated 30th June, 2017 No 407 was approved.

The Concept defines the main goal, which is to achieve and maintain the level of protection of information systems and information and communication infrastructure against threats and ensure sustainable development of the country. To achieve the goal, some tasks were formed:

- formation of conditions for raising awareness of threats, human capital development and development of the potential of the domestic industry to develop software and systems of cybersecurity;
- improvement of law enforcement practices and organizational and technical support for the safe use of information and communication technologies in the national system of information security and the security of automated process control systems;
- creation of a highly adaptive and integrated system of state information security management in the field of informatization and communication in relation to the entire national information and communication infrastructure. [9]

The expected results of the Concept are shown in Table 3.

One of the priority expected results of this Decree implementation is the constant growth of the global cybersecurity index of Kazakhstan, which includes a set of measures aimed at enhancing the country's cybersecurity.

The Global Cybersecurity Index is a measure of the cybersecurity level of a particular country.

According to the Global Cybersecurity Index 2017, compiled by the International Telecommunication Union (ITU), the top 5 countries of the global rating include the following countries: Singapore, USA, Malaysia, Oman and Estonia. In total there are 193 countries in the list. Kazakhstan took 83th place. The index of Kazakhstan in 2017 was reached and amounted to 0.352, exceeding the expected result set in the Concept.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 3: The Expected Results Of The Cybersecurity Concept ("Cybershield Of Kazakhstan") Until 2022 [9]

The global cybersecurity index is compiled on the basis of five criteria: legal, technical, organizational measures, capacity building and cooperation.

In order to determine the measures required to achieve the indicators set out in the Decree, we will consider further the methodology for calculating the global cybersecurity index, as well as the best practices of some countries.

The methodology for calculating the Global Cybersecurity Index in 2015 was to use a statistical model based on multicriteria analysis (MCA). The MCA established preferences when choosing among the several options, giving an indication of clearly defined objectives, and also proposing certain measurable criteria for assessing the extent to which the objectives were achieved. There is used a simple model of estimation by the method of linear addition. [42]

Notation:

X_{qc} - Value of the individual indicator q for country c, with q = 1, ..., Q and c = 1, ..., M.

I_{qc} - Normalized value of individual indicator q for the country c.

CI_c - Value of the composite indicator for country c.

For the comparative analysis was used the score of the hypothetical country, which is the maximum value of the overall readiness assessment (34 points). The resulting composite index ranges between zero (worst possible readiness) and one (the benchmark for comparative analysis):

$$CI_c = I_{qc} / 34$$

The normalization technique was based on a rating method:

$$I_{qc} = \text{Rank}\ (X_{qc})$$

The methodology for calculating the Global Cybersecurity Index in 2017 was changed and a new questionnaire including 25 indicators and 157 questions was compiled. The indicators of the Global Cybersecurity Index 2017 are shown in Table 4.

Table 4: The Indicators Of The Global Cybersecurity Index Of 2017 [43]

The whole concept of the new iteration of the Global Cybersecurity Index is based on the map of the tree of cybersecurity development and the binary response possibility. [43]

Table 5 shows the best practices of countries that have the best indicators for the Global Cybersecurity Index of 2017.

Table 5: The Best Practices Of Countries That Have The Best Indicators For The Global Cybersecurity Index Of 2017 [43-45]

5. DISCUSSION

Table 6 presents the results of Kazakhstan for each of the global index of cybersecurity indicators in the form of the total level of indicators achievement by the country.

Table 6: The Level Of Achievement Of The Global Index Of Cybersecurity Indicators By Kazakhstan. [43]

Talking about the positive aspects of Kazakhstan, which allowed reaching an indicator 0.352 in a short period of time, it is necessary to list the following:

- Modernization of legislative acts in the field of information and information security (modernization of the Law of the Republic of Kazakhstan No418-V dated 24th September, 2015 "On informatization", approval of the Cybersecurity Concept "Cybershield of Kazakhstan", Decree of the Government of the Republic of Kazakhstan dated 20th December 2016 No832 "On Approving Uniform Requirements in the Field of ICT and Information Security", Decree of the Government of the Republic of Kazakhstan dated 8th September, 2016 No529 "On Approving Rules and Criteria of the objects of information and communication infrastructure relating to critical objects of information and communication infrastructure", etc.);
- The establishment of the Information Security Committee of the Ministry of Defense and Aerospace Industry of the Republic of Kazakhstan, which exercises regulatory, implementation and monitoring functions, participates in the implementation of the strategic functions of the Ministry in the field of information security;
- National State and Branch Computer Emergency Response Team of Kazakhstan, the membership in the international organization-Forum FIRST (Forum of Incident Response and Security Teams);
- e-government portal and electronic digital signature (EDS) issuance centers. A lot of work on promoting EDS was done in Kazakhstan, where the number of valid digital signatures according to the information of the National Certifying Center of the Republic of Kazakhstan for September 2016 amounted to more than 3.8 million certificates.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- Educational programs for governmental specialists. Under the Office of the Prime Minister, there is a state institution "Center for training and improving the skills of specialists in the field of information security" in Kazakhstan, etc.

