BRITISH VIEW

MULTIDISCIPLINARY JOURNAL

www.britishview.co.uk

Anthropologie, Applied Linguistics, Applied Physics, Architecture, Artificial Intelligence, Astronomy, Biological Sciences, Botany, Chemistry, Communication studies, Computer Sciences, Computing technology, Cultural studies, Design, Earth Sciences, Ecology, Education, Electronics, Energy, Engineering Sciences, Environmental Sciences, Ethics, Ethnicity and Racism Studies, Fisheries, Forestry, Gender Studies, Geography, Health Sciences, History, Interdisciplinary Social Sciences, Labour studies, Languages and Linguistics, Law, Library Studies, Life sciences, Literature, Logic, Marine Sciences, Materials Engineering, Mathematics, Media Studies, Medical Sciences, Museum Studies, Music, Nanotechnology, Nuclear Physics, Optics, Philosophy, Physics, Political Science, Psychology, Publishing and editing, Religious Studies, Social Work, Sociology, Space Sciences, Statistics, Transportation, Visual and Performing Arts, Zoology and all other subject areas.

Manuscripts typed on our article template can be submitted through our website here. Alternatively, authors can send papers as an email attachment to editor@britishview.co.uk
Editor Multidisciplinary Journals

British View ISSN 2041-3963 Volume 8 Issue 5 2023
Universal impact factor 8.528
SJIF 2022: 4.629

ANALYTICAL METHOD OF FORECASTING THE SECURITY LEVEL OF INFORMATION SYSTEMS BASED ON A TIME SERIES MODEL

Djamatov Mustafa Khatamovich,

associate professor of the Department of Information Technologies of the Ministry of Internal Affairs of the Republic of Uzbekistan

Mirzaeva Malika Bakhadirovna,

associate professor of the department "Hardware and software of management systems in telecommunications"

Abstract: This paper is based on modern approaches and methods of predicting a certain level of predicting a certain level of security with the help of the need to protect the level of security in the information system,which is considered the most important today. The method of increasing the accuracy and reliability of the assessment of the security level of information systems based on the collected databases and time series model of their weaknesses has been developed. In working on the dissertation, using information protection methodology, system analysis methods, set theory, probability theory, time series theory, developing the concept of building information systems with a predetermined level of security is formed and secured with security mechanisms, web servers, the use of the interaction protocol and the timely understanding of the impact of disruptive ideas and their prevention was formed.

Keywords: IT, Uz domain, CYBER security

In order to ensure information security, every country and organization is creating and developing different levels of tools and methods. In the Republic of Uzbekistan, in this field, "On Principles and Guarantees of Freedom of Information", "On Informatization", "On Improvement of the Regulatory Legal Framework in the Field of Use of Electronic Digital Signatures" , "Regarding increased liability for illegal actions in the field of information and data transmission" and "Additional

measures to ensure computer security of national information and communication systems" acceptance and implementation is a clear indication of this.

As a result of the expansion of information and communication systems, their security problems are also increasing. It is more effective to use a complex method rather than a single method in estimating information security in these networks. This, in turn, creates the need to research and analyze the protection methods used in information and communication systems. Unsolicited unsolicited e-mail affects the security of users' sensitive information. Along with spam, programs can be sent that can lead to complete or partial destruction or corruption of information. They can attach malware to spam messages to steal users' credit card numbers, usernames, and passwords. In accordance with the security policy adopted by the organization, it is necessary to control not only incoming but also outgoing traffic. Despite the use of spam detection tools by organizations and individual users, the overall share of spam messages is very high.

The relevance of information protection problems is generally taken into account, which is confirmed by high-ranking proceedings on illegal activities with protected information. Damages to companies due to information security breaches are estimated at trillions of dollars. At the same time, the analysis of crime statistics shows that there are serious problems in this area, mainly due to shortcomings in the design and operation of protective equipment.

