Aspects of the development of the comprehensive information security system in the information systems

Nosyk Andrii[1]
Kucherenko Yurii[2]
Nosyk Kateryna[3]

[1]National Technical University "Kharkiv Polytechnic Institut", 22 Kyrpychova str, Kharkiv UA-61002, Ukraine, nampbch@gmail.com
[2]Kharkiv National Air Force University of Ivan Kozhedub , 77/79 Sumska str, Kharkiv UA- 61023, Ukraine,kucherenkoYF@gmail.com
[3]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, kateryna.nosyk@nure.ua

Abstract. *Here are considered some aspects on the comprehensive information security system development of any information system of civil purposes, which manages the critical infrastructure or process in a relevant field, or control systems for special purposes. The basis for the functioning of these systems is information, and because of it the issue of protection is paramount in their functioning. The questions on the choice of general security policy in them, the choice of methods for identification and authentication, authentication of documents, circulating them. This will conceptually define the future of information security records they elaborate.*

Keywords*: information, information systems, comprehensive information security system, method, unauthorized access, security policy,*

I. Introduction and Problem statement

Large-scale application of information systems (IS) in various sectors of society, including commercial activities, management of critical infrastructure facilities or systems of state management, military (air traffic control systems, automated control systems of nuclear power plants, and command and control facilities and other commercial systems) requires solving the issue of information security in them [1]. Information security in the IS aims to prevent access by unauthorized persons and various technical devices to electronic resources (data banks and knowledge banks) and information circulating in the system, for its copying, destruction or distortion. Access to information held in the IS by strangers can cause large economic losses and environmental and technological disasters, and therefore, to prevent these phenomena should develop robust information security system in IC for various purposes. Therefore, the proposed review of certain aspects to develop a comprehensive information security system (CISS) IS has particular relevance to the developer, the formation of different accounting systems to protect information that they have developed [2].

II. Problem solution and Results

The issue regarding the IS Security Policy different function is only possible through an integrated approach to sustainable use of software and hardware (software, hardware) protection and relevant information (including designation system) organizational and technical measures to be implemented in the CISS of a system [1-5].

The organizational measures directed staff to work with the relevant IS (organization of physical protection, responsibility for implementation of personnel protection, the monitoring of performance, protection measures) [3].

Technical (engineering) measures aimed at reducing the dangers caused by external factors influence the operation of the IS (natural disasters, man-made phenomenon, means fire destruction, etc.), providing the required level of survivability of the system and eliminate certain threats to information security through the use of different information security controls and security situation.

Software and hardware (software, hardware) methods provide protection against threats associated with the process of collecting, processing, storage, retrieval, communication system among its users [4-5].

It should be noted that the level of safety and reliability CISS will not only depend on the tools and measures selected for data protection and overall security policy but, in our opinion, and from an integrated application of these measures and methods to implement targeted effect of information security.

In developing CISS developers must firstly define information security policy, such as which methods of security policies to choose - discretionary or mandatory. The simplest method of constructing security policy is discretionary method of access to facilities. When using which the current random access Agent of subjects (users) to other objects IS (using the access matrix). Credentials method of access to facilities using tags matching security levels of subjects and objects. Much easier to operate cocks term security than large-scale matrix fill unstructured access. Therefore, we may suggest a complex (critical) in the development of IS security policy to apply a combination of the two methods.

The second, equally important task is the development of CISS issues of protection from unauthorized access of IS, namely the implementation of identification and authentication of users. The identification of users by using methods that use some material an intimation (access key - "password" media key information - "smart card" measuring biometrics (eye's retina, fingerprints, speech recognition, etc.). These methods differ a complexity, reliability and cost of implementation. for complex (critical) IS appropriate to use methods based on measuring biometric characteristics of users as the most

reliable and accurate (because the unique parameters person do not change over time and are special) and promising technology in this area is to analyze the characteristics of Human DNA. Because users of IS exchange between a variety of documents, they should be sure that the documents are genuine. The authenticity of the documents provided by the use of electronic signatures, allowing through the use of cryptographic techniques (mathematical relationship between the document and the secret and public key digital signature) firmly establish the authorship and authenticity of the document. In this case, each user must have only one secret key and a list of public keys of users IS, formed a "security center" that is trusted by all users and which provides its control. The presence of the user private key, which is interconnected with the public key does not allow him to change his number in the IS and prevents him an opportunity to make signature to the number of another user.

In the third, some IS (including control systems, military systems) should take certain measures to protect against leakage through technical channels and counter reconnaissance equipment, in order to prevent information leaking confidential nature by hiding tell-tale signs, establishing active sources of influence on technical channels of information collection and so on.

III. Conclusions

Some aspects on the development of an integrated system of information security in the IS allow us to conclude that only through a comprehensive approach to the management and use of integrated software and hardware protection of information and appropriate organizational and technical measures possible target implementation of security policy in the IS. This material should be developers account when forming a comprehensive information security system in various information systems.

References

[1] Московитов Н. Перспективы создания глобальной информационной сети МО США / Н. Московитов, Г. Рыбаков // Зарубежное военное обозрение. – 2013. – №7. – С. 8-19.

[2] Martovytskyi V.A. Модель мультиагентної системи збору та зберігання інформації / V.A. Martovytskyi, I.V. Ruban // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2017. – Т. 6 (46). – С. 150-153

[3] Методология создания комплексной системы защиты информации/ Онацкий А.В. // Прикладная радио электроника: научн.-техн. журнал. — 2014. — Том 13. — № 3. — С. 350–356.

[4] [3] ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems —Requirements. [Електрон. ресурс]: – Режим доступу: http://www.itgivernance.co.uk/standards.arx

[5] [4] НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі". [Електрон. ресурс]: – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article ?art_id=46074&cat_id=38835.