As can be seen from Table 6, the indicator "Cybersecurity Regulation" has a medium level. There are Laws "On Informatization", "On Personal Data and their Protection" and other normative legal acts in Kazakhstan. Criminal legislation provides for computer terminology and provides liability for violation of certain requirements in the field of information security. To improve this indicator requires the improvement of legislation in part of the development of a special regulatory act: 1) regulating in compliance with the rules of cybersecurity, for example, the US Federal Law on Information Security Management of 2002; 2) relating directly to specific aspects of cybercrime (for example, the British Law on the Unlawful Use of Computer Technologies of 1990)

The indicator "standards" is at a low level. To increase it, it is necessary to approve the state program for the application of internationally recognized standards of cybersecurity (standards developed by the following bodies: ISO, ITU, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, IEC, NERC, NIST, FIPS, PCI DSS, etc.) in the public sector and in the management of critical infrastructure.

The indicator "standards and certification for professionals" is also low and for its improvement it is recommended that the state approve a program for the certification and accreditation of state bodies and specialists in internationally recognized standards of cybersecurity. Such certification and accreditation programs and standards include the following: Cloud Security Knowledge (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, Cybersecurity Forensic Analyst (ISC), GIAC, GIAC GSSP (SANS), CISM, CISA, CRISC (ISACA), CompTIA, C|CISO, CEH, ECSA, CHFI, OSSTMM (ISECOM), PCIP / CCISP (Institute for Critical Infrastructure), Q / ISP, Technical Software Security Certification (Security Institute), CPP, PSP, PCI (ASIS), LPQ, LPC (Institute for Prevention of Damage), CFE (Association of Certified Investigators for Fraud), CERT-certified specialists for the elimination of a computer incidents (SEI), CITRMS (Institute for Financial Education of Consumers), CSFA (Cybersecurity Institute), CIPP (IAPP), ABCP, CBCP, MBCP (DRI), BCCP, BCCS, BCCE, DRCS, DRCE (BCM), CIA, CCSA (Institute of Internal Auditors), (International Association of Risk Professionals), PMP (Institute for Project Management), etc.

The "strategy" and "cybersecurity metrics" indicators are low. The development and adoption of Kazakhstan's cybersecurity strategy, as well as the use of officially recognized comparative analysis tools or reference materials used to assess the level of cyber security development, will significantly increase the low level of these indicators.

The indicator "responsible agency" is at an medium level. In addition to the existing government bodies responsible for meeting the requirements of information security, policies and strategies, it is necessary to create formal working groups, advisory councils or interdisciplinary centers in the field of cybersecurity.

The low level of the indicator "capacity building" indicates a lack of research, education and training programs in the field of cybersecurity in Kazakhstan, respectively, of qualified professionals and domestic products. Training qualified personnel in the field of information security and raising the level of specialists' qualification in the budgetary and state institutions is one of the engines for the successful development of the sphere of electronic public services and their security [46-48]

The "cooperation" indicator is at the lowest level relative to other indicators. Thus, interstate cooperation includes any officially recognized national and sector-specific partnerships for the exchange of materials on cybersecurity between different countries (i.e., bilateral or multilateral agreements). Interstate cooperation also includes such initiatives as implemented by the European Union, the Council of Europe, the G8, the Asia-Pacific Economic Cooperation (APEC), the Organization of American States (OAS), the Association of Southeast Asian Nations (ASEAN), the League of Arab States, the African Union, Shanghai Cooperation Organization (SCO), Network Operation Units (GSO), etc.

Interdepartmental cooperation includes national and sector-specific programs for the exchange of materials on cybersecurity in the public sector. These include initiatives and programs implemented jointly by different sectors, as well as by different departments / ministries.

Public-Private Partnerships (PPPs) are joint ventures between representatives of the public and private sectors. This performance indicator can be evaluated based on the number of officially recognized national and sector-specific PPPs for

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

sharing cybersecurity assets between the public and private sectors.

The "international cooperation" indicator refers to any officially recognized participation in international platforms and forums in the field of cybersecurity. Such cooperation initiatives include initiatives implemented by the following organizations: the UN General Assembly; International Telecommunication Union (ITU); Interpol / Europol; Organization for Economic Cooperation and Development (OECD); The United Nations Organizations on Drugs and Crime Problems (UNODC); The United Nations Interregional Crime and Justice Research Institute (UNICRI); Internet Corporation for Assigned Names and Numbers (ICANN); International Organization for Standardization (ISO); International Electrotechnical Commission (IEC); Internet Engineering Task Force; Forum of Incident Response and Security Team (FIRST).