To date, the need for information protection is indisputable, that is, any system developed and implemented must adequately protect the functions of the information processed in the system against existing threats. Undoubtedly, information protection should be comprehensive, and at the same time, it is necessary to take into account the possibility of threats specific to this particular information system. At the analysis stage, important details should not be missed and, at the same time, some of them should not be overestimated, because this would incur unreasonable financial and material costs for the organization of a system to prevent such situations. During the system design phase, it is necessary to determine what level of protection the final

system should have, and during the testing phase, it is necessary to be able to evaluate the security parameters of the final system and compare them with the initial security task. At the stage of testing, it is necessary to use an effective analysis algorithm to assess the security of the system, the results of which will not depend on the qualifications of the auditor's expertise. To date, there are no standardized, accurate, and high-level IP protection analysis methods, although recently efforts to address this issue have begun to emerge. In each case, the auditors' behavior algorithms can differ significantly, which in turn can lead to significant differences in the evaluation results. **Scientific novelty of the results**

• Based on the division of the entire system into subsystems, an extended model of security assessment of complex information systems - blocks with specific characteristics of the level of vulnerability - is proposed. Within the framework of the proposed concept, it becomes possible to create systems with predefined safety features, which, in turn, increases the reliability of the system in the long term.

• A new method of assessing the level of IP protection is proposed, which allows to predict more reliable results using a time series model based on databases of vulnerabilities of information systems collected by the world community, in contrast to existing expert assessments.

• Using the set-theoretic approach, a new structural and functional model of vulnerability is proposed, which allows to parametrically describe each vulnerability, systematize and compile existing information on vulnerabilities in order to create appropriate databases for automated audit systems.

CONCLUSION

The main methods of analyzing the level of protection of information systems used in the modern world were considered in the thesis work. A detailed analysis of these methods showed a significant influence of the subjective factor on the person of the audit expertise, as well as the inability to predict the development of security indicators. The method of building predictive models of changes in the level of vulnerability of information systems based on the data obtained from international

vulnerability databases developed during the dissertation research made it possible to significantly increase the accuracy and reliability of the results of the assessment of the security of information systems.

Based on the above definitions of methods and methods of analyzing information systems for the availability of safe connections, a number of requirements for the proposed scanning system can be formulated. Such a system should have the following properties:

• Improved test request/response definition grammar specifically designed for high performance, simultaneous use of multiple non-blocking sockets, and maximum efficiency

• Determine the name of the program and, if possible, its version number

• Support for TCP and UDP protocols, as well as support for text-based (ASCII) and batch binary services.

• Support for various platforms such as Linux, Windows, Mac OS X, FreeBSD / NetBSD / OpenBSD, Solaris.

• Full IPv6 support over TCP, UDP and SSL.

• Identify unknown services. If data is received from a previously unknown service, a new "fingerprint" must be entered into a special database.

• Maintenance and operating system fingerprint database required.

• Security of the scanning process, ie: prevention of various buffer overflows, misinterpretation of string words, control sequence processing, etc.

• The system should have a scalable modular architecture to enable continuously updated coverage of the scanning and analysis process for emerging threats and vulnerabilities.

It is necessary to implement a constantly updated database of vulnerable services with a description of the possibility of eliminating these vulnerabilities.

The availability of a scripting language to manage scanning actions and the ability to describe the process of discovering new vulnerabilities to increase the ease of filling vulnerability databases.

The existence of a universal validator (interpreter) of XML-passports, capable of distinguishing a passport with any XML-structure.

The following results were obtained:

• An analysis of existing directions and methods of assessing the level of security of information systems is carried out. In the analysis, it was found that the issues of obtaining reliable results of the analysis of the level of protection and its prognosis were not sufficiently developed.

• Based on the expected access points, an extended model for assessing the security of complex information systems and dividing the entire system into subsystems - blocks with specific characteristics of the level of vulnerability - was developed. Within the framework of the proposed concept, it becomes possible to create systems with predefined safety features, which, in turn, increases the reliability of the system in the long term.

• A method for assessing the level of IP protection has been developed, which allows to predict more reliable results using a time series model based on databases of vulnerabilities of information systems collected by the world community, in contrast to existing expert assessments.

• A structural and functional vulnerability model was developed using a set-theoretic approach, which allows for parametric description of each vulnerability, systematization and compilation of available information on vulnerabilities in order to create appropriate databases for automated audit systems.

• Using heuristic vulnerability analysis methods (CISGuard software package), the architecture and prototype of the system for dynamic analysis of computer network security was developed. The advantages of the proposed complex include its openly scalable architecture and the use of integrated vulnerability databases. The practical results were obtained on the basis of automated analysis of computer networks of a number of local enterprises, which demonstrate the effectiveness of the proposed methods and technologies for security analysis.