подходить к выбору начального вектора весовых коэффициентов, учитывая особенности реализации протокола. Количество ВК должно быть достаточным для формирования секретного ключа. Однако криптостойкость зависит от времени вхождения ИНС в синхронизм. Как вариант, можно формировать секретный ключ как результат конкатенации нескольких более коротких ключей, полученных в результате вхождения ИНС в синхронизм.

DEVELOPMENT OF INFORMATION SECURITY OF CORPORATE INFORMATION SYSTEMS ON THE BASE OF INTELLECTUAL TECHNOLOGIES

ZAHRA GHNABARI, V.A. VISHNYAKOV

The analysis of two directions of intellectual technologies in information security (IS) of corporate information systems (CIS) are given: intellectual supports of decision-making in IS of corporate systems and use it in cloud computing. As tendencies of development are considered improvement of methods, models, architecture, hardware-software decisions IT in IS for corporate systems.

For the development the theory and practice of information security (IS) for corporate information systems (CIS) exists such situation: on the one hand, increased attention to security of information objects, increased requirements for IS, on the other hand, increasing the damage caused by the owners of information resources [1]. The way out of this situation is the introduction in all phases of security the intellectual technology (IT), growing in importance in systems of IS. The main tasks that must address the intellectual system IS (ISIS): security detection the unknown attacks; auto-decision support solutions (DSS) on the redeployment of resources means IS CIS.

In work [2] separate offers on an intellectual problem of DSS are made: it is offered to consider threats as a set of channels of unauthorized access, information leakage and destructive influences; the technique of a numerical assessment of level of information security on a set of these channels is developed; the method of synthesis of rational sets of the means of protection consisting of compatible hardware-software products on criterion function is offered; algorithmic providing a subsystem of DSS on operational management of information security is developed; the architecture of creation of intellectual system of IS is offered.

Results on a problem of intellectual DSS in IS are received in work [1]:

1. The model of counteraction to threats of violation of the information security, based on use of the rational option of reaction of a method of decision-making adapted for a choice, is that the decision on a choice of option of reaction is made depending on probability of attack which is estimated with use of the mechanism of an indistinct logical conclusion, on the basis of data on safety events from various detectors.

2. Method of formation of a rational complex of means of protection being that on the basis of three-level model of protection are developed: morphological matrixes for each of levels; system of hierarchical criteria of quality of means of protection on the basis of their technical characteristics; options of hardware are generated; the rational option of a set for each level of protection on the criterion function maximizing the relation of a total indicator "security of information" to a total indicator of "expenses" gets out.

3. The structure of system of information security joins the rational sets which total cost doesn't exceed the resources allocated for protection that allows to receive a complex of the means of protection certified on the set class of security, meeting requirements to admissible expenses for its realization.

IS in the environment of cloud computing consists on [3]: the mathematical model of software representation is synthesized; the way and algorithm of the formal description of a classifying sign software and approach to an assessment of similarity of various copies of the

software are offered; the verification technique software on existence of destructive properties for environments of cloud computing is synthesized.

As development tendencies of the ISIS use are the following [1, 4]:

– improvement of system architecture of IS in CIS providing effective management in the conditions of uncertainty of a condition of the information environment;

– development of new models of counteraction to threats of violation of IS in CIS on the basis of a choice of optimum option of response to safety events;

– improvement of tool program complexes with intellectual support of decision-making with research of efficiency of methods, models and algorithms;

– development of technologies the multi-agent systems for detection of attacks, counteraction to threats of violation of IS, an assessment of level of security of information in CIS.

References

1. *Mashkina I.V.* // Control systems and information technologies. Voronezh, 2008. No 2 (32). P. 98–104 pp.

2. *Rahimov E.A.* Models and methods of support of decision-making in intellectual system of information security. Abstract PhD on speciality 05.13.19. Ufa: UAI, 2006.

3. *Tumanov Yu.M.* Protection of environments of cloud computing by software verification on existence of destructive properties. Abstract PhD on speciality 05.13.19. M.: MIFI, 2009.

4. *Vishnyakov V.A.* // Proc. of 4th Int. Conf. OSTIS-2014. Minsk: BSUIR, 2014. P. 373–376.

INFORMATION SECURITY TOOLS AND THE USE OF INTELLECTUAL AGENTS

ZAHRA GHNABARI, V.A. VISHNYAKOV

The analysis of methods and means of information protection in information systems is done. The directions of intellectual systems in data protection (ISDP) are given. Learn about how to use expert systems, neural networks, and their combination in DP. The promising method explains how to use intellectual agents in ISDP.

The methods of information protection include: management, obstacle, regulation, motivation, compulsion, concealment of information. Information security tools include: formal (technical, software), informal (organizational, legal, moral and ethical). Levels of information protection can be: the hardware and software, procedural, administrative. legislative. The protection system components: physical security, safety personal, legal security, safety equipment, security software, security is telecommunication environment. Organizational protection measures determine the order: reference system of protection from unauthorized access; restrict access to premises; assignment of access; control and accounting of events; software maintenance; control of protection system.

Implementation of the system of information protection passes steps: the solution concept, system design, implementation, maintenance, sanctions. This are: engineering survey and description of information resources system; identifying the most critical places of the system; probabilistic assessment of threats to the security of information resources; economic evaluation of damage; value analysis of possible ways and means of information security; define profitability of information security systems.

It is must be protected from the point of software view: against loss (backup), invalid access (encrypt, restrict), invalid modification (electronic signature).

Along with the traditional means of protecting enterprise systems: antivirus, detection of vulnerabilities, firewalls and intrusion detectors. The applied automation tools are used including event correlate's, program updates, authentication, authorization, and administration, risk management systems.