It is also important to note that 41 measures are envisaged in the action plan for the implementation of the CyberSecurity Concept ("Cybershield of Kazakhstan") until 2022 (Decree of the Government of the Republic of Kazakhstan dated 28th October 2017 No676). In Table 7 was presented the main measures that are aimed at increasing the index of cybersecurity in Kazakhstan.

Table 7: The main measures for the implementation of the Cybersecurity Concept ("Cybershield of Kazakhstan") until 2022, which are aimed at increasing the cybersecurity index [49]

In addition to the measures listed in Table 7, we list some of the additional measures recommended by us for implementation:

- Preparation of a national strategy in the field of cybersecurity, based on the best foreign and international on the analogues. Following the example of other leading countries in the rating, state bodies responsible for the formation of a cybersecurity policy should, based on international experience, work out and adopt a national cybersecurity strategy with an action plan that takes into account organizational and technical measures and reflects the current state of technological development;
- Adoption of the state road map on cybersecurity;
- Training of specialists not only technical specialization, but also organizational and legal;
- Development of a special regulatory act that regulates in compliance with cybersecurity rules, and is directly related to specific aspects of cybercrime, including the regulation and reduction of SPAM mailings in Kazakhstan;
- Approval of the list of critical objects of the information and communication infrastructure and implementation of measures aimed at their protection, etc.

However, given the fact that in the countries with the best indicators of the global cybersecurity index the Council of Registered Ethical Security Testers (CREST) was established, it is recommended to consider the possibility of Kazakhstan's official membership in CREST.

Also, based on the experience of other countries in the world, it is recommended that the Computer Security Incidents Response Team be established on the basis of universities in order to thoroughly analyze the ongoing security incidents and develop domestic products to prevent them (in Brazil – Computer Security Incidents Response Team CAIS RNP, in Norway - UiO-CERT, in the Netherlands - CERT-UU, etc.)

6. CONCLUSION

Analysis of the methods and technologies of reliability and security of information systems and information and communication infrastructures functioning shows that dozens of the foreign software products for risk analysis and audit of the organizations are currently known: Risk Watch (USA), CRAMM (United Kingdom), COBRA (United Kingdom) , "AvanGard" (Russia), GRIF (Russia), CONDOR (Russia) and others.

Now Kazakhstan does not have domestic software for risk analysis, despite the need for such a product both state bodies and critical infrastructure [50-51]. At the same time the risk assessment plays the main role in ensuring information system reliability. Considering the importance of the domestic software development aimed at ensuring information system reliability and security, further research to develop the approach for risks assessing and ensuring the software reliability proposed in [27-29] is needed.

Analysis of developed countries best practices related to for cybersecurity issues made it possible to identify the measures needed to improve the global cybersecurity index of Kazakhstan, which are recommended to be included in the action plan for the implementation of the Cybersecurity Concept ("Cybershield of Kazakhstan") until 2022:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- the development of the national cybersecurity strategy based on the best foreign and international analogues;

- the development of the action plan that takes into account the organizational and technical measures and reflects the current state of technological development, the adoption of the state road map on cybersecurity;

- the development and use of domestic products, the granting state grants to the domestic IT companies, universities and research institutes for the creation of these products;

- updating educational programs (secondary, graduate and postgraduate education) in terms of adding information security courses, increasing the number of grants in the field of information security, training of specialists in the field of cybersecurity, not only technical specialists, but also legal specialists and managers;

- the modernization of legislation, the development of a special regulatory act that regulates in compliance with cybersecurity, and relating directly to specific aspects of cybercrime, including the regulation and reduction of SPAM mailings in Kazakhstan;

- approval of a program for the application of internationally recognized standards for cybersecurity in the public sector and in the management of critical infrastructure;

- approval of the certification and accreditation program based on internationally-recognized standards of cybersecurity for state bodies and specialists;

- the preparation of an annual report on the country's state of cybersecurity on the model of other countries best practices, the use of officially recognized comparative analysis tools or reference materials to assess the level of cybersecurity development;

- the establishment of official working groups, advisory councils and interdisciplinary centers in the field of cybersecurity;

- the organization of research, education and training programs in the field of cybersecurity, qualified specialists training and the development of domestic products to monitor and detect botnets and other information security threats, to analyze risks and ensure information systems reliability, etc.;

- approval of the list of critical objects of information and communication infrastructure and implementation of measures to protect them;

- the development of international cooperation in the field of information security, including officially recognized national or sector-specific partnerships for sharing cybersecurity assets across borders with other nation states, signing of bilateral and multilateral agreements;- the development of interdepartmental cooperation in the field of information security, including national and sector-specific programs for sharing cybersecurity assets in the public sector;

- organization of joint ventures of representatives of the public and private sectors;

- organization of regular information of the population on the protection of personal data, cybersecurity issues;

- membership in such organizations in the field of information security, as the Council of Registered Ethical Security Testers (CREST);

- organization of Computer Security Incidents Response Team on the basis of universities in order to analyze deeply security incidents, develop domestic products to prevent the incidents, work in this field with undergraduate, graduate and doctoral students;

- the implementation of other measures based on continuous monitoring and analysis of the world experience in the field of cybersecurity.

Acknowledgment

This work is supported by grant financing of the Ministry of Education and Science of the Republic of Kazakhstan for 2018-2020, grant № AP05131784.

REFERENCES:

[1] Shvalev I.S., Chusavitina G.N., Davletkireyeva L.Z.. Comparative characteristics of automated tools for managing information risks. *Electronic scientific and practical journal "Modern scientific research and innovations"* http://web.snauka.ru/issues/2012/11/18524.

[2] http://kz-cert.kz/page/604.

[3] http://kz-cert.kz/page/567.

[4] http://kz-cert.kz/page/570.

[5] Juknius J., Goranin N. "Botnet spreading detection and prevention via website". *Journal of young scientists.* Šiauliai: Šiaulių universitetas. Nr. 1(26), priedas (2010), p. 293-298.

[6] Zorin K.M. "Forecasting of network attacks using machine learning methods and data mining. Information security of Russian regions" (IBRD-2013). St. Petersburg Interregional Conference: *Proceedings of the Conference*. - 2013.-St. Petersburg, p. 293.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[7] Goranin N. "Genetic algorithm application in information security systems " (2010). *Doctoral Dissertation.*

[8] Čenys A. "Malware propagation modeling by the means of genetic algorithms." *Elektronika ir elektrotechnika.* 2008, No. 6(86), p. 23-26.

[9] Goranin N.; Čenys A. "Genetic algorithm based internet worm propagation strategy modeling". *Information technology and control* / Kaunas University of Technology. Kaunas: Technologija. Vol. 37, no. 2 (2008), p. 133-140.

[10] Goranin N., Čenys A. "Genetic algorithm based Internet worm propagation strategy modeling under pressure of countermeasures". *JESTR.* Kavala: Kavala Institut of Technology. Vol. 2, iss. 1 (2009), p. 43-47.

[11] Goranin Nikolaj; Čenys Antanas; Juknius Jonas. Malicious Botnet survivability mechanism evolution forecasting by means of a genetic algorithm. *Science – future of Lithuania: Electronics and electrical engineering.* Vilnius: Technika. ISSN 2029-2341. T. 4, nr. 1 (2012), p. 13-19.

[12] Goranin N., Čenys A., Juknius J. "Extension of the genetic algorithm based malware strategy evolution forecasting model for botnet strategy evolution modeling". *Information assurance and cyber defence: symposium organised by the Information Systems and Technology Panel, Estonia/ NATO, Partner for Peace Nations and Med Dialogue Nations.* Tallinn: Research and Technology Organisation, 2010, p. 1-20.

[13] Juzonis V., Goranin N., Čenys A. "Genetic algorithm modeling approach for mobile malware evolution forecasting. *Information technologies'2010: proceedings of the 16th international conference on Information and Software Technologies*, IT 2010. Lithuania, 2010. Kaunas: Technologija, 2010.

[14] Goranin N., Čenys A. "Analysis of malware propagation modeling methods". *11-osios Lietuvos jaunųjų mokslininkų konferencijos „Mokslas – Lietuvos ateitis" 2008 metų teminės konferencijos INFORMATIKA*. Vilnius: Technika, 2008, p. 428-434.

[15] Goranin N.; Čenys A. "Evolutionary algorithms application analysis in biometric systems". *JESTR*. Kavala: Kavala Institut of Technology. Vol. 3, iss. 1 (2010), p. 43-47.

[16] Čenys A.; Gibavičius D.; Goranin N.; Marozas L. "Genetic algorithm based palm recognition method for biometric authentication systems". *Elektronika ir elektrotechnika*. Kaunas: KTU. Vol. 19, no. 2 (2013), p. 69-74.

[17] Juzonis V.; Goranin N.; Čenys A.; Olifer D. "Specialized genetic algorithm based simulation tool designed for malware evolution forecasting". *Annales UMCS Informatica.* Lublin: Versita. Vol. 12, iss.4 (2012), p.23-37.

[18] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf.

[19] Decree of the Government of the Republic of Kazakhstan "On the approval of the Cybersecurity Concept ("Cybershield of Kazakhstan")" dated 30th June 2017 No. 407.

[20] Malkov M.V. On the Reliability of Information Systems Proceedings of the Kolsk Science Center of the Russian Academy of Sciences. - 4/2012 (11). *Information Technology.* - Apatity: Publ. KNC RAS. -2012, pp.49 - 58.

[21] Osipenko N.B. "The basics of software standardization and certification: reliability and quality of software: practice direction for students of the specialty 1-40 01 01 *"Information Technology Software"* / ME of. RB, F. Skaryna Gomel State. un-ty, 2014 – p.57.

[22] Rasulova S.S. "Reliability of Information Systems: Lecture notes". *Tashkent: TashGTU,* 2007, -p. 117.

[23] Miloslavskaya N.G., Senatorov M.Yu. "Information Security Risk Management." - *Moscow: Hot line-Telecom*, - 2014, p.130.

[24] Agishev T.Kh., Khasanov Sh.A. "Tools for information security risks managing". *Materials of the international scientific and practical conference "Information technologies. Problems and Solutions"* - 2017", Ufa, 2017, p.291 - 295.

[25] Modern methods and tools of risk analysis and management of companies information systems https://dsec.ru/ipm-research-center/article/modern_methods_and_means_for_analysis_and_risk_management_of_information_systems_of_companies/.

[26] Janulevičius J.; Šiaudinytė L.; Čenys A.; Goranin N. "Detection and measurement of information system risks through adaptive management diagnostic expert systems." *12th IMEKO TC10 Workshop on Technical Diagnostics: New Perspectives in Measurements, Tools and Techniques for*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Industrial Applications. Italy: IMEKO, 2013, p. 45-49.

[27] Boranbayev A.S., Boranbayev S.N., Yersakhanov K.B., Nurusheva A.M. "Methods of information systems reliability." *Bulletin of ENU*, №2 (117), Astana, 2017, p. 61-70.

[28] Boranbayev A.S., Boranbayev S.N., Yersakhanov K.B., Nurusheva A.M. "Identifying of potential software failures and neutralizing them". *A collection of reports of the IV International Scientific and Practical Conference - Astana: ENU*, 2017, p.338-340.

[29] A. Boranbayev, S. Boranbayev, K. Yersakhanov, A. Nurusheva, and R. Taberkhan. "Methods of Ensuring the Reliability and Fault Tolerance of Information Systems". *15th International Conference of Information Technology, Information Technology - New Generations*, (2018), pp. 729-730.

[30] K.G.Lough, R. Stone, and I. Tumer. Prescribing and implementing the risk in early design (RED) method. *In Proceedings of DETC'06,* number DETC2006-99374, PA, 2006.

[31] K.G. Lough, R.B. Stone, I.Y. Tumer Implementation procedures for the risk in early design (red) method. J Ind Syst Eng 2 (2008), (2), pp. 126-143.

[32] Krus, Daniel A., "The risk mitigation strategy taxonomy and generated risk event effect neutralization method" (2012). *Doctoral Dissertations.*

[33] Boranbayev S.N., Popov P., Altayev S.A. The Usage Of Design Diversity For Software Fault Tolerance And Reliability. *Materials of the republican scientific-practical conference "Problems of application of modern mathematical methods and computer technologies in engineering sciences and construction" - Astana: ENU,* 2013, p.237-243.

[34] Boranbayev S.N., Popov P., Altayev S.A. Software Reliability Issues. Materials *international scientific-practical conference "Actual problems of computer science and management processes".* -Almaty, 2012, p.61-65.

[35] S.Boranbayev, A.Boranbayev, S.Altayev. Development of a mathematical model for designing reliable information systems and its properties. *The 2014 International Conference on Software Engineering Research and Practice (SERP'14),* USA, 2014, P. 286-290.

[36] S.Boranbayev, A.Boranbayev, S.Altayev, A.Nurbekov. Mathematical model for optimal designing of reliable information systems. *Proceedings of the 2014 IEEE 8th International Conference on AICT2014*, Kazakhstan, 2014, pp.123-127.

[37] S.Boranbayev, A.Boranbayev, S.Altayev, Y.Seitkulov. "Application of diversity method for reliability of cloud computing." *Proceedings of the 2014 IEEE 8th International Conference on AICT2014,* Kazakhstan, 2014, pp.244-248.

[38] S.Boranbayev, S.Altayev, A.Boranbayev, "Applying the method of diverse redundancy in cloud based systems for increasing reliability". *Proceedings of the 12th International Conference on Information Technology: New Generations* (ITNG 2015), 2015, USA, pp.796-799.

[39] S.Boranbayev, A.Nurbekov. Development of the methods and technologies for the information system designing and implementation. *Journal of Theoretical and Applied Information Technology*, 2015, Vol.82, No.2, pp.212-220.

[40] S.Boranbayev, A.Boranbayev, A.Nurbekov, S.Altayev. "The method of design and development of information systems". *Proceedings of the 7th ICLTET'2015*, South Africa, pp.145-149.

[41] Boranbayev A.S., Boranbayev S.N., Karasayeva K. Reliability of software systems based on the method of diversification. *Bulletin of ENU*, №4, 2016, p.64-70.

[42] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-R.pdf.

[43] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

[44] https://psm7.com/news/nazvana-samaya-kiberbezopasnaya-strana-evropy.html.

[45] https://digital.report/globalnyiy-indeks-kiberbezopasnosti-ot-itu-gruziya-i-rossiya-voshli-v-top-10/.

[46] Boranbayev S.N., Nurusheva A.M., Yersakhanov K.B. "The modern state and the further development prospects of information security in the Republic of Kazakhstan." *Herald of ENU*, №1 (119), Astana, 2017, pp. 52-62.

[47] Boranbayev S.N., Nurusheva A.M., Yersakhanov K.B. Analysis of the state of information security of the Republic of Kazakhstan and prospects for its development.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A collection of reports of the IV International Scientific and Practical Conference - Astana: ENU, 2017, p.341-344.

[48] A. Boranbayev, S. Boranbayev, K. Yersakhanov, A. Nurusheva, and R. Taberkhan. "The Modern State and the Further Development Prospects of Information Security in the Republic of Kazakhstan". *15th International Conference of Information Technology, Information Technology - New Generations*, (2018), pp.33-38.

[49] http://adilet.zan.kz/rus/docs/P1700000676.

[50] Boranbayev S.N., Tasmagambetov O.K., Baidildina M. (2016): "Methods for safety and reliability of information systems". *Herald of ENU,* 2, pp.33-40.

[51] Boranbayev S.N., Tasmagambetov O.K. (2016): "Forms and methods of integration of information systems for law enforcement of Kazakhstan." *Herald of ENU*, 2, pp.26-32.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: The Factors That Influence Reliability Of Information System At The Various Stages [20]

Factors that influence reliability during design stage	**Factors that influence reliability during the manufacturing stage**	**Factors that influence reliability during exploitation stage**
the number and quality of elements in the system	the quality of materials	personnel qualifications
the elements operation mode	the quality of material and component storage	the external conditions (climatic conditions, vibration, overload, etc.)
the use of standard and unified elements	compliance with manufacturing and assembly technology	time factor

Table 2: The Classification Of Software Reliability Models [21]

Software reliability models					
Analytical				Empirical	
Dynamic		Static			
Discrete	Continuous	Error area	Data area	The complexity model	The model that determines time for debugging programs
The Schumann's model	The Jelinski-Moranda model	The Mills model	The Nelson model		
The LaPadula model	The Muse model	The Lipov Model			
The Schick-Wolverton model	The model of transition probabilities	The simple intuitive model			
		The Corcoran model			

Table 3: The Expected Results Of The Cybersecurity Concept ("Cybershield Of Kazakhstan") Until 2022 [9]

	2018	2019	2020	2021	2022
Global cybersecurity index	0,3	0,4	0,5	0,55	0,6
Increase awareness of information security threats	-	by 5%,	by 10%	by 15%	by 20%;
Number of retrained specialists in the field of information security	300	500	600	700	800
An increase in the share of domestic software in the field of informatization and communication used in the state and quasi-public sectors	by 10%,	by 20%,	by 30%	by 40%	by 50%;
The share of the use of domestic security certificates for encrypted transfer of the data by Internet resources with .KZ domain name.	20%	40%	60%	80%	100%
The share of information systems of state bodies, non-state information systems, integrated with state ones, critical objects of information and communication infrastructure, connected to the information security monitoring centers	20%	40%	60%	80%	100%

Table 4: The Indicators Of The Global Cybersecurity Index Of 2017 [43]

Legal	**Technical**	**Organizational**	**Capacity Building**	**Cooperation**
Cybercriminal Legislation	National CIRT	Strategy	Standardization bodies	Intra-state Cooperation
Cybersecurity Regulation	Government CIRT	Responsible agency	Good practices	Multilateral agreements
Cybersecurity Training	Sectoral CIRT	Cybersecurity Metrics	R&D programmes	International participation
	Standards for organizations		Public awareness campaigns	Public-Private Partnerships
	Standards and certification for professionals		Professional training courses	Inter-agency partnerships
	Child online protection		National education programmes and academic curricula	
			Incentive mechanisms	
			Home-grown cybersecurity industry	

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 5: The Best Practices Of Countries That Have The Best Indicators For The Global Cybersecurity Index Of 2017 [43-45]

Country	Innovate experience	Place in the rating
Singapore	There is a long history of initiatives on cybersecurity in the state. It launched its first master plan for cybersecurity back in 2005. The Cybersecurity Agency was established in 2015 as a specialized unit for cybersecurity oversight, and the country issued a comprehensive strategy in 2016 (https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.aspx ? la = en). Internet content providers and Internet access service providers are licensable under the Broadcasting Act and they are required to comply with the Internet Code of Child Protection Practices on the Internet. Since 2012, all service providers have been legally obligated to offer filtering services with Internet subscriptions and inform consumers about them when they subscribe. The authorized body for media development also blocks 100 pornographic and extremist websites.	1
The USA	To coordinate cybersecurity among all states, the National Governor's Association established the Cybersecurity Resource Center, which presents best practices, tools and guidelines for all states (https://www.nga.org/cms/center/issues/hsps/state- cybersecurity).	2
Malaysia	The state body responsible for information security in Malaysia offers professional training via higher education institutions in Malaysia. It supports the Cyberguru website, dedicated to professional security training (http://www.cyberguru.my).	3
Oman	Has a robust organizational structure, including a high-level cybersecurity strategy, a master plan and a complete roadmap.	4
Estonia	Since 2007, when Estonia became the first country in the world to become a victim of cyberconflict, here the cybersecurity sector began to develop rapidly. Estonia signed a treaty on the development of cybersecurity with Austria, Luxembourg and South Korea.	5
Mauritius	The Botnet Tracking and Detection Project allows the Mauritian Computer Emergency Response Team (CERT-MU) to actively take measures to curtail threats in the country's network. The State Information Security Unit conducted 180 awareness sessions for approximately 2000 state employees in 32 state ministries and departments.	6
Australia	There is a certification program for information security provided by the Council of Registered Ethical Sacurity Tester (CREST) in the country. Modeled after CREST, the Council provides assessment, accreditation, certification, education and training in the field of cyber and information security for individuals and legal entities in both Australia and New Zealand. Also, CREST was established in the UK, USA, Singapore and Hong Kong.	7
Georgia	After large-scale cyber attacks on the country in 2008, the government of Georgia has strongly supported protection of the country's IT systems. The Information Security Law created a special Cybersecurity Bureau. Its main task is to protect the most important systems of the Ministry of Defense of Georgia. It is worth noting that the Georgian legislation on cybercrime meets the principles and rules of the Budapest Convention, including in terms of procedures. Illegal access, interference in the operation of systems, malicious use of technological devices is criminalized by the Criminal Code of the country. The law on the protection of personal data was adopted by Parliament in 2011 and is designed to protect human rights and freedoms, including the right to privacy in the processing of personal data.	8
France	There is cybersecurity training courses are widely distributed in France, the National Agency for Information Systems Security publishes a list of universities that provide accredited cybersecurity degrees.	8
Canada	The Personal Information Protection and Electronic Documents Act (PIPEDA) contains several sections relating to cybersecurity and requires organizations to notify authorities in the event of privacy breaches. The concealment entails appropriate penalties.	9
Russia	Among the CIS countries, Russia showed the best results in capacity building in the field of cybersecurity. This area includes the development of standards for cybersecurity, R&D, public awareness, and the promotion of a home-grown cybersecurity industry. There is actively improving the legislation in Russia: National Security Strategy was officially approved in 2000, National Security Concept and Foreign Policy Concept – in 2013. In 2000, the President signed the first Information Security Doctrine of the Russian Federation. All state bodies inspect networks and IT systems in accordance with regulatory annual requirements.	10
Norway	In addition to laws on cybersecurity, Norway has also conducted research on its cybersecurity, including surveying citizens about the degree to which they will accept monitoring of their online activities. Denmark, Finland, Iceland, Norway and Sweden cooperate in the framework of the Nordic National Cooperation CERT. It includes technical cooperation and cybersecurity activities to assess and strengthen cyber-preparedness, examine incident response processes and enhance information sharing in the region	11
The United Kingdom	The UK issued its second five-year Strategy for national cybersecurity in 2016. The strategy issued by the Cabinet Office aims at making the country one of the safest places in the world to carry out online business and doubles investments in cybersecurity compared to the first plan. The UK is working with the local company Netcraft on initiatives in the field of cybersecurity.	12

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

	There is a combating phishing and malicious programs in the UK, as well as phishing aimed at the government. The partnership helped to stop 34,550 potential attacks on government departments in the last 6 months of 2016 or 200 incidents a day.	
Korea	Korean Internet Security Agency (KISA) is committed to creating a network basis for Internet users and Internet companies by increasing competitiveness of Internet services and reliability of Internet information and knowledge. KISA supports start-ups to commercialize their business models and enhance competitive advantage in security technologies through programs aimed at developing startups in the Internet-of-things, security and Fintech industries. They also created the one-stop service to support start-ups to make a profit not only in the domestic market, but also in the world market to expand their business models.	13
Netherlands	An annual report on the cybersecurity assessment of Netherlands is published. The National Center for Cybersecurity (NCSC) collects reports on security and incidents. These metrics allow trends to be observed and acted on.	15
Germany	In 2009, Germany signed an agreement on cooperation in the field of information security research between the Federal Ministry of Education and Research (BMBF) and the Federal Ministry of the Interior Affairs. The IT security research program covers research and development in the field of new information security technologies. Since 2011, BMBF has supported 3 research centers that unite the leading institutions in the field of cybersecurity.	24
Belarus	A special feature of Belarus is that initiatives to protect children include public-private partnerships. The Ministry of Education together with the MTS operator implemented a program to teach children about safe use of the Internet, that has so far reached about 6000 children.	39 (3 place among CIS countries)
Bulgaria	In 2009, Bulgaria established the International Cyber Investigation Training Academy, which is a non-governmental organization. The Academy aims to improve the skills of specialists working in the field of cybersecurity. It has trained over 1300 people from the public and private sectors.	44
Kenya	The Kenyan Educational Network (KENET) is the National Network for Research and Education (NREN). KENET is the Computer emergency response team (CERT) for the academic community and is licensed by the Communications Authority of Kenya (CA) as a non-profit operator serving educational and research institutions. It provides an affordable, effective and low-congestion Internet bandwidth services for universities in Kenya.	45 (3 place among African countries)

Table 6: The Level Of Achievement Of The Global Index Of Cybersecurity Indicators By Kazakhstan. [43]

Global cybersecurity index indicators	Level of achievement of indicators by Kazakhstan
Cybercriminal Legislation	High
Cybersecurity Regulation	Medium
Cybersecurity Training	Low
Legal	Medium
National CIRT	High
Government CIRT	High
Sectoral CIRT	High
Standards for organizations	Low
Standards and certification for professionals	Low
Child online protection	High
Technical	High
Strategy	Low
Responsible agency	Medium
Cybersecurity Metrics	Low
Organizational	Low
Standardization bodies	Medium
Good practices	Low
R&D programmes	Medium
Public awareness campaigns	Low
Professional training courses	High
National education programmes and academic curricula	Medium
Incentive mechanisms	Low
Home-grown cybersecurity industry	Low
Capacity Building	Low
Intra-state Cooperation	Low
Multilateral agreements	Low
International participation	High
Public-Private Partnerships	Low
Inter-agency partnerships	Low
Cooperation	Low
Result	Low

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 7: The main measures for the implementation of the Cybersecurity Concept ("Cybershield of Kazakhstan") until 2022, which are aimed at increasing the cybersecurity index [49]

Organizational and legal measures	Carry out issues aimed at: - use of domestic products and provision of state grants to domestic IT companies; - creating a registry of trusted software products; - improvement of legislative acts on issues of information security; - Creation of a council on cybersecurity issues; - updating of standards in the field of information and communication technologies and information security; - accreditation and licensing of activities for the audit of information security and pentistry; - development of the project of target scientific program for the development of the electronic industry (2021-2025) and the project of the target scientific and technical program on information security (2018-2020).
Organizational and technical measures	Carry out measures aimed at: - attraction of specialists and students in the field of information security for cooperation with enterprises of the electronic industry, research and development laboratories for the implementation of projects in the field of cybersecurity; - creation: • Information system "Portal of information security"; • Methods for defining typologies and models of information security threats in the field of informatization, as well as creating and developing industry and departmental operational information security centers; • National Information Security Coordination Center; • Single backup storage of critical data of state bodies information systems; • Cybersecurity sectors for building domestic capacity; • Center for training and professional development of cybersecurity specialists on the basis of "Astana EXPO-2017" infrastructure; • systems for the effective protection of departmental information resources of the authorized body in the field of defense; - development of international cooperation in the field of information security; - development of recommendations on building up Kazakhstan's potential in the field of scientific and educational activities in the field of cybersecurity.
Human Resource Management	- renewal of educational programs; - an increase in grants for the specialty "Information Security Systems".
Promotion of measures for the safe use of information and communication technologies	- public awareness about the protection of personal data, cybersecurity issues; - modernization of the secondary education